Behavioural threshold analysis in the context of information security

DP Snyman

orcid.org/0000-0001-7360-3214

Thesis accepted in fulfilment of the requirements for the degree *Doctor of Philosophy in Computer Science* at the North-West University

Promoter: Prof HA Kruger

Graduation June 2021

20570856

Acknowledgements

This thesis is dedicated to my loving wife, Annuschka, and my three children, Inge, Hannah, and Rebekka (who was born just after submitting the thesis for examination). I am grateful for your support (and sometimes hindrance) over the years that have contributed to me successfully completing this research.

With deep appreciation, I would like to thank my supervisor, Prof Hennie Kruger, for his support and the wealth of knowledge that he contributed to this research. Thank you for inspiring me to always deliver high quality work, and for spending all those uncomfortable hours travelling with me to present this work at the various conferences.

To my colleagues at the School of Computer Science and Information Systems (NWU), thank you for always being interested in my progress. A special thank you to Prof Estelle Taylor (school director), Prof Lynette Drevin (subject chair) and Prof Magda Huisman (research director, Unit for Business Mathematics and Informatics) for providing operational and financial support, which allowed me to be able to travel, and for facilitating periods of study leave that allowed me to focus solely on my research.

To Dr Wayne Kearney (industry partner), and Johann Allers (a former MSc student of mine), thank you for your assistance in the distribution of questionnaires, and to Erik Jonker and Arno Strydom (former BSc Hons students of mine) for their help in programming the decision support system. Thank you, Dr Isabel Swart, for language editing this thesis.

Finally, I would like to acknowledge the various publication editors, conference chairs, and anonymous reviewers for their contributions to the publication of the articles in this thesis.

The boundary lines have fallen for me in pleasant places;
surely I have a delightful inheritance. (Psalm 16:6)

Preface

This thesis is submitted in an article format, in accordance with the General Academic Rules (A.5.4.2) of the North-West University. The series of papers produced in this research comprise thirteen publications. Four of the papers were originally published in conference proceedings after which the conference chairs and editors of related journals identified and invited submissions of extended versions of these papers for further journal publication. Therefore, the extended versions are included in the ensuing nine publications that comprise this anthology thesis:

- Snyman, D. P., & Kruger, H. A. 2017. The application of behavioural thresholds to analyse collective behaviour in information security. *Information & Computer Security, 25*(2):152-164.

  This publication is a journal article extension of the original paper published in conference proceedings upon invitation from the editors: Snyman, D. P. and Kruger, H. A. 2016. *Behavioural thresholds in the context of information security*. In Clarke, N. L. & Furnell, S. M. Eds., Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016), Frankfurt, Germany: Plymouth University, pp. 22-32.

- Snyman, D. P., & Kruger, H. A. 2017. *Optical polling for behavioural threshold analysis in information* security. In Arabnia, H.R., Deligiannidis, L., Hashemi, R., Tinetti, F.G. Eds., Proceedings of the 16th International Conference on Information and Knowledge Engineering (IKE'17), Las Vegas, USA, pp. 39-45.

- Snyman, D. P., Kruger, H. A., & Kearney, W. D. 2018. I shall, we shall, and all others will: Paradoxical information security behaviour. *Information & Computer Security, 26*(3):290-305.

  This publication is a journal article extension of the original paper published in conference proceedings upon invitation from the editors: Snyman, D. P., Kruger, H. A., & Kearney, W. D. 2017. *The lemming effect in information security.* In Clarke, N. L. & Furnell, S. M. Eds., Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017), Adelaide, Australia, pp. 91-103.

- Snyman, D. P., & Kruger, H. A. 2019. Behavioural threshold analysis: Methodological and practical considerations for applications in information security. *Behaviour & Information Technology, 38*(11):1-19.

- Snyman, D. P., & Kruger, H. A. 2019. *Theorising on information cascades and sequential decision-making for analysing security behaviour*. In Mori, P., Furnell, S. M., & Camp, O. Eds., Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP2019), Prague, Czech Republic, pp. 205-212.

- Snyman, D. P., & Kruger, H. A. 2020. Contextual factors in information security group behaviour: A comparison of two studies. Submitted to *Communications in Computer and Information Science.* Springer International Publishing.

  This publication is a journal article extension of the original paper published in conference proceedings upon invitation from the editors: Snyman, D. P., & Kruger, H. A. 2020. *External contextual factors in information security behaviour*. In Furnell, S. M., Mori, P., Weippl, E., & Camp, O. Eds., Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), Valletta, Malta, pp. 185-194.

- Snyman, D. P., & Kruger, H. A. 2020. A management decision support system for evaluating information security behaviour. In Venter, H, Loock, M., Coetzee, M., Eloff, M., & Eloff, J. Eds., *Information and Cyber Security - 18th International Conference, ISSA 2019, Johannesburg, South Africa, August 15, 2019, Proceedings* (1st ed.): Springer International Publishing, pp. 15-27.

- Snyman, D. P., & Kruger, H. A. 2020. Collective information security behaviour: A technology-driven framework. To appear in *Information & Computer Security.*

  This publication is a journal article extension of the original paper published in conference proceedings upon invitation from the editors: Snyman, D. P., & Kruger, H. A. 2020. Information security behavioural threshold analysis in practice: An implementation framework. In Clarke, N. L. & Furnell, S. M. Eds., *Advances in Information and Communication Technology: Proceedings of the 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, 2020* (Vol. 593): Springer International Publishing, pp. 133-143.

- Snyman, D. P., & Kruger, H. A. 2020. Group behaviour in Cybersecurity. To appear in *Encyclopedia of Cryptography, Security and Privacy* (5th ed.): Springer International Publishing.

The original versions of extended journal articles, which were published in conference proceedings, are available in the Appendices.

In accordance with academic rules A5.10.8 and A5.10.9, the co-authors of the articles in this thesis, Prof HA Kruger (Promoter) and Dr WD Kearney (industry partner), hereby give permission to the candidate, Mr DP Snyman, to include these articles as part of a PhD thesis. The contributions (advisory and supportive) of these co-authors were kept within reasonable limits, thereby enabling the candidate to submit this thesis for examination purposes.

This thesis therefore serves as fulfilment of the requirements for the degree *Doctor of Philosophy in Computer Science* within the *School of Computer Science and Information Systems* in the *Faculty of Natural and Agricultural Sciences* at the *North-West University*.

Declaration

This serves to confirm that I, Isabella Johanna Swart, registered with and accredited as professional translator by the South African Translators' Institute, registration number 1001128, language edited the following thesis:

Behavioural threshold analysis in the context of information security

by

Dirk Snyman

Dr Isabel J Swart

Date: 12 December 2020

23 Poinsettia Close
Van der Stel Park
Dormehlsdrift
GEORGE
6529
Tel: (044) 873 0111
Cell: 082 718 4210
e-mail: isaswart@telkomsa.net

Abstract

The human aspect in information security provides a unique challenge for its assessment and management. Many studies seek to address this challenge by employing psychological models to understand the behaviour of individuals when confronted with information security issues. Such models typically only address the behaviour of individuals and do not provide for the intricacies of the behaviour of people in groups. Few models exist to quantify group behaviour and as far as the researcher is aware, none have been applied in information security group behaviour before. Based on *threshold models of collective behaviour*, behavioural threshold analysis is used to quantify the individual inclinations of the members of a group and, based on the aggregation of these quantifications, predict possible outcomes of the collective behaviour of that group. Therefore, this study aims to address the following research question: *How can behavioural threshold analysis be employed as an aid for managing the human factor in information security group behaviour?*

In this thesis as a series of papers, research articles are presented that describe the full range of activities that relate to the establishment of behavioural threshold analysis as a novel method for the evaluation of information security group behaviour. The approach is developed from the ground up and the activities that are described include, the initial exploratory investigation of the model in the new context of information security, the investigation of alternative strategies for fine-tuning the approach, the establishment of a formal methodology, real-world applications of the formal method in practice, and the development of practical and theoretical artefacts that can be used by future researchers and practitioners.

This study makes contributions in three categories: literature, theory and practice. By publishing the findings and contributions in journals, conference proceedings, and book series, new knowledge is contributed to the existing body of literature. Theoretical contributions include a formalised methodology and application framework. The contribution to the practice of information security is in the form of a decision support system. Therefore, by adopting an approach from the field of sociology, which was previously not applied in the field of information security, and adapting it to the unique and specialised requirements for evaluating information security group behaviour, the research question was answered.

Key terms: Behavioural threshold analysis; human aspects of information security; information security awareness; information security decision support system; information security group behaviour; information security implementation framework; sequential decision-making; theory of planned behaviour.

TABLE OF CONTENTS

Acknowledgements ..... **i**

Preface ..... **ii**

Declaration ..... **iv**

Abstract ..... **v**

List of Tables ..... **xiii**

List of Figures ..... **xiv**

CHAPTER 1 - PROBLEM STATEMENT AND RESEARCH DESIGN **1**

1.1 Chapter introduction **2**

1.2 Contextualisation **2**

1.3 Problem statement and primary research question **4**

1.4 Secondary research questions **4**

1.5 Aims and objectives **5**

1.6 Research design and methodology **6**

1.6.1 Research design 6

1.6.2 Methodology 8

1.6.3 Ethical considerations 9

1.7 Chapter deployment **10**

1.8 Contributions of the study **13**

1.9 Chapter summary **15**

Chapter references **16**

CHAPTER 2 - LITERATURE REVIEW 18

2.1 Chapter introduction 19

2.2 Literature review methodology 19

2.3 Overview of relevant literature 19

2.3.1 Information security 20

2.3.2 Behavioural information security: Models and theories 23

2.3.2.1 Individual behaviour 23

2.3.2.2 Group behaviour 29

2.3.3 Behavioural threshold analysis contextualised for information security 31

2.3.3.1 Definition 31

2.3.3.2 Background – Group behaviour 31

2.3.3.3 Application – Example in cybersecurity 32

2.3.4 Sources for further reading 36

2.4 Chapter summary 42

Chapter references 43

CHAPTER 3 - ARTICLE I: THE APPLICATION OF BEHAVIOURAL THRESHOLDS TO ANALYSE COLLECTIVE BEHAVIOUR IN INFORMATION SECURITY 53

3.1 Preamble to Article I 55

3.2 Emerald journal style requirements 56

3.3 Article I 56

3.3.1 Introduction 57

3.3.2 Contextual background 59

3.3.3 Typical threshold analysis 63

3.3.4 Illustrative example of threshold analysis in the context of information security 64

3.3.5 Future work 67

3.3.6 Conclusion 67

3.3.7 References 68

CHAPTER 4 - ARTICLE II: OPTICAL POLLING FOR BEHAVIOURAL THRESHOLD ANALYSIS IN INFORMATION SECURITY 70

4.1 Preamble to Article II 72

4.2 IKE'17 conference proceedings style requirements 73

4.3 Article II 73

4.3.1 Introduction 74

4.3.2 Background 75

4.3.3 Methodology 76

4.3.4 Discussion 79

4.3.5 Conclusion 79

4.3.6 References 80

CHAPTER 5 - ARTICLE III: I SHALL, WE SHALL, AND ALL OTHERS WILL: PARADOXICAL INFORMATION SECURITY BEHAVIOUR 81

5.1 Preamble to Article III 83

5.2 A note on the authors 84

5.3 Emerald journal style requirements 84

5.4 Article III 84

5.4.1 Introduction 85

5.4.2 Behavioural threshold analysis 87
5.4.3 Application of behavioural threshold analysis 88
5.4.4 Results 91
5.4.5 Discussion 96
5.4.6 Conclusion and future work 98
5.4.7 References 98

CHAPTER 6 - ARTICLE IV: BEHAVIOURAL THRESHOLD ANALYSIS: METHODOLOGICAL AND PRACTICAL CONSIDERATIONS FOR APPLICATIONS IN INFORMATION SECURITY 101

6.1 Preamble to Article IV 103

6.2 Taylor & Francis journal style requirements 104

6.3 Article IV 104

6.3.1 Introduction 105
6.3.2 Related work 107
6.3.3 Information security behaviours 110
6.3.4 Example information security questions for behavioural threshold analysis 111
6.3.5 Illustrative case studies 113
6.3.6 Proposed methodology 115
6.3.7 Validation 117
6.3.8 Reflection 119
6.3.9 Conclusion 120
6.3.10 References 121

CHAPTER 7 - ARTICLE V: THEORISING ON INFORMATION CASCADES AND SEQUENTIAL DECISION-MAKING FOR ANALYSING SECURITY BEHAVIOUR.....124

7.1 Preamble to Article V.....126

7.2 ICISSP conference proceedings style requirements 127

7.3 Article V 127

7.3.1 Introduction 128

7.3.2 Sequential decision-making 129

7.3.3 Illustrative case study.....131

7.3.4 Reflection 133

7.3.5 Conclusion 134

7.3.6 References.....135

CHAPTER 8 - ARTICLE VI: CONTEXTUAL FACTORS IN INFORMATION SECURITY GROUP BEHAVIOUR: A COMPARISON OF TWO STUDIES 136

8.1 Preamble to Article VI.....138

8.2 Springer book chapter style requirements 139

8.3 Article VI 139

8.3.1 Introduction 140

8.3.2 Information security behaviour: a product of circumstance?.....142

8.3.3 Experimentation 145

8.3.4 A comparison of two studies through behavioural threshold analysis.....150

8.3.5 Discussion.....154

8.3.6 Conclusion 157

8.3.7 References.....159

8.3.8 Appendix 161

CHAPTER 9 - ARTICLE VII: A MANAGEMENT DECISION SUPPORT SYSTEM FOR EVALUATING INFORMATION SECURITY BEHAVIOUR 164

9.1 Preamble to Article VII 166

9.2 Springer book chapter style requirements 167

9.3 Article VII 167

9.3.1 Introduction 168

9.3.2 Background 170

9.3.3 Description of the system 172

9.3.4 Critical reflection 177

9.3.5 Conclusion and future work 179

9.3.6 References 179

CHAPTER 10 - ARTICLE VIII: COLLECTIVE INFORMATION SECURITY BEHAVIOUR: A TECHNOLOGY-DRIVEN FRAMEWORK 181

10.1 Preamble to Article VIII 183

10.2 Emerald journal style requirements 184

10.3 Article VIII 184

10.3.1 Introduction 185

10.3.2 Literature review 186

10.3.3 Framework model and development 189

10.3.4 Framework evaluation 192

10.3.5 Technology dimension 195

10.3.6 Contributions 198

10.3.7 Conclusion 198

10.3.8 References....199

CHAPTER 11 - SUMMARY AND CONCLUSION 202

11.1 Chapter introduction 202

11.2 Synopsis of the study 202

11.3 Contributions of the study....207

11.4 Limitations and directions for future research 209

11.5 Chapter summary 209

Appendix A – Group behaviour in cybersecurity (*Encyclopedia of Cryptography, Security and Privacy*)....210

Appendix B – Behavioural thresholds in the context of information security (HAISA2016)....216

Appendix C – The lemming effect in information security (HAISA2017) 228

Appendix D – External contextual factors in information security behaviour (ICISSP2020) 242

Appendix E – Behavioural threshold analysis in practice: An implementation framework (HAISA2020)....253

Appendix F – Information and Computer Security publication guidelines (Emerald) 265

Appendix G – Proceedings publication guidelines (IKE'17) 276

Appendix H – Behaviour & Information Technology publication guidelines (Taylor & Francis) 281

Appendix I – SCITEPRESS proceedings publication guidelines (ICISSP2019/20)....288

Appendix J – Springer book chapter publication guidelines....298

Appendix K – Information security behavioural threshold analysis measurement instrument....311

List of Tables

This list contains only the tables of Chapters 1, 2, and 11. The tables that form part of the published articles that are included in the various chapters are not listed here.

Table 2.1: Example measurement instrument 32

Table 2.2: Cumulative threshold table 33

Table 2.3: Alphabetical list of additional literature sources 36

List of Figures

This list contains only the figures of Chapters 1, 2, and 11. The figures that form part of the published articles that are included in the various chapters are not listed here.

Figure 1.1: Design science research cycles (Hevner & Chatterjee, 2010) 7

Figure 1.2: Activities of this study in the context of the Design Science Research cycles of Hevner and Chatterjee (2010) 9

Figure 1.3: Graphical representation of chapter deployment 14

Figure 2.1: Theory of reasoned action (Fishbein, 1979) 27

Figure 2.2: The theory of planned behaviour (Ajzen, 1991) 28

Figure 2.3: Cumulative threshold graph 34

Chapter 1
-
Problem statement and research design

Chapter table of contents

1.1 Chapter introduction 2

1.2 Contextualisation 2

1.3 Problem statement and primary research question 4

1.4 Secondary research questions 4

1.5 Aims and objectives 5

1.6 Research design and methodology 6

1.6.1 Research design 6

1.6.2 Methodology 8

1.6.3 Ethical considerations 9

1.7 Chapter deployment 10

1.8 Contributions of the study 13

1.9 Chapter summary 15

Chapter references 16

1.1 Chapter introduction

Chapter 1 serves to introduce the reader to the context of this research and provide background on the research problems, questions, aims, and objectives of this study. To this end, this chapter is deployed in the following manner:

- Contextualisation;
- Problem statement and research question;
- Research aims and objectives;
- Research paradigm, design, and methodology;
- Thesis layout; and
- Contributions of the study.

Each subsequent chapter concludes with a summary and the bibliography details of the references that were used in the chapter.

1.2 Contextualisation

Information security forms an integral part of any modern organisation (Vaidya, 2019). In this context, information security refers to the protection of the information-related assets of an organisation. Traditionally, this included both physical and technological aspects of information protection, but in the contemporary landscape has become synonymous with the protection of digital assets and the information contained therein and is therefore often referred to as cybersecurity (Lundgren & Möller, 2019). Without adequate protection afforded by high levels of information security, organisations and their information systems are at risk of being targeted by malicious individuals or groups that seek to exploit them for their own (financial) gain. Some of the associated risks include financial losses, reputational damage, and physical safety issues. These information systems are inextricably linked to those who develop and use them. As such, the human factor in information security is widely recognised as a vital aspect that evokes much interest and research. This integral part of information security is also commonly considered one of the most troublesome to secure and manage (Furnell *et al.*, 2019). Humans are prone to unpredictable and even paradoxical behaviour. Controls, policies, and procedures that are put in place to minimise information security risks are voluntarily disregarded or circumvented for the sake of comfort or ease associated with the use of a system. This is even the case when such behaviour is known to be risky or even dangerous. Further compounding this issue is the naïve and accidental behaviours that humans sometimes exhibit concerning security. They do not even

realise that there is risk involved in certain actions and may be unaware of suggested best practices and expose their organisation through inexperience (Calic *et al.*, 2016). It is precisely this erratic nature of human behaviour in information security that necessitates close scrutiny in order to safeguard organisations and systems, but which makes investigating the underlying issues a difficult endeavour.

One of the most popular (and arguably most successful) approaches to assess human behaviour in general is to conceptually map and model behaviour and apply such models to real-world behaviour (Kuppusamy *et al.*, 2020). Combining the leading principles of the fields of behavioural psychology and information security, has given rise to a research field with the specific focus on addressing information security behaviour, and by extension the human factor in information security. This relatively new field is called *behavioural information security* (Crossler *et al.*, 2013). Many psychological models exist that attempt firstly, to help to understand the phenomenon that is human behaviour, and secondly, once the phenomenon is understood, help to address it through structured interventions to address the root cause of said behaviour. This approach of applying behavioural models is also favoured in behavioural information security research. One of the limitations of most of the models on which these approaches are built on is that they only focus on individuals and individual behaviour. Contextual factors such as group behaviour are not considered in the associated research, which leaves a gap in the existing literature that begs to be filled.

It is for these reasons that this study that investigates new models to assess, and methods to address group behaviour in information security, was undertaken. Specifically this research investigates the *threshold models of collective behaviour* (Granovetter, 1978) as a possible underlying theory for understanding group behaviour. The model posits that individuals are influenced by group behaviour and other external factors and it is subsequently applied to information security. Behavioural threshold analysis, which can be used to assess group behaviour and predict future outcomes, is then employed as a method for evaluating information security group behaviour.

Currently, there is no mention in the literature of this model and method being applied to information security and therefore this study develops the concept from the ground up. This involves synthesising new knowledge from a collection of detached ideas and theories, leading to a mature behavioural information security approach. This contribution of a novel information security group behaviour approach to the body of knowledge helps in filling the existing gap in literature.

1.3 Problem statement and primary research question

The aforementioned contextualisation establishes a link between behaviour and information security. It was indicated that there is a lack of behavioural information security models able to evaluate group behaviour in this environment. Therefore, this study will aim to answer the following research question: *How can behavioural threshold analysis be employed as an aid for managing the human factor in information security group behaviour?*

1.4 Secondary research questions

In Section 1.3, the primary research question was established. In order to ultimately answer this question, six secondary research questions are identified that each addresses a more specific theme to support the research question that is of a more general nature. These secondary questions are expressed as follows:

- *What is the current state of behavioural information security with specific regard to the models and methods to address the human factor in information security?*

  Behavioural models that are currently used to assess information security behaviour focusses on factors of individual behaviour, *e.g.* attitude and intention, and do not provide for behaviour in groups. The environment or context such as a corporate environment or educational institution is also not considered This question serves to investigate possible gaps in the existing literature where this study can contribute to the field of behavioural information security.

- *Can behavioural threshold analysis be applied to assess information security group behaviour?*

  Behavioural threshold analysis is currently proposed in literature as a generic mechanism for evaluating any group behaviour scenario. Therefore, it is imperative to critically reflect upon whether this generic approach is applicable to information security behaviour.

- *How can generic behavioural threshold analysis be improved for applications in the context of information security?*

  Depending on whether the previous question could be satisfactorily answered, investigate the opportunities that arise to tailor the generic behavioural threshold analysis approach to be a better fit for information security group behaviour assessments through experimental applications. The experimental results can be used to answer this secondary research question by establishing specialised requirements.

- *How can behavioural threshold analysis be established as a novel approach for evaluating information security group behaviour?*

  Given the specialised requirements for applying behavioural threshold analysis in information security behaviour, this question is based on the formalisation of the methodology and related measurement instrument.

- *Can this novel approach, based on the formalised methodology, be successfully applied in practical real-world contexts to assess information security group behaviour?*

  Using the methodology that was established, apply the approach to test its efficacy in practice. This question addresses the issue of validating the proposed approach through applications in different contexts.

- *How can this approach be embodied as a supporting tool to contribute to the theory of behavioural information security and the management of the human factor in practice?*

  Enable practitioners to use the approach that was developed through practical and theoretical artefact deliverables. For the former, automate parts of the application of behavioural threshold analysis by means of a software system. The latter addresses the bridging of the gap between behavioural information security research and its implementation in practice.

The resulting aims and objectives of this research are discussed in the following section.

1.5 Aims and objectives

The primary aim of this research is to *develop a mechanism whereby information security behavioural threshold analysis may be used as a tool to contribute to the management of the human factor in information security.* The objectives that need to be achieved in order to realise the primary aim are inferred from the secondary research questions that are established in the previous section. These objectives comprise the following activities through which the purpose is to obtain answers to said questions:

1. *Conduct* a literature review on topics relating to human behaviour, information security, and behavioural threshold analysis;
2. *Perform* an initial assessment of the suitability of behavioural threshold analysis for information security by experimenting with the application of the model within this context;
3. *Determine* best practises for data collection for behavioural threshold analysis when it is applied to information security;
4. *Apply* behavioural threshold analysis in a real-world setting to assess an organisation's information security and evaluate the newly adapted approach at the same time;

5. *Construct* and *validate* a formal methodology and provide practical guidance for applications in information security;
6. *Evaluate* the applicability of employing behavioural threshold analysis to assess group behaviour, based on other theoretical models of group behaviour to substantiate its validity;
7. *Compare* different industries in terms of their information security behavioural threshold analysis results, related to the difference in environments;
8. *Contribute* to the practice of behavioural information security by automating implementations of the identified methods whereby behavioural threshold analysis may be employed as a tool for information security management; and
9. *Contribute* to the theory and practice of behavioural information security by creating and *validating* a framework for applying the proposed approach in the real world.

1.6 Research design and methodology

This section addresses the research design and methodology that guides the research activities of this study. Ethical considerations are also highlighted.

1.6.1 Research design

The initial description of the *threshold model of collective behaviour* (Granovetter, 1978; Granovetter & Soong, 1983) and an analogical application thereof through *behavioural threshold analysis* (Growney, 1983) introduce the core theory and approach to evaluating group behaviour that is employed in this research to the otherwise sparse body of literature. In its simplest form, behavioural threshold analysis can be performed by surveying people in a group environment and mathematically analysing the resulting data on individuals' thresholds in order to predict group behaviour. To the best of the author's knowledge, no literature existed to describe the application of the model on a terrain, such as information security at the start of this study. As such, this investigation entails a bottom-up approach to assess the suitability of the model and, if needed, to adapt the approach for its application in information security. This leads to ultimately delivering research artefacts of both a theoretical and practical nature to contribute to filling the gaps in existing knowledge and literature.

Many studies in computer science, information systems, and engineering that seek to follow such an exploratory and developmental approach draw on the principles of a Design Science Research (DSR) method for structuring the different research activities that form part of such studies (Hevner & Chatterjee, 2010; Vaishnavi & Kuechler, 2015; Van der Merwe *et al.*, 2020).

DSR is succinctly defined as:

> *"… a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artefacts, thereby contributing new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem."* (Hevner & Chatterjee, 2010:5)

DSR is structured to include three interrelated and iterative research cycles, namely *relevance*, *design*, and *rigour* (Hevner & Chatterjee, 2010). These cycles are represented in Figure 1.1 and are subsequently briefly introduced.

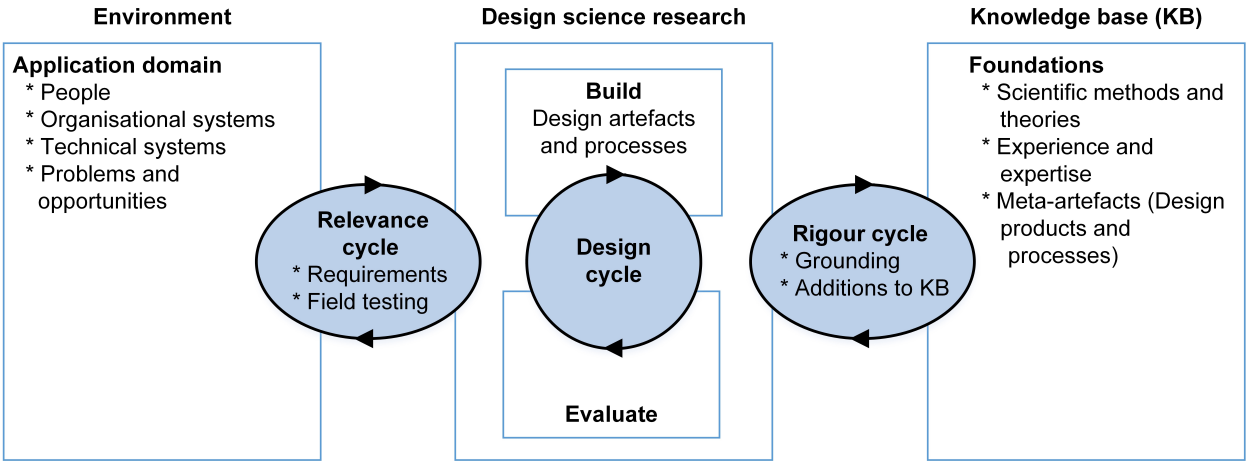


Figure 1.1: Design science research cycles (Hevner & Chatterjee, 2010)

The *relevance cycle* concerns the environment and context in which the research is to be performed and eventually where the research is to have an impact. Relevance also entails an assessment of the requirements for solutions in the specific context and provides a platform for trial and error applications of candidate solutions and artefacts after iterations of the design cycle. The fundamental cycle of DSR, the *design cycle*, is where the innovative design and implementation of artefacts, solutions, and processes take place. Iterative evaluation is a crucial activity whereby the artefact is assessed against specific criteria to determine whether it is fit for purpose. While the first two cycles have a more practical inclination, the *rigour cycle* grounds the developed artefact in science. Theories and methods from the scientific body of knowledge feed into the development of the artefact. In turn, during the design cycle, new knowledge is generated through artefact development and evaluation. This new knowledge generates experience and insight, which contributes to expanding the scientific knowledge base, especially through peer-reviewed publication. Given the similarities between the aforementioned aims and objectives and those of the activities guided by DSR, the same was identified as the overarching research method for this study.

1.6.2 Methodology

This study is structured around a series of research articles. As such, the research activities that are performed extend the aims and objectives and correspond to the subsequent chapter deployment (see Section 1.7). This methodology is described as follows:

- *Conduct* a literature review with specific focus on general information security, security awareness, behavioural information security models for individual and group behaviour, and behavioural threshold analysis;
- *Apply* threshold models of collective behaviour and behavioural threshold analysis to group behaviour in information security in an exploratory experiment to *test* the suitability thereof and *learn* the strengths and weaknesses of the approach in its original form (see Article I in the following section);
- *Refine* the data collection method based on the insights from the first application of behavioural threshold analysis in information security (Article I) and experimentally *test* the new data collection method to show its compatibility (Article II);
- After the adaptation of the different aspects of the model has been completed, *apply* the model in a real-world environment to assess the human aspects of an organisation's information security practises while simultaneously *testing* the redesigned approach (Article III);
- Based on the evidence in Articles I-III, *formalise* (theoretical artefact) the measurement instrument and methodology that are used for behavioural threshold analysis in information security and confirm the validity through a series of experiments (Article IV);
- The method that was established in Article IV for behavioural threshold analysis in information security, is applied to evaluate group behaviour contextualised as sequential decision-making to evaluate the rigour of the approach when applied across domains (Article V);
- *Compare* the results of behavioural threshold analysis for information security in different contextual settings (Article VI);
- *Create* a decision support system (practical software artefact) to facilitate future applications of information security behavioural threshold analysis in organisational settings (Article VII); and finally
- *Conceptualise* a framework (theoretical artefact) by which the maturity of the finalised approach is assessed for applications in practise (Article VIII).

Each of these activities can be placed in context of the aforementioned DSR approach as indicated in Figure 1.2. It should be noted that some activities contribute to more than one cycle. However, they are classified according to their main contribution and coherence in the context of this specific study's relation to DSR.

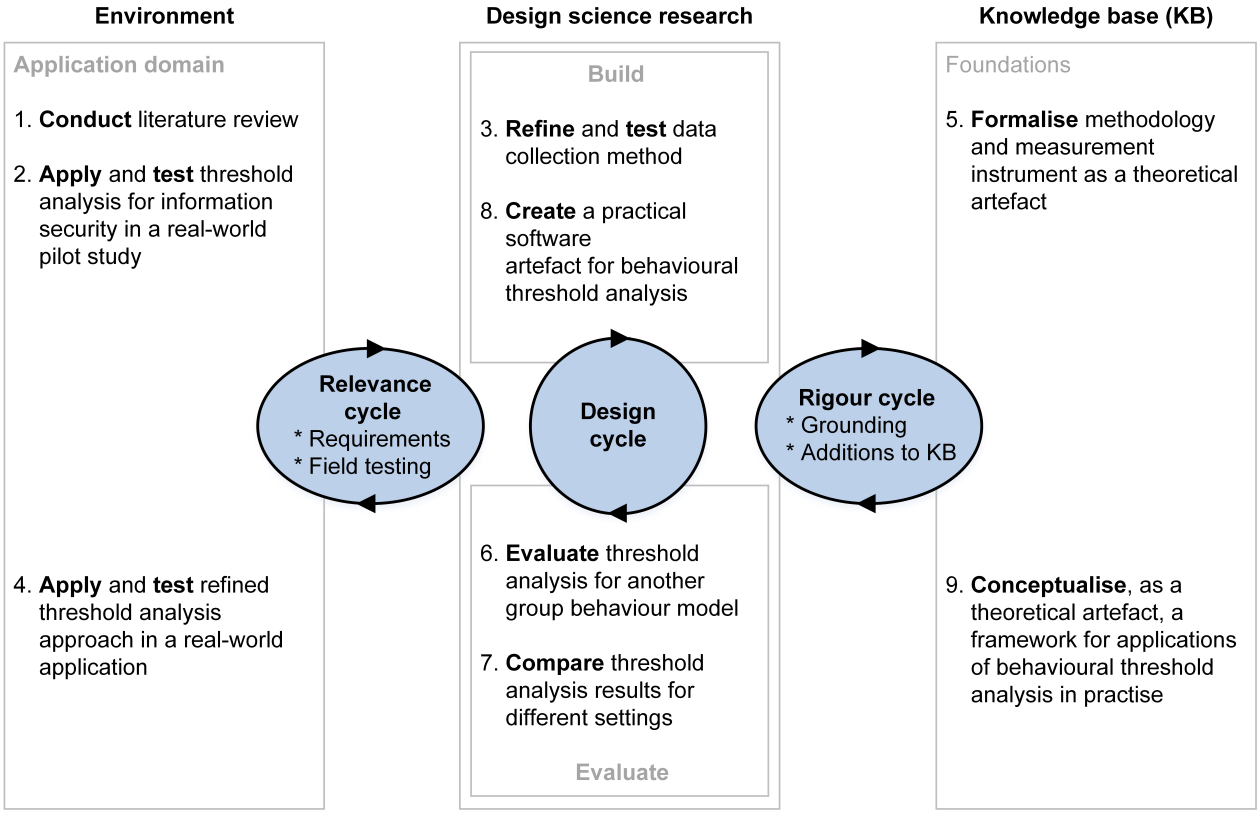


Figure 1.2: Activities of this study in the context of the Design Science Research cycles of Hevner and Chatterjee (2010)

1.6.3 Ethical considerations

Ethical clearance for this study was obtained after related ethical considerations were evaluated both by the scientific committee of the School of Computer Science and Information Systems, and by the Faculty of Natural and Agricultural Sciences ethics committee at the North-West University. The study was approved as a no-risk project with ethics number NWU-01208-19-S9.

In the submission to the ethics committee, attention was given to the following:

- Participation in this study is not compulsory. If a respondent or participant wishes to decline their participation or withdraw at a later stage, he/she may do so at any time;
- If he/she agrees to participate in the study, he/she is not likely to experience any risk or specific distress from answering questions in the survey;

- He/she will not receive any payment or personal benefit from participating in this research;
- All participants need to complete an informed consent form in order get access to the surveys. The surveys are facilitated through Google Forms;
- He/she will be asked to complete a series of questions about her/his personal inclination towards behaviour about certain information security related scenarios;
- Once the online surveys are completed, the researcher will utilise the data for purposes of analysis and mathematical aggregation;
- The results of this study will contribute to scientific knowledge and promote better management of information security within organisations, but will probably have no benefits or risks to a participant;
- Any information that he/she provides will be kept strictly private, confidential, and anonymous. His/her personal identifying information will not be collected with the survey responses in any way and as such no response can be connected to an individual; and
- Results from this study will be presented as statistical summaries and other analysis results, but no information will be presented about individual participants/respondents.

1.7 Chapter deployment

The remainder of this thesis as a series of papers is structured as follows:

Chapter 2 – Literature review

The relevant literature is summarised and presented in this chapter. The main themes that are introduced include information security in general, security awareness, behavioural information security, and behavioural threshold analysis. A submission to the forthcoming 5th edition of the *Encyclopedia of Cryptography, Security and Privacy* is employed in this chapter to facilitate the discussion on behavioural threshold analysis (see Section 2.4).

Chapter 3 – Article I: *The application of behavioural thresholds to analyse collective behaviour in information security*

Generic behavioural threshold analysis is presented and applied in the domain of information security by collecting data on the behavioural thresholds of individuals in a group setting and how the individuals influence each other in terms of information security behaviour. This paper describes an exploratory study that was performed to gauge the suitability of the approach for assessing information security behaviour.

Chapter 4 – Article II: *Optical polling for behavioural threshold analysis in information security*

Many psychological and sociological models exist to describe, and test human behaviour. Such approaches are all reliant on data. This article presents a novel approach for data collection for the specific application of behavioural threshold analysis. It addresses some of the data collection issues associated with behavioural threshold analysis which were identified from Chapter 3, Article I, as well as behavioural information security research in general.

Chapter 5 – Article III: *I shall, we shall, and all others will: Paradoxical information security behaviour*

The first full-scale application of behavioural threshold analysis in an industry setting is presented. The model is applied after adapting the measurement instrument based on lessons learned from Articles I and II (Chapters 3 and 4) to attempt to address any deficiencies that were identified. Behavioural threshold analysis is used to identify and describe information security problem areas in the surveyed department within an organisation.

Chapter 6 – Article IV: *Behavioural threshold analysis: Methodological and practical considerations for applications in information security*

The application of behavioural threshold analysis to analyse group behaviour in information security presents a unique challenge in terms of the measurement instruments used to gather the relevant attitude data. This paper presents an analysis of the specialised requirements for such a measurement instrument and makes recommendations on the content and presentation of information security topics in this context. Once again, this article draws on the experiences gleaned through Articles I, II, and III (Chapters 3, 4 and 5) and formalises the methodology and practical strategy for applications of behavioural threshold analysis in information security.

Chapter 7 – Article V: *Theorising on information cascades and sequential decision-making for analysing security behaviour*

Individual behaviour formation in information security is often reliant on the example that is set by others. The observation of the behaviour of others and the influence on one's own behaviour can be described as sequential decision-making, *i.e.,* one decision informs another. This process can be formally explained as an instance of information cascades. Information security behavioural threshold analysis (as conceptualised in Chapter 6, Article IV) is proposed as a method for evaluating sequential decision-making in the context of information security. The reasoned arguments put forth in this paper corroborate the appropriateness of behavioural threshold analysis as a valid method for evaluating information security group behaviour.

Chapter 8 – Article VI: *Contextual factors in information security group behaviour: A comparison of two studies*

The role and influence of the environment (context) on an individual's behaviour (specifically with reference to information security behaviour) are investigated in this paper. Most studies only address individual thought processes and fail to incorporate the influence of external forces in the human group behaviour equation. A practical experiment is conducted in an academic residence setting. The resulting evaluation is compared against the industry experiment from Article III, Chapter 5, to assess how the differences in environment, *i.e.,* contextual factors, result in different information security group behaviour between the two groups. The methodology for applying behavioural threshold analysis in information security, as established in Chapter 6, Article IV, was used as the theoretical underpinning for the experiments.

Chapter 9 – Article VII: *A management decision support system for evaluating information security behaviour*

The methodology and strategy for information security behavioural threshold analysis created in Chapter 6, Article IV, are embodied as a software decision support system (DSS) in this article. This system automates much of the process of performing behavioural threshold analysis exercises in an organisational setting. After initial expert involvement, the DSS empowers otherwise lay managers to perform assessments of the levels of information security group behaviour of their workforce and to identify problem areas.

Chapter 10 – Article VIII: *Collective information security behaviour: A technology-driven framework*

Article VIII represents the culmination of the preceding research by proposing an implementation framework for applying information security behavioural threshold analysis in practise. This framework is critically evaluated through exploiting a combination of two qualitative framework evaluation methods. The findings from the former articles (Articles I-VII, Chapters 3-9) are used to substantiate the successful evaluation of the implementation framework while observing the evaluation criteria. Emphasis is placed on the technology dimension of framework implementation and validation.

Chapter 11 – Conclusion

In this final chapter, the study is concluded by summarising the different papers and reflecting on how the stated objectives were reached. The contributions of this research are discussed. Subsequent recommendations from the study will also be presented in this chapter. Future avenues for investigation in behavioural threshold analysis in information security are identified.

The chapter layout is subsequently presented as a graphical representation of the journal articles, book chapters, and papers in conference proceedings that are included in these collected works. Their logical order and interrelatedness are presented in Figure 1.3, which follows on the next page. The diagram will also be employed at the start of each chapter to serve as contextualisation for the reader.

1.8 Contributions of the study

The contributions of this study are summarised here and are revisited in detail in the conclusion in Chapter 11. The main contribution of this study is the development of a novel mechanism for evaluating information security group behaviour through the application of behavioural threshold analysis. To accomplish this main contribution, the following additional contributions were made:

- Contributed the first ever application of behavioural threshold analysis in the context of information security;
- Identified novel techniques for the specialised data collection required for information security behavioural threshold analysis;
- Identified suitable information security themes for behavioural threshold analysis;
- Contributed a validated methodology for information security behavioural threshold analysis;
- Contributed a theorisation on behavioural threshold analysis and its applicability to assess group behaviour in the context of other models;
- Identified contextual factors that influence information security group behaviour in different industries;
- Contributed a practical mechanism for using information security behavioural threshold analysis results as a management tool; and
- Contributed a framework for guiding the practical application of information security behavioural threshold analysis.

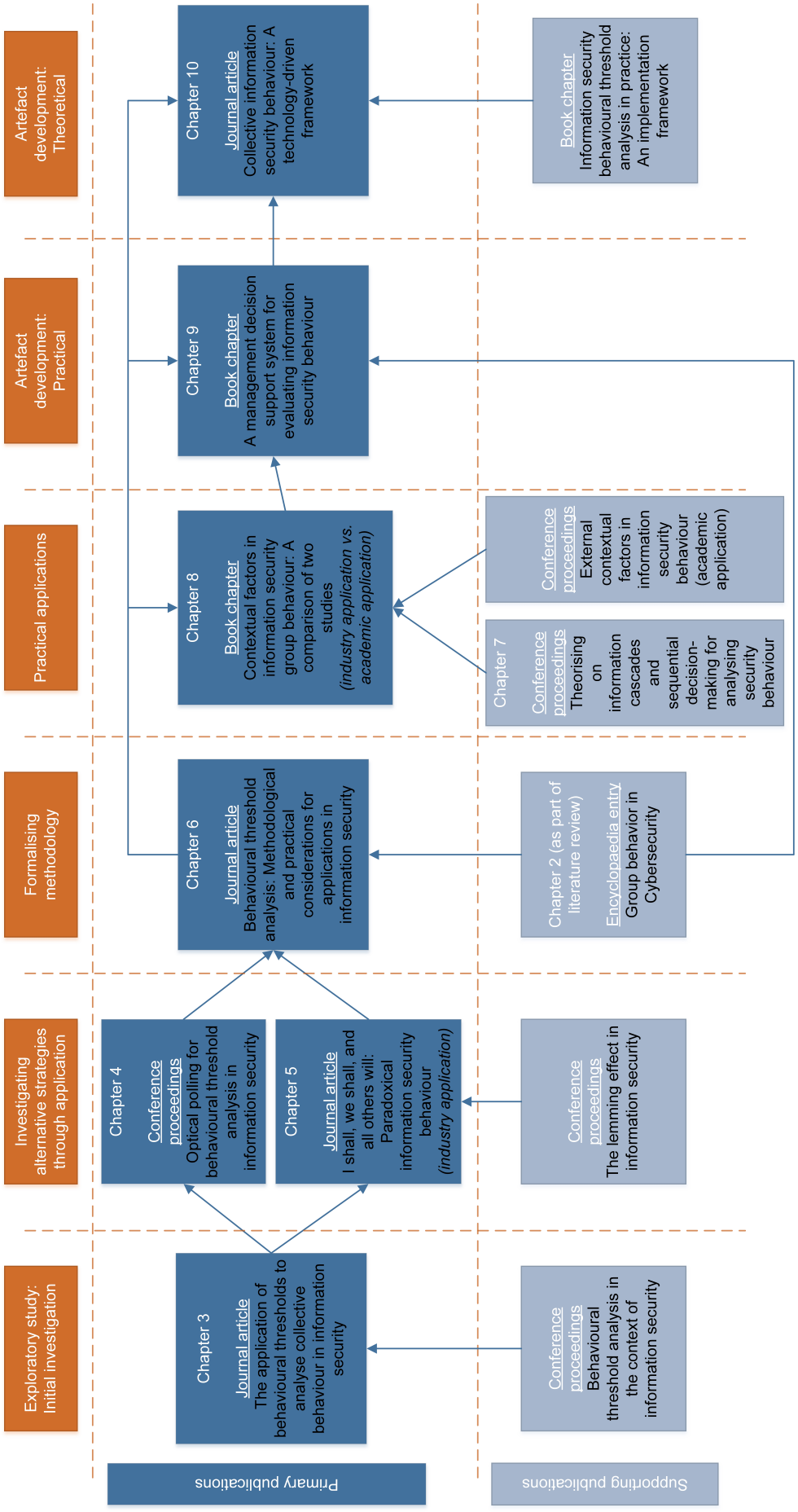


Figure 1.3: Graphical representation of chapter deployment

1.9 Chapter summary

In Chapter 1, the research study was introduced. The study was contextualised whereafter a problem statement and research questions were formulated. Research aims and objectives were stated, and specific attention was given to how they relate to the underlying research design and methodology and ultimately, influence the chapter deployment and structure of this thesis. The chapter concludes with a look ahead at the envisaged contributions of this study.

Chapter references

Calic, D., Pattinson, M., K., P., Butavicius, M. and McCormac, A. 2016. Naïve and accidental behaviours that compromise information security: What the experts think. In Proceedings of the *Tenth International Symposium on Human Aspects of Information Security & Assurance*, Frankfurt, Germany: Plymouth University, pp. 12-21.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. and Baskerville, R. 2013. Future directions for behavioral information security research. *Computers & Security,* 32(2013):90-101.

Furnell, S., Millet, K. and Papadaki, M. 2019. Fifteen years of phishing: Can technology save us? *Computer Fraud & Security,* 2019(7):11-16.

Granovetter, M. 1978. Threshold models of collective behavior. *American Journal of Sociology,* 83(6):1420-1443.

Granovetter, M. and Soong, R. 1983. Threshold models of diffusion and collective behavior. *Journal of Mathematical Sociology,* 9(3):165-179.

Growney, J. S. 1983. I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior. Modules in undergraduate mathematics and its applications - Tools for teaching. Bedford, MA: COMAP Inc., pp. 108-137.

Hevner, A. and Chatterjee, S. 2010. Design science research in information systems. New York: Springer.

Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B. and Perumal, S. 2020. Systematic literature review of information security compliance behaviour theories. In Proceedings of the *Journal of Physics: Conference Series*: IOP Publishing, pp. 1-14.

Lundgren, B. and Möller, N. 2019. Defining information security. *Science and Engineering Ethics,* 25(2):419-441.

Vaidya, R., Department for digital, culture, media and sport (2019) *Great Britain. Cyber security breaches survey 2019: Statistical release.* London.

Vaishnavi, V. K. and Kuechler, W. 2015. Design science research methods and patterns: Innovating information and communication technology. Boca Raton, NW: CRC Press.

Van der Merwe, A., Gerber, A. and Smuts, H. 2020. Guidelines for conducting design science research in information systems, *Annual conference of the Southern African computer lecturers' association (2019): Communications in Computer and Information Science*: Springer, pp. 163-178.

Chapter 2
-
Literature review

Chapter table of contents

2.1 Chapter introduction 19

2.2 Literature review methodology 19

2.3 Overview of relevant literature 19

2.3.1 Information security 20

2.3.2 Behavioural information security: Models and theories 23

2.3.2.1 Individual behaviour 23

2.3.2.2 Group behaviour 29

2.3.3 Behavioural threshold analysis contextualised for information security 31

2.3.3.1 Definition 31

2.3.3.2 Background – Group behaviour 31

2.3.3.3 Application – Example in cybersecurity 32

2.3.4 Sources for further reading 36

2.4 Chapter summary 42

Chapter references 43

2.1 Chapter introduction

Each of the articles that is included in this thesis has its own literature review section that highlights the literature that was recent and relevant to the specific topic at the time of writing. Therefore, in this chapter, only a cursory look at some of the main recurring and overarching themes of this research in general terms is provided. At the end of the *Overview of relevant literature* section, Table 2.3. is presented that provides additional literature sources on these themes. The chapter is divided into the following sections:

- Literature review methodology;
- Overview of relevant literature; and
- Chapter summary.

2.2 Literature review methodology

The literature review that is presented here is based on the main identifiable themes that are of interest to this research. Under these themes, and also for each of the articles presented later, published works from journal articles, conference proceedings, book chapters, and industry reports (such as published surveys) were consulted. All materials were accessed through institutional subscriptions and repositories, or were freely available online, and are duly referenced and listed under the different reference sections in this thesis.

2.3 Overview of relevant literature

The main themes that are reviewed in this section include information security in general (Section 2.3.1) with specific reference to the human aspect of information security and information security awareness, and behavioural models for individual (Section 2.3.2.1) and group behaviour (Section 2.3.2.2). The chapter concludes with a brief introduction of behavioural threshold analysis in information security (Section 2.3.3). This section is concluded with additional references for further reading on the various themes in Table 2.3.

2.3.1 Information security

Information security (also called information system security, cybersecurity, or computer security) is concerned with the safeguarding of information assets of organisations and individuals, commonly in reference to the protection of information in the digital domain (Aminzade, 2018). Traditionally, the purpose of information security is to address three basic requirements or principles, known as the CIA triad, namely *Confidentiality*, *Integrity*, and *Availability*. Therefore, information, in its protected state, adhere to the principles that are described below based on the definitions of Taherdoost *et al.* (2013), Van Niekerk (2010), and Whitman and Mattord (2011):

Confidentiality – This principle guarantees the privacy or non-disclosure of information. The information is only made available to the intended parties and processes, *i.e.,* those with the required rights that afford them the permission to access the information. Any other entity should be denied access to the information. The principle should be applied to all information whether in transit or at rest. This means that the information in data transmissions should be protected through means such as sufficient encryption techniques. If the communication between authorised parties is intercepted, the interceptor cannot simply view the underlying information. The same is required for data that is stored in databases and systems. Firewalls and other methods for preventing access to systems and the data therein should be employed. Encryption can once more help protect the underlying information if unauthorised access is obtained to the stored data and ensure its *confidentiality*.

Integrity – Information that conforms to this principle is said to be complete and accurate. The information has in no way been altered and is representative of its original state of being, *i.e.*, nothing has been added to the information, nothing has been changed, and nothing has been deleted. Therefore, the data remains a verbatim instance. It should be noted that the factual accuracy or correctness of information is not implied by *integrity*. If the original data was faulty or lacking in any way, *integrity* simply ensures that the information is unchanged by any unauthorised entity. The recipient entity that uses the information can rest assured that the underlying data is true to its origin. Threats to the *integrity* of information can be of an intentional or accidental nature. Accidental threats include data corruption due to errors in data transmissions, hardware failures, or other unintentional causes of data destruction or alteration. Intentional threats refer to parties that gain access to information with the specific goal of altering the information in some way, *e.g.* autonomous malicious software designed to cause data destruction or corruption.

Availability – One of the main reasons for employing information systems in an organisation is to have information which is accessible on demand (in real-time). The caveat being that the information should only be *available* to those who are authorised for such access and to no others. Information should be delivered timeously and conform to the requirements of the expected format, all the while keeping its *integrity*. *Availability* can be interrupted by network outages, if information is required from a remote site, or if required locally, hardware issues or electricity supply interruptions.

If this protected state is realised through adherence to the principles of CIA, the organisation or individual is assured that it/he/she will not likely suffer any information losses (which typically lead to material or financial losses) with respect to external digital exploitation insofar as the security controls which were implemented are able to prevent incidents. However, recent critique (Lundgren & Möller, 2019; Samonas & Coss, 2014) speculates that the CIA model alone is deficient in providing for all the facets of information security, especially the human or organisational aspects thereof. Lundgren and Möller (2019) argue in favour of an appropriate access definition over the existing CIA definition due to it being both too broad and too narrow. The result is that there are human behaviours that can compromise security while still complying tot the CIA definition.

On the organisational front, international standards for the management of information security have been under development for more than two decades by bodies such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the British Standards Institution (BSI). The British standard, BS7799, was introduced in 1995 as a *standard code of practice* for information security management (Li *et al.*, 2000). The original standard was concerned with providing guidance to organisations to institute their own information security system and identified ten controls that are considered critical for providing sufficient information security. The standard has undergone a second revision in 1998, referred to as part two, which provides a *standard specification* that specifies the requirements for an information security management system. This is done through providing the framework, objectives and control requirements to establish such a system. BS7799 has since been replaced by the ISO/IEC 27000-series standards which were introduced in 2005 (Disterer, 2013). The standards that are set out in this series relate to topics such as security policies, incident management, compliance, and physical and environmental security, among others. Standards set the baseline for organisations to be able to firstly assess their current security practices and then address any deficiencies to meet this baseline.

The aforementioned standards, specifically BS7799-1, do make mention of the human factor and related areas for concern in the standard code of practice, but do not provide specifics for approaching the evaluation and management of human behaviour in information security.

Technology is often employed as a panacea to protect the information assets of organisations and to meet the requirements as set out in the standards. Technological solutions, however, for the most part do not provide for the way in which people will interact with information systems (Stewart & Jürjens, 2017; Butavicius *et al.*, 2020). One of the main approaches to attempt to address security behaviour is by employing information security awareness campaigns (Fertig & Schütz, 2020; Scholl, 2018; Kemper, 2019). The goal of such programmes is to educate and instruct the members in an organisation about issues regarding information security and to ultimately influence their behaviour to reflect higher levels of security than before the campaigns were instituted (Tsohou *et al.*, 2015).

Even when awareness campaigns are employed in an organisation, they often do not succeed in changing the security behaviour of the members of the organisation for the better (Bada *et al.*, 2019). Education can address the awareness in terms of the required knowledge that members of an organisation require to be able to be secure, but it does not necessarily address the antecedents to human behaviour that include attitude and intensions. Without addressing these factors, awareness in and of itself is not effective. Another possible reason might be that through training too frequently, awareness campaigns can lose their effectiveness due to the participants becoming security fatigued (Furnell & Thomson, 2009). It becomes a balancing act of not addressing the human factor through education alone. Campaigns need to be sensitive to the very nature of the phenomenon that makes it so challenging to manage in the first place.

To address this shortcoming, *Behavioural information security* has emerged as a field that is dedicated to describing and understanding human behaviour, specifically in relation to information security. The following section is devoted to a cursory discussion of the common models and methods for assessing behaviour in this context.

2.3.2 Behavioural information security: Models and theories

Researchers in the domain of behavioural information security often borrow methods and approaches from the social sciences and psychology to explain behavioural phenomena with respect to information security (Lebek *et al.*, 2013; Khan *et al.*, 2011; Fertig & Schütz, 2020). Some of the more prevalent models and theories are described here under two categories, *i.e.,* individual behaviour, and group behaviour below.

In Table 2.3., literature sources relating to behavioural information security in general are presented that do not specifically relate to evaluating individual and/or group behaviour by employing models similar to those described next, but are still relevant to provide background reading on behavioural information security.

2.3.2.1 Individual behaviour

Four models that are used in literature to evaluate behaviour are presented below. They are *knowledge, attitude, behaviour; protection motivation* theory; *general deterrence theory*; and the *theory of planned behaviour.*

Knowledge, Attitude, Behaviour (KAB) – KAB traditionally referred to the psychological analysis of each of the individual constituents, rather than describing a specific model. The interaction between three of these constructs was only later formalised in the KAB model that is known today, save for an early mention of a weak relationship between knowledge, attitude and behaviour (Bettinghaus, 1986). This incorporated model has the central theory that the accrual of knowledge will eventually alter behaviour through changes in attitude (Schrader & Lawless, 2004), where **K**nowledge can be explained as what an individual knows, **A**ttitude as what the individual feels or thinks, and **B**ehaviour as what the individual does (Kruger & Kearney, 2006).

In the field of behavioural information security, the many studies employed (variants of) the unified KAB model. Indeed, from a recent literature review, Fertig and Schütz (2020) estimate that as many as 40% of information security awareness studies utilise KAB. Some examples of KAB information security research are discussed briefly below.

Moletsane and Tsibolane (2020) identify a strong relationship between knowledge and intention towards behaviour. In the study, they surveyed 397 students at a South African higher education institution about their mobile security behaviour. Their underlying theoretical model draws on the KAB continuum in combination with the theory of planned behaviour. They identify students' knowledge about mobile security risks and the intention to comply with good security practices as the main impetus for actual information security behaviour.

Parsons *et al.* (2014) present a measurement instrument (questionnaire) to evaluate the human aspect in information security, referred to as the *Human aspects of information security questionnaire* (HAIS-Q). In a follow-up study, Parsons *et al.* (2017) validated the instrument. Their KAB model, underpins the theoretical framework for the development of the focus areas of the HAIS-Q. After a series of experiments and applications, the HAIS-Q was found to be sufficiently reliable and valid. The contribution of KAB to the instrument highlighted that the effectiveness of security awareness campaigns in addressing behaviour can be enhanced by not only focussing on imparting facts (knowledge), but by also addressing the understanding of why the facts are important (attitude).

Finally, Kaur and Mustafa (2013) hypothesise that there is a relationship between the general information security notions of CIA and the theoretical framework of KAB. Using a questionnaire to survey 110 employees in the aerospace technologies industry, they suggest that there is a significant relationship of the respondents' attitude and behaviour to their information security awareness. Furthermore, attitude and behaviour were shown to have a significant relationship to confidentiality (CIA). Contrary to the earlier mentioned study of KAB (Moletsane & Tsibolane, 2020), Kaur and Mustafa (2013) did not find knowledge to correlate well with awareness.

Protection motivation theory (PMT) – First described by Rogers (1975), PMT assesses aspects of fear in behaviour determination. The model assesses three threat appraisal processes that take place in the mind of an individual before the ultimate behaviour is formed in response to the threat, *i.e.*, the degree to which the threat is hazardous to you, the perceived effectiveness of a possible reactive response to protect oneself, and the likelihood that the event will actually occur. The contribution of each of these processes to behaviour establishment can then be harnessed to predict eventual behaviour and provides insight into how the behaviour formation process can be influenced to achieve positive behaviour through threats-based appeals. PMT is one of the prevailing theories in behavioural information security research (Kuppusamy *et al.*, 2020) and a few examples from literature are discussed next.

Hassandoust and Techatassanasoontorn (2020) attempt to understand the security awareness and intentions of users by applying PMT. Their goal is to describe a full nomology of PMT through an analysis of security education, training, and awareness programs and the role of fear and maladaptive rewards in these programs. Based on a pilot study of 47 students at a tertiary education institution in New Zealand, the study finds that PMT can help explain the information security protection intentions of individuals. Furthermore, the study contributes through describing an experiment where threat appeals manipulation is not performed in isolation, but in comparison to a control group where threat appeal manipulation was not applied. The role of fear as a motivator in improving information security is recognised.

PMT is applied by Menard *et al.* (2017) to assess human motivation in information security behaviour. They argue that motivation, as a construct, does not form part of the traditional PMT model and, as such, it fails to recognise the contribution of motivation to eventual behaviour. PMT is subsequently compared to and incorporated with self-determination theory (SDT) which focusses on individual motivation. They then investigated the effectiveness of using motivation rather than fear in positively changing information security behaviour by constructing security messages with a positive appeal, rather than using threatening language. Such security messages appeal to the autonomy and competence of the individual as well as how they personally relate to the positive behaviour. The study concludes that by combining SDT with the traditional PMT it bridges the gap in adapting PMT for applications in information security, and that future studies that implement PMT should explicitly provide for the measurable construct of motivation for better results.

Hanus and Wu (2016) investigate the information security behaviour of the home computer user. They apply PMT as the model to evaluate information security awareness and identify how awareness contributes as a precursor to eventual security behaviour. Awareness is sub-divided into two major components that relate to PMT, namely the role of threats, and the role of countermeasures to address said threats. They then map these components to each of the PMT threat appraisal processes and evaluate their contribution to behaviour. The conclusion is drawn that the home user's threat awareness is not enough without the necessary knowledge about the tools (countermeasures) that can be used to combat these threats to convey the necessary self-efficacy for being cyber secure. Finally, the study emphasises that PMT, with security awareness considered as precursors to the constructs thereof, is sufficient for assessing the multidimensional nature of home user awareness.

General Deterrence theory (GDT) – Similar to the aspect of threats in PMT, GDT leverages the notion of the fear of consequences as a deterrent for unwanted behaviour. GDT as a theory originates from the fields of criminology, and specifically penology (Blumstein, 1978), and comprises two constructs that relate to the abovementioned consequences, *i.e.,* the certainty that there will be punishment for prohibited behaviour, and that the punishment is sufficiently severe to prevent an individual from partaking in the behaviour (Park *et al.*, 2012). When applied in information security, studies typically focus on the consequences other than the possible monetary and data losses of the organisation. The focus is on the individual and the role that punishments and other types of deterrents play in ensuring information security compliant behaviour.

Connolly *et al.* (2017) apply the GDT as the central theory in investigating information security behaviour in organisations in Ireland and the United States. They extend GDT by including information security awareness as part of the model. The premise is that awareness (stemming from education and policy) should contribute to more compliant security behaviour. They find that elements of organisational culture can influence information security either positively or negatively. Values such as camaraderie and people-orientation contribute positively, while aspects such as a task-orientated focus and sociability have a negative impact. The structuring of the organisation also influences the levels of information security, *i.e.*, a stronger hierarchy has a negative impact and conversely, flatter structures encourage better security efficacy of the workforce in the organisation.

Theory of planned behaviour (TPB) – TPB was identified as the theoretical grounding and contextualisation for the group behaviour model which was to be investigated during the conceptualisation of this research. The theory is revisited and contextualised in terms of this research in Chapter 3, Article 1. Therefore, the TPB is only discussed here in general terms. The articles in the subsequent chapters address the link of TPB with information security, and specifically information security group behaviour. TPB has its origins in an earlier model, referred to as the theory of reasoned action (TRA). Before a brief discussion of TPB, a summary of TRA is presented where the common constructs between the two models are discussed.

It was proposed by Fishbein (1979) as a model to understand and predict human social behaviour. The model focusses on the properties of behaviour that are innate to the individual that is to perform the behaviour. TRA bases its prediction of individual behaviour on the intention or motivation of a person to perform the behaviour. The stronger the intention is, the more likely that the behaviour will be performed. Intention is said to be influenced by attitude and subjective norms. Attitude, in the context of TRA, refers to whether the intended behaviour is perceived to have a positive or negative effect to the doer, while subjective norms refer to the perceived notion of whether behaviour is acceptable or ethical (Moody *et al.*, 2018). In Figure 2.1, the relationship among these constructs is depicted.

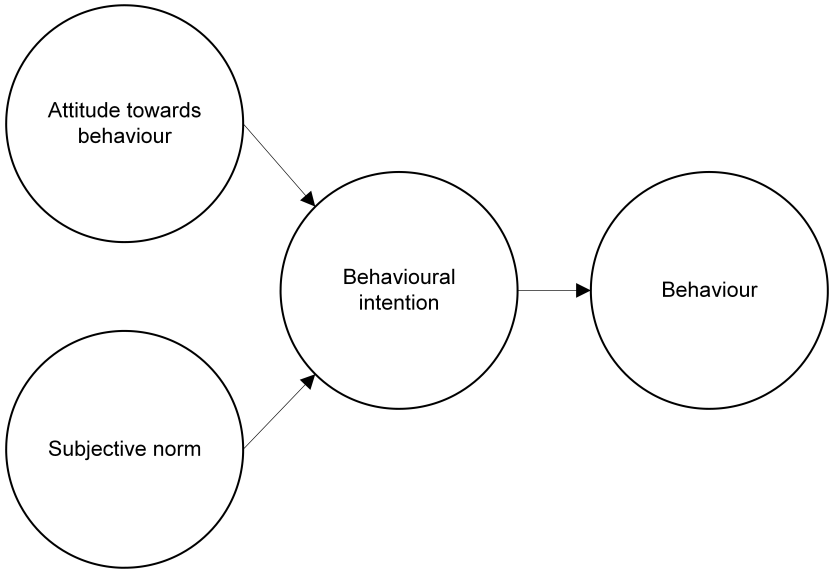


Figure 2.1: Theory of reasoned action (Fishbein, 1979)

TRA was then later extended by Ajzen (1991) as the TPB to include *perceived behavioural control* as a precursor to intention, but which also directly influences the success of the intended behaviour. Perceived behavioural control refers to the instinctive awareness of one's own ability (Godin, 1993). This relates to whether the behaviour in question will be performed successfully, *i.e.,* does the individual see him/herself as having the necessary ability. Furthermore, it also relates to the amount of control one has towards the eventual execution of behaviour. Is the behaviour of one's own volition, or do circumstances dictate the behaviour with little internal control by the individual? The extended model is represented in Figure 2.2. (on the next page) where the interrelatedness and mutual influence of the constructs can be seen.

TPB is a more integrated model of individual behaviour than its predecessor is and has therefore found popularity in information security behaviour studies. In a systematic literature review of the most prevalent behavioural models in information security research, Kuppusamy *et al.* (2020) identified TPB as the dominant theory in security policy compliance studies, followed by PMT. Given this popularity of TPB in information security literature, two recent applications of the TPB are summarised below as an illustration of the way in which the model is typically employed. Additional examples are presented in Table 2.3 for further reading.

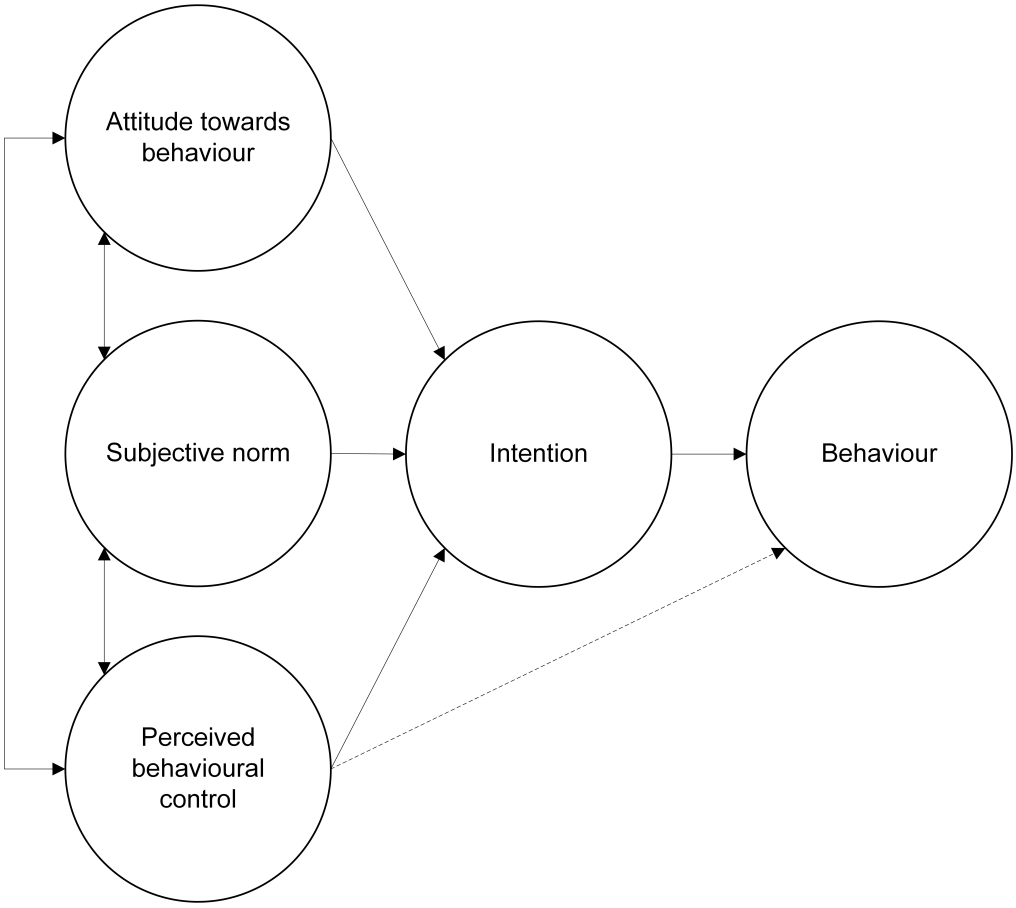


Figure 2.2: The theory of planned behaviour (Ajzen, 1991)

Sommestad *et al.* (2017) investigated the sufficiency assumption of the TPB in relation to information security policy compliance. The sufficiency assumption in this context is that a model does not lack representation for any variable, *i.e.*, the predictive power of the model is sufficient and including external variables do not enhance the model. The study surveys 645 people and evaluates the gain of adding eleven different variables to the TPB. They find that adding a variable for *anticipated regret* contributes to the analytical prowess of the model in predicting behaviour.

Using the constructs of TPB, namely attitude, subjective norms and perceived behavioural control, Vafaei-Zadeh *et al.* (2019) investigated the intention for using anti-malware software of university students. Positive links were found between all three constructs and the intention to protect their computing devices from malware. The attitude that students exhibit towards information security can be improved through promoting awareness of the associated risks. They note that intention without eventual behaviour still leaves gaps in the information security fence that can be used for malicious purposes.

In Table 2.3, additional literature sources are presented on the individual behavioural models presented above as well as other models and theories that are applied to evaluate it.

2.3.2.2 Group behaviour

This sub-section is devoted to two theories that describe group behaviour formation, namely information cascades and collective models of threshold behaviour. These models have not yet been applied in information security and is therefore presented in terms of generic applications.

Information cascades – Bases on the principles of sequential decision-making, information cascades can be used to model collective behaviour. The model was employed in this study and is presented in Chapter 7, Article V. Therefore, the concept of information cascades is presented here briefly.

The decisions of a person are informed by signals, *i.e.*, information, in relation to an expected gain. These signals come in two forms, namely private- and public signals. A private signal is information that is currently known to the person, be it a belief or a fact. When a person makes a decision in isolation, a private signal is what determines the outcome of the decision. When the signal aligns with an associated gain and is powerful enough to overcome the risk associated with potential loss, the decision is made solely on the information conveyed by the signal.

Easley and Kleinberg (2010) note that everyday decisions are rarely made in isolation from the rest of society. Information can be conveyed by signals that are formed extrinsically. Such public signals are based on information that does not come from the individual, but rather from the observation of the decisions that others have made. In a public setting, both private- and public signals will inform the decision. If the signals indicate the same course for the decision, the outcome is obvious but if the two signals provide contrasting information, the strongest signal will inform the decision. It is important to note that both signals are normally imperfect and do not convey infallible information. The signal is always weighed against the probability that the corresponding course for the decision will result in gain, rather than loss.

Due to the sequential nature of decision-making, the public signal becomes stronger with each decision that was made in its favour. The decision-maker is aware of all the public decisions, each one informed by the previous. As a result, the perceived probability that the public signal suggests the “correct” course for the decision becomes higher. The main premise of the model, therefore, is that the public signal will usually prove stronger and influence the decision even when the private signal initially informed a contrasting course.

Information cascades rely on four prerequisites for the model to be applied to a situation (Easley & Kleinberg, 2010):

1. There is a (binary/contrasting) decision to be made;
2. Each person has a private signal that originally informs their initial proclivity;
3. The decisions that were made by others can be observed and the decisions happen sequentially; and
4. The private information of others is not known to the individual.

However, inferences can be made about another's private information based on their publicly noticeable decision from number 3 above. This cascade of information will ultimately lead to the decision-making processes of the individuals that comprise a group to converge and lead to a collective behaviour outcome.

Collective models of threshold behaviour – The way group behaviour is formed from the actions of the individuals that comprise the group may be understood by employing a theory on the formation of group behaviour. Formally, the model is termed threshold models of collective behaviour. This theory was developed by Granovetter (1978) in the field of sociology. The premise of the theory is that the behaviour of a person in a group setting is guided by an inborn threshold for participating in a specific behaviour. Such a threshold refers to the proportion of other group members that must exhibit, or be believed to exhibit, the behaviour, before the individual is stimulated to also perform the behaviour.

When someone is confronted with two discrete behaviours with two distinct outcomes, usually participation or abstention, (s)he will unconsciously compare his/her own threshold level with the number of others they perceive as already performing the behaviour. If the number of others that behave in a certain way exceed their threshold for participation, (s)he will be swayed to join in the behaviour. This process continues with each subsequent group member that also must make the binary, contrasting decision of partaking or not and participation will grow until the group (or at least a significant percentage) performs the behaviour. This growth and the eventual group behaviour can be modelled by applying behavioural threshold analysis, based on the description of Growney (1983). This is approach forms the basis of investigation of this research and is therefore addressed in more detail in the following section.

Additional sources of other approaches to assess group behaviour in general and relation to information security is presented in Table 2.3.

2.3.3 Behavioural threshold analysis contextualised for information security

Preamble – This subsection, in which behavioural threshold analysis is presented as an approach to evaluate information security group behaviour, is based on an excerpt and adaptation of a contribution to the *Encyclopedia of Cryptography, Security and Privacy*. This contribution, with the title *Group behaviour in cybersecurity*[1] was written in response to an invitation from the editors to contribute to the forthcoming fifth edition of the encyclopaedia. It is currently in press after being accepted for publication. The full article as it was submitted can be found in Appendix A.

The concepts that are presented here and how they are applied to information security behaviour will be explained in more detail in the subsequent chapters and articles. This includes the methodology for applying behavioural threshold analysis, the measurement instrument, data collection methods, the cumulative threshold tables and graphs, *etc*.

2.3.3.1 Definition

Group behaviour in cybersecurity refers to the interaction between two or more individuals, where they are exposed to the cybersecurity behaviour and actions of others. This mutual interaction influences the behaviour of the members of the group, and ultimately the collective behaviour of the group in terms of cybersecurity.

2.3.3.2 Background – Group behaviour

The human aspect of cybersecurity is an ever-present occurrence that needs to be factored into cybersecurity policy and management strategies. The way an individual behaves in terms of cybersecurity, is based on determinants, such as his/her motivations, convictions, and intentions. These determinants are the result of influences that affect the individual and originate from the environments in which (s)he functions. Behaviour is, therefore, a product of the context in which it occurs. Typically, a person does not function solely in isolation with specific regards to their role within an organization. Much of the everyday existence is in the company of others, *i.e.*, he/she is part of a group. Given enough impetus between group members, the eventuality is that most members of the group will start to behave in a similar, if not the same, manner.

[1] Snyman, D. P., & Kruger, H. A. 2020. Group behaviour in Cybersecurity. To appear in *Encyclopedia of Cryptography, Security and Privacy* (5th ed.): Springer International Publishing.

This convergence of behaviour is often referred to as the lemming effect or herding behaviour which means that a person will follow the behaviour of the group without much forethought, even against his/her own better judgment. This phenomenon of group behaviour has been recognised as a prevailing human factor in cybersecurity which can be modelled by applying behavioural threshold analysis, based on the description of Growney (1983).

2.3.3.3 Application – Example in cybersecurity

An illustrative example of the application of behavioural threshold analysis, as applied in cybersecurity, is presented here. This example is intended to be instructive of the underlying methodology of analysing cybersecurity group behaviour (Article IV, Chapter 6) and is presented here in a hypothetical setting.

Scenario – An organisation has identified that password sharing among employees has become a noticeable problem that has to be addressed. To quantify the extent of password sharing and the future extent thereof if no intervention is made, behavioural threshold analysis is employed.

Behavioural threshold analysis – Behavioural threshold analysis aggregates the inherent thresholds that group-members have towards participating in cybersecurity group behaviour. The thresholds (expressed as a percentage) for the individuals making up the group are determined by means of a short measurement instrument (questionnaire) on password sharing (or other relevant cybersecurity behaviour) that is distributed to all the group members. The measurement instrument is presented below in Table 2.1. Note the layout of the question-and-answer grid; it is important to elicit effective and truthful thresholds.

Table 2.1: Example measurement instrument

Percentage of colleagues who share their passwords	How inclined would you be to also share your organisation password, given the percentage of colleagues who share their passwords?			
	Never	Somewhat inclined	Strongly inclined	Always
0—10%	1	2	3	4
11—20%	1	2	3	4
21—30%	1	2	3	4
31—40%	1	2	3	4
41—50%	1	2	3	4
51—60%	1	2	3	4
61—70%	1	2	3	4
71—80%	1	2	3	4
81—90%	1	2	3	4
91—100%	1	2	3	4

Based on the responses that were received on the questionnaire, the resulting individual behavioural thresholds are aggregated by creating a cumulative threshold table. An illustrative example of a cumulative threshold table is presented in Table 2.2.

Table 2.2: Cumulative threshold table

Threshold (%)	Individuals with given threshold (%)	Individuals with a threshold not more than the given threshold (%)
0	0	0
10	4	4
20	10	14
30	15	29
40	20	49
50	12	61
60	10	71
70	15	86
80	4	90
90	0	90
100	0	90
Individuals with no threshold (*i.e.*, will never participate) (%)	**10**	

Note the number of respondents with no reported threshold for participation. This happens when a respondent selects “Never” for all threshold intervals as per the measurement instrument (Table 2.1), *i.e.,* no matter how many others perform a behaviour, (s)he will not be persuaded to join in. Respondents with no threshold are excluded from further calculations.

The cumulative thresholds from Table 2.1 are then plotted in a behavioural threshold graph in contrast to an equilibrium line (a uniform distribution of cumulative thresholds such that $x = y$) as presented in Figure 2.3.

Results – The interpretation of a behavioural threshold graph is dependent on the intersection(s) (P_A and P_B) of the threshold graph with the equilibrium line. Each intersection of the two lines represents a possible equilibrium in which the group behaviour stabilises, *i.e.*, the number of participants in the behaviour does not continue to grow or decline.

For an intersection to be an actual equilibrium, the line segments to the left (L_1) and right (L_2) of said intersection must have a gradient

$$m_{L_1}, m_{L_2} = \frac{\Delta y}{\Delta x} < 1. \tag{2.1}$$

This implies that only intersections where the threshold graph intersects the equilibrium line from above will satisfy the requirement as an intersection from below will always be

$$m > 1 \ for \ L_1, \tag{2.2}$$

e.g. Intersection P_A (as shown in Figure 2.3) does not satisfy the requirements for equilibrium. However, the behaviour of password sharing among employees reaches equilibrium at P_B because

$$m_{L_1}, m_{L_2} = 0 < 1, \tag{2.3}$$

and the participation rate is said to be stable against both increase and decrease.

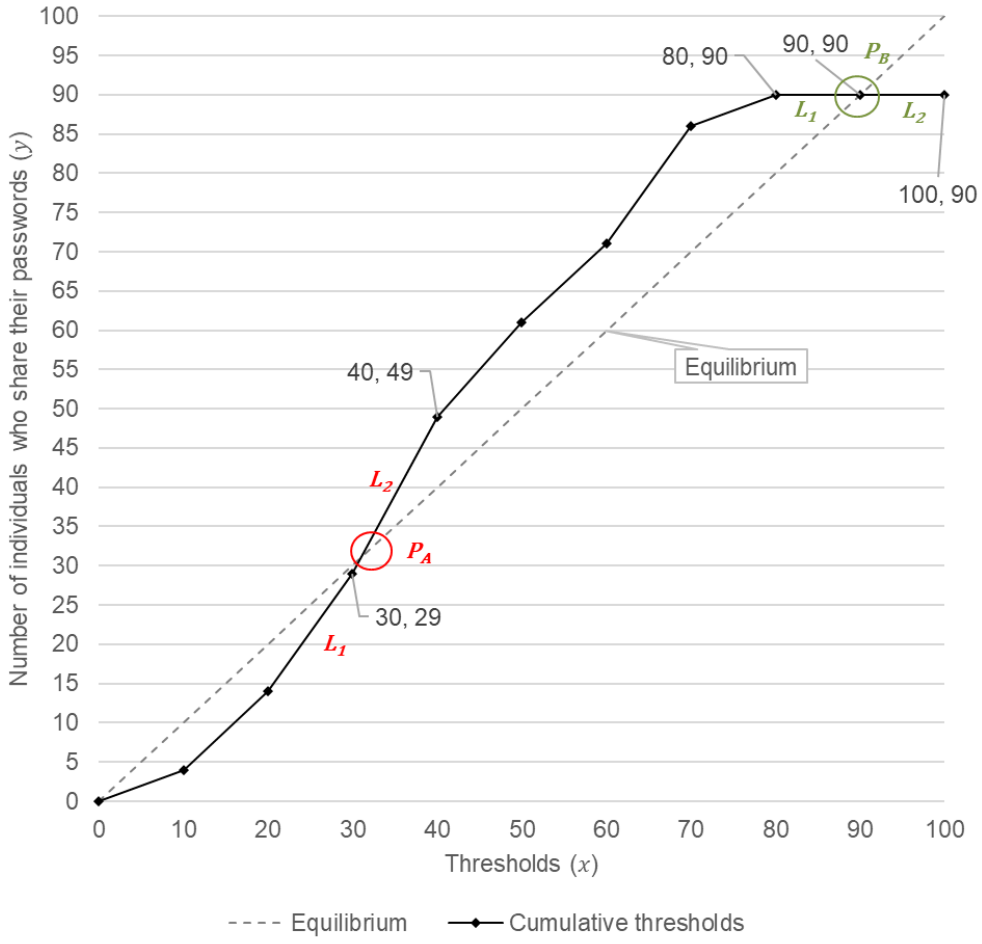


Figure 2.3: Cumulative threshold graph

The relevance of the cumulative thresholds reaching a behavioural equilibrium to the cybersecurity behaviour of password sharing is that the equilibrium at point $P_B(90,90)$ indicates that the participation rate of password sharing is likely to increase until 90% of the employees are sharing their passwords. The group behaviour will become stagnant at this ultimate participation rate unless an external stimulus (*i.e.*, a cybersecurity awareness campaign) is utilised to change the behaviour.

Discussion – A discussion on using behavioural threshold analysis to analyse group behaviour in cybersecurity is presented here in terms of the advantages it presents and some challenges in its application.

Advantages – Behavioural threshold analysis considers the behaviour of people in groups and not just the behaviour of individuals in seclusion like most other behavioural theories; it may be employed as a preventative measure in cybersecurity management, *i.e.*, current behavioural trends in troublesome security behaviour may be identified, and forecasts may be made on future behaviour to predict participation growth in the absence of targeted interventions, cost and time savings through tailored security awareness campaigns with a specific focus on behaviours which have been identified as imperative through behavioural threshold analysis, and the effectiveness of interventions may be gauged by means of the relative ease of repeatability of behavioural threshold analysis as both a pre and post intervention assessment of group cybersecurity behaviour.

Challenges – Behavioural threshold analysis requires that the members of the group have a working knowledge of the behaviour of other group members and works best if performed in a relatively small group or organisational division. In addition, the results cannot be extrapolated to a greater population and is only relevant to the surveyed group. Furthermore, the approach is sensitive to external contextual factors in a group setting which may influence its results.

2.3.4 Sources for further reading

As mentioned in Section 2.1, as part of each of the research articles in this thesis, a literature review section is included with references specific to the article. Therefore, only a brief overview of the main themes was provided. For further reading on these topics the reader is referred to Table 2.3 where additional sources, that were not included in the discussion above, are presented for further reading.

Table 2.3: Alphabetical list of additional literature sources

Additional source related to information security in general		
Author(s)	**Title**	**Theme**
Al-Omari *et al.* (2012)	*Information security policy compliance: The role of information security awareness*	An investigation into the role that security awareness plays in the adoption and compliance of information security policies.
Alshaikh *et al.* (2018)	*An exploratory study of current information security training and awareness practices in organizations*	An overview of industry best practices reveals shortcomings in the current approaches in security awareness training, namely that training is mostly conceptual and not proven, and also it is not specific enough for diverse contexts.
Bada *et al.* (2019)	*Cyber security awareness campaigns: Why do they fail to change behaviour?*	This paper identifies understanding and motivation as psychological antecedents that explain why cybersecurity awareness campaigns often fail to address eventual behaviour.
Berger (2011)	*CSI/FBI Computer crime and security survey. 2011-2012*	A survey of computer crime and related security that was conducted in the United States of America, which focusses on security, breaches and other exploits which resulted in financial and other losses.
Bulgurcu *et al.* (2010)	*Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness*	Rationality-based factors are contextualised with the theory of planned behaviour as an influencing factor on an employee's attitude to comply with information security policies.
Chesney and Citron (2018)	*Deep Fakes: A looming challenge for privacy, democracy, and national security*	An overview of the challenges that so-called deep fakes pose to information security.
Furnell and Esmael (2017)	*Evaluating the effect of guidance and feedback upon password compliance*	An investigation into the types of feedback that is provided to users of commonly used web services when choosing the associated passwords. Guidance should be provided on how users are to comply with password practices such as minimum requirements for password constituents.
Furnell *et al.* (2013)	*Plugging the cyber-security skills gap*	This study investigates the lack of qualified and skilled workers in the field of information security. People from a wide range of different backgrounds should be encouraged to pursue cybersecurity-related careers due to the variety of skills they bring to the table and then trained for the specifics of the profession.
Gardner and Thomas (2014)	*Building an information security awareness program: Defending against social engineering and technical threats*	A book on the development of effective information security awareness programs. The chapter on social engineering and related security risks was of interest to this study.

Table 2.3: Continued

Author(s)	Title	Theme
Hekkala *et al.* (2012)	*Information security challenges of social media for companies*	Social media poses significant risks to organisations in terms of privacy and security due to lack of awareness, differentiating between personal and business-related social media roles, and unregulated communication between employees and customers.
Kruger and Kearney (2006)	*A prototype for assessing information security awareness*	A prototype model to assess security awareness in organisations is presented and validated through application in an international mining company.
Miller and Stuart Wells (2007)	*Balancing security and privacy in the digital workplace*	A trade-off exists between technical security controls and the degree to which they violate the privacy of workers. This paper discusses the legal and ethical issues that need to be considered. The findings indicate that organisations should be responsive and find a balance between privacy and security.
IBM Security (2018)	*IBM X-Force Threat Intelligence Index 2018: Notable security events of 2017, and a look ahead*	A summary of information security incidents and future perspectives for new challenges.
Taherdoost *et al.* (2013)	*Definitions and criteria of CIA security triangle in electronic voting system*	Definitions of Confidentiality, Integrity, and Availability in the context of electronic voting.
Additional sources related to behavioural information security		
Author(s)	**Title**	**Theme**
Ashenden (2008)	*Information security management: A human challenge?*	Information security management is purported to be largely a human-based issue. The paper evaluates the challenges that the human factor poses to businesses and organisations.
Barth and de Jong (2017)	*The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review*	A literature review on the privacy paradox based on different categories of the paradox, its influence on decision-making, and solutions for the paradox.
Barth *et al.* (2019)	*Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources*	Real-world behaviour of mobile phone users is observed to gauge the influence of technical knowledge, privacy awareness, and financial resources on the privacy paradox.
Boss *et al.* (2009)	*If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security*	The perception of the employee that he/she is being watched by management enhances the feeling of security policy compliance being mandatory, thereby reinforcing it in eventual security behaviour.
Brown (2001)	*Studying the Internet experience*	A qualitative study of internet use uncovers a privacy paradox between users' concerns in terms of privacy and online shopping behaviour.

Table 2.3: Continued.

Author(s)	Title	Theme
Crossler *et al.* (2013)	*Future directions for behavioral information security research*	Behavioural information security is identified as an emerging field of study. The paper gives direction for new avenues of exploration.
Calic *et al.* (2016)	*Naïve and accidental behaviours that compromise information security: What the experts think*	Fifteen information security experts were asked to deliberate on the most prevalent naïve and accidental information security behaviours. These behaviours were identified through qualitative, focus group data collection methods. The identified behaviours were used to validate a human aspects of information security questionnaire.
Egelman and Peer (2015)	*Scaling the security wall: Developing a security behavior intentions scale (SeBIS)*	Developing an instrument for evaluating and predicting information security behaviour. The instrument consists of sixteen questions, rated on a 5-point Likert scale. These questions map to four information security focus areas, namely device securement, password choices, proactive security, and software updating.
Egelman *et al.* (2016)	*Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS)*	An experimental application and validation of the security behaviour intention scale as a measurement instrument for evaluating the self-reported intent of an individual to employ good security practices. The scale was found to be predictive of specific information security behaviours.
Fazio (1990)	*Multiple processes by which attitudes guide behavior: The MODE model as an integrative framework*	The MODE model (motivation and opportunities as determinants) indicates that if circumstances are conducive, attitude and intention become an antecedent to behaviour.
Herath and Rao (2009a)	*Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness*	A theoretical model to evaluate information security behaviour by testing the relationship between social influence, the role of penalties as a deterrent, and behavioural intention.
Kearney and Kruger (2016)	*Theorising on risk homeostasis in the context of information security behaviour*	Risk homeostasis is contextualised as a behavioural model for evaluating information security behaviour.
Kokolakis (2017)	*Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*	A literature review on studies that investigate the privacy paradox.
Kokolakis (2017)	*Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*	A literature review on studies that investigate the privacy paradox.
Kroenung and Eckhardt (2015)	*The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship*	Based on an extensive literature review, factors in the attitude-behaviour relationship with respect to existing models in information systems adoption are identified and conceptualised into a new model.
Lebek *et al.* (2013)	*Employees' information security awareness and behavior: A literature review*	A literature study on the underlying theories, models, and approaches that are commonly used to contextualise and evaluate information security behaviour and awareness.
Nguyen and Kim (2017)	*Enforcing information security protection: risk propensity and self-efficacy perspectives*	An investigation into the factors that influence self-efficacy as it relates to information security behaviour. The study is based on self-efficacy theory.

Table 2.3: Continued

Author(s)	Title	Theme
Ooi *et al.* (2018)	*Unfolding the privacy paradox among mobile social commerce users: A multi-mediation approach*	The privacy paradox is investigated, and a model is presented. The model provides predictive capabilities towards user intention, but not the ultimate privacy behaviour.
Additional sources related to models for assessing individual behaviour in information security		
Author(s)	**Title**	**Theme**
Apau and Koranteng (2019)	*Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior*	An application of the theory of planned behaviour that is used to contextualise the intention to purchase e-commerce technologies. The study finds that attitude, perceived behavioural control and subjective norms can be precursors to the underlying intentions, influenced by the perceptions of related cybercrime. A survey was conducted with 476 respondents and the resulting responses were analysed by means of partial least square structural equation modelling.
Ashenden (2018)	*In their own words: Employee attitudes towards information security*	A personal construct theory analysis by means of repertory grid interviews (as a means to limit social desirability) of the attitudes that employees exhibit towards information security.
Bishop *et al.* (2020)	*Examining human individual differences in cyber security and possible implications for human-machine interface design*	In this study, a combination of protection motivation theory and theory of planned behaviour served as the basis for a measurement instrument that was completed by 71 individuals. Individual differences such as propensity to risk-taking, personality, and decision-making style are identified as influences on cybersecurity behaviour. These findings inform new human-oriented approaches to design human-machine interactions.
Brown (2001)	*Studying the Internet experience*	A qualitative study of internet use uncovers a privacy paradox between users' concerns in terms of privacy and online shopping behaviour.
Cuganesan *et al.* (2018)	*How senior management and workplace norms influence information security attitudes and self-efficacy*	Workplace dynamics have an effect on employee attitudes and self-efficacy in relation to information security. The role of management and norms and how they influence employee security behaviour is investigated in a law enforcement organisation. The study draws on the theory of planned behaviour and general deterrence theory.
D'arcy and Herath (2011)	*A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings*	This study reviews deterrence theory in information security research. Literature has diverging views on the theory and its application. They identify factors that moderate behaviour and thus influences results as well as methodological issues that should be addressed in deterrence studies.

Table 2.3: Continued

Author(s)	Title	Theme
Fazio (1990)	*Multiple processes by which attitudes guide behavior: The MODE model as an integrative framework*	The MODE model (motivation and opportunities as determinants) indicates that if circumstances are conducive, attitude and intention become an antecedent to behaviour.
Herath and Rao (2009b)	*Protection motivation and deterrence: a framework for security policy compliance in organisations*	An integrated protection motivation and deterrence model is developed and validated. The resulting model is a combination of general deterrence theory and protection motivation theory.
Hooper and Blunt (2020)	*Factors influencing the information security behaviour of IT employees*	A model, combining protection motivation theory, theory of planned behaviour, and theory of reasoned action, was employed to evaluate the information security behaviour of 70 IT employees through an online survey. Their determinants of behavioural intention was different form non-IT employees and included the perception of the impact of their behaviour, and self-efficacy.
Ifinedo (2012)	*Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory*	Combining protection motivation theory and the theory of planned behaviour into a conceptual framework. The union of the two methods allows for different perspectives from both the theoretical models on security policy compliance in organisations.
Jouda *et al.* (2020)	*Mobile banking adoption: Decomposed theory of planned behavior with perceived trust*	The theory of planned behaviour is deconstructed and applied to the adoption and perceived trust in mobile banking in Palestine. Based on a survey with 682 participants, the study finds that the promise of high security in this context helps retain existing customers and grow the customer base. In combination with perceived trust as a new construct, attitude and perceived behavioural control indicated a positive contribution to the adoption of mobile banking.
Kaur and Mustafa (2013)	*Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME*	The knowledge, attitude, behaviour (KAB) model is applied to information security awareness.
Khan and AlShare (2019)	*Violators versus non-violators of information security measures in organizations — A study of distinguishing factors*	Factors that influence individuals to violate, or not violate, information security measures in an organisation are investigated in this research. The authors draw on various behavioural information security theories, *i.e.*, theory of planned behaviour, theory of reasoned action, protection motivation theory, and social cognitive theory. A survey of 195 respondents was conducted in a university setting. The behavioural differences between violators and non-violators could be illuminated by many of the constructs of the aforementioned theories.

Table 2.3: Continued

Author(s)	Title	Theme
Khan *et al.* (2011)	*Effectiveness of information security awareness methods based on psychological theories*	Linking information security awareness with behavioural information security approaches in the next section, this paper evaluates how effective the tools for addressing awareness are. The evaluation is based on psychological models. This is in contrast to most studies that only discuss novel techniques for addressing awareness in the first instance.
Kroenung and Eckhardt (2015)	*The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship*	Based on an extensive literature review, factors in the attitude-behaviour relationship with respect to information systems adoption are identified and conceptualised into a new model.
Mahfuth (2020)	*An investigation on the relationship between security knowledge constructs and employee behaviour in organisations*	A doctoral thesis in which the author investigated the role of knowledge in information security behaviour. The study was based on the knowledge, attitude, behaviour model. The study found that security-knowledge constructs have an indirect positive effect on behaviour through attitudes.
Medeiros *et al.* (2020)	*Assessing the determinants of millennials' online protective behavior: How their protection motivation translates into actual use behavior*	Combining protection motivation theory, and reasoned action approach, factors that influence the online security behaviours of Millennials, was investigated in this study. A comparison was made between the users' intention towards secure behaviour and the actual behaviour they exhibit. A disconnect was found between intention and behaviour of 236 respondents.
Ooi *et al.* (2018)	*Unfolding the privacy paradox among mobile social commerce users: A multi-mediation approach*	The privacy paradox is investigated and presented as a predictive model. The model provides predictive capabilities towards user intention, but not the ultimate privacy behaviour.
Sommestad and Hallberg (2013)	*A review of the theory of planned behaviour in the context of information security policy compliance*	A literature study and analysis of the theory of planned behaviour and its applications in information security policy compliance.
Van Bavel *et al.* (2019)	*Using protection motivation theory in the design of nudges to improve online security behavior*	A large-scale study including 2024 respondents was conducted across five European countries to evaluate how effective short messages are in helping individuals minimize their online security exposure. Based on protection motivation theory, the study compared coping messages with threat appeals. It was found that coping messages outperform fear appeals in helping promote secure behaviour.
Additional sources related to models for assessing group behaviour		
Author(s)	**Title**	**Theme**
Banerjee (1992)	*A simple model of herd behavior*	Sequential decision-making is formalised as a model to explain the herding phenomenon in human group behaviour.
Belk (1975)	*Situational variables and consumer behaviour*	Contextual factors in human behaviour
Bikhchandani *et al.* (1992)	*A theory of fads, fashion, custom, and cultural change as informational cascades*	Information cascades are presented as a model to describe the adoption of group behaviour by an individual.

Table 2.3: Continued

Author(s)	Title	Theme
Dang-Pham *et al.* (2014)	*Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach*	A structured literature review reveals that the current trend in information security behaviour focusses on individual cognition. The paper suggests that it is not enough to glean a holistic view of insider misbehaviour and that the influence of group dynamics can be observed through a social network approach.
Dang-Pham *et al.* (2017)	*Applications of social network analysis in behavioural information security research: Concepts and empirical analysis*	The social network analysis approach offers analytical capabilities to explore the interactions and relationships between members of a group. A case study of a Vietnamese organisation where social network analysis methods were used showed an improvement in behavioural information security.
De Klerk (2013)	*Initiation, hazing or orientation? A case study at a South African university*	Social hierarchy (in a university residence context), and the interaction between those higher and lower in the hierarchy, leads to behaviours which are contrary to rules and regulations, and/or better judgement.
Easley and Kleinberg (2010)	*Networks, crowds, and markets: Reasoning about a highly connected world*	A book on network approaches to analyse connectedness in the modern society. Of particular interest is the notion of diffusion of behavioural trends through cascading behaviour in a social group or network.
Helfinstein *et al.* (2015)	*If all your friends jumped off a bridge: The effect of others' actions on engagement in and recommendation of risky behaviors*	The perception and overestimation of the behaviour of others will influence the individual to engage in risky behaviour that he/she would normally avoid.
Johnson *et al.* (2005)	*Predictors of alcohol consumption in university residences*	Social and group dynamics, such as peer pressure, are shown to be predictors of alcohol consumption in a university residence setting.
Johnston *et al.* (2019)	*It takes a village: Understanding the collective security efficacy of employee groups*	This study explores how groups of employees formulate a collective efficacy in dealing with information security threats and incidents. The research is based on a case study at a large healthcare research organisation.

2.4 Chapter summary

In this chapter, an overview of the recurring themes from literature with specific reference to general information security, behavioural information security, and behavioural threshold analysis was provided. Additional references to supplement the discussion in the various sub-sections were provided in a tabular format.

Chapter references

Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes,* 50(2):179-211.

Al-Omari, A., El-Gayar, O. and Deokar, A. 2012. Information security policy compliance: The role of information security awareness. In Proceedings of the *18th Americas Conference on Information Systems (Paper 16)*, Seattle, WA, pp. 1-10.

Alshaikh, M., Maynard, S. B., Ahmad, A. and Chang, S. 2018. An exploratory study of current information security training and awareness practices in organizations. In Proceedings of the *51st Hawaii International Conference on System Sciences*: IEEE, pp. 5085-5094.

Aminzade, M. 2018. Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security,* 2018(5):9-11.

Apau, R. and Koranteng, F. N. 2019. Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. *International Journal of Cyber Criminology,* 13(2):228-254.

Ashenden, D. 2008. Information security management: A human challenge? *Information Security Technical Report,* 13(4):195-201.

Ashenden, D. 2018. In their own words: Employee attitudes towards information security. *Information & Computer Security,* 26(3):327-337.

Bada, M., Sasse, A. M. and Nurse, J. R. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour?, In Proceedings of the *1st International Conference on Cyber Security for Sustainable Society*, pp. 118–131.

Banerjee, A. V. 1992. A simple model of herd behavior. *The Quarterly Journal of Economics,* 107(3):797-817.

Barth, S. and de Jong, M. D. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics,* 34(7):1038-1058.

Barth, S., De Jong, M. D., Junger, M., Hartel, P. H. and Roppelt, J. C. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics,* 41(2019):55-69.

Belk, R. W. 1975. Situational variables and consumer behavior. *Journal of Consumer research,* 2(3):157-164.

Berger, U. 2011. CSI/FBI Computer crime and security survey: 2011-2012. Computer Security Institute.

Bettinghaus, E. P. 1986. Health promotion and the knowledge-attitude-behavior continuum. *Preventive Medicine,* 15(5):475-491.

Bikhchandani, S., Hirshleifer, D. and Welch, I. 1992. A theory of fads, fashion, custom, and cultural change as informational cascades. *Journal of Political Economy,* 100(5):992-1026.

Bishop, L. M., Morgan, P. L., Asquith, P. M., Raywood-Burke, G., Wedgbury, A. and Jones, K. 2020. Examining human individual differences in cyber security and possible implications for human-machine interface design, in Moallem, A. ed. *HCI for Cybersecurity, Privacy and Trust*. Cham, Switzerland: Springer International Publishing, pp. 51-66.

Blumstein, A. 1978. Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates. Washington, DC, USA: National Academy Press.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems,* 18(2):151-164.

Brown, B. 2001. Studying the Internet experience. *Technical report (HPL-2001-49).* Bristol: HP Laboratories.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly,* 34(3):523-548.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M. and Calic, D. 2020. When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. *Computers & Security,* 98(2020):1-11.

Calic, D., Pattinson, M., K., P., Butavicius, M. and McCormac, A. 2016. Naïve and accidental behaviours that compromise information security: What the experts think. In Proceedings of the *Tenth International Symposium on Human Aspects of Information Security & Assurance*, Frankfurt, Germany: Plymouth University, pp. 12-21.

Chesney, R. and Citron, D. K. 2018. Deep Fakes: A looming challenge for privacy, democracy, and national security. *107 California Law Review; University of Texas Law, Public Law Research Paper No. 692; University of Maryland Legal Studies Research Paper No. 2018-21.*

Connolly, A. Y., Lang, M., Gathegi, J. and Tygar, D. J. 2017. Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security,* 25(2):118-136.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. and Baskerville, R. 2013. Future directions for behavioral information security research. *Computers & Security,* 32(2013):90-101.

Cuganesan, S., Steele, C. and Hart, A. 2018. How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology,* 37(1):50-65.

D'arcy, J. and Herath, T. 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems,* 20(6):643-658.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. 2014. Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach. In Proceedings of the *25th Australasian Conference on Information Systems (ACIS)*, Auckland, New Zealand.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. 2017. Applications of social network analysis in behavioural information security research: Concepts and empirical analysis. *Computers & Security,* 68(2017):1-15.

De Klerk, V. 2013. Initiation, hazing or orientation? A case study at a South African university. *International Research in Education,* 1(1):86-100.

Disterer, G. 2013. ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security,* 2013(4):92-100.

Easley, D. and Kleinberg, J. 2010. Networks, crowds, and markets: Reasoning about a highly connected world. New York, NY, USA: Cambridge University Press.

Egelman, S., Harbach, M. and Peer, E. 2016. Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS). In Proceedings of the *2016 CHI Conference on Human Factors in Computing Systems*: ACM, pp. 5257-5261.

Egelman, S. and Peer, E. 2015. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In Proceedings of the *33rd Annual ACM Conference on Human Factors in Computing Systems*: ACM, pp. 2873-2882.

Fazio, R. H. 1990. Multiple processes by which attitudes guide behavior: The MODE model as an integrative framework. *Advances in Experimental Social Psychology,* 23(1):75-109.

Fertig, T. and Schütz, A. 2020. About the measuring of information security awareness: A systematic literature review. In Proceedings of the *53rd Hawaii International Conference on System Sciences*, Wailea-Makena, Hawaii, USA: IEEE, pp. 6518-6527.

Fishbein, M. 1979. A theory of reasoned action: some applications and implications. In Proceedings of the *Nebraska Symposium on Motivation*, pp. 65–116.

Furnell, S. and Esmael, R. 2017. Evaluating the effect of guidance and feedback upon password compliance. *Computer Fraud & Security,* 2017(1):5-10.

Furnell, S., Fischer, P. and Finch, A. 2013. Plugging the cyber-security skills gap. *Computer Fraud & Security,* 2013(7):5-10.

Furnell, S. and Thomson, K.-L. 2009. Recognising and addressing ‘security fatigue’. *Computer Fraud & Security,* 2009(11):7-11.

Gardner, B. and Thomas, V. 2014. Building an information security awareness program: Defending against social engineering and technical threats. Waltham, MA, USA: Elsevier.

Godin, G. 1993. The theories of reasoned action and planned behavior: Overview of findings, emerging research problems and usefulness for exercise promotion. *Journal of Applied Sport Psychology,* 5(2):141-157.

Granovetter, M. 1978. Threshold models of collective behavior. *American Journal of Sociology,* 83(6):1420-1443.

Growney, J. S. 1983. I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior. Modules in undergraduate mathematics and its applications - Tools for teaching. Bedford, MA: COMAP Inc., pp. 108-137.

Hanus, B. and Wu, Y. A. 2016. Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management,* 33(1):2-16.

Hassandoust, F. and Techatassanasoontorn, A. A. 2020. Understanding users' information security awareness and intentions: A full nomology of protection motivation theory, *Cyber Influence and Cognitive Threats*: Elsevier, pp. 129-143.

Hekkala, R., Väyrynen, K. and Wiander, T. 2012. Information security challenges of social media for companies. In Proceedings of the *20th European Conference on Information Systems*, pp. 1-12.

Helfinstein, S. M., Mumford, J. A. and Poldrack, R. A. 2015. If all your friends jumped off a bridge: The effect of others' actions on engagement in and recommendation of risky behaviors. *Journal of Experimental Psychology: General,* 144(1):12-17.

Herath, T. and Rao, H. R. 2009a. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems,* 47(2):154-165.

Herath, T. and Rao, H. R. 2009b. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,* 18(2):106-125.

Hooper, V. and Blunt, C. 2020. Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology,* 39(8):862-874.

IBM Security 2018. IBM X-Force threat intelligence index 2018: Notable security events of 2017, and a look ahead. USA: IBM Corporation.

Ifinedo, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security,* 31(1):83-95.

Johnson, A. M., Rodger, S. C., Harris, J. A., Edmunds, L. A. and Wakabayashi, P. 2005. Predictors of alcohol consumption in university residences. *Journal of Alcohol and Drug Education,* 49(3):9-17.

Johnston, A. C., Di Gangi, P. M., Howard, J. and Worrell, J. 2019. It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems,* 20(3):186-212.

Jouda, H., Abu Jarad, A., Obaid, T., Abu Mdallalah, S. and Awaja, A. 2020. Mobile banking adoption: Decomposed theory of planned behavior with perceived trust. In Proceedings of the *1st International Conference on Information Technology and Business*, Virtual conference, pp. 1-10.

Kaur, J. and Mustafa, N. 2013. Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In Proceedings of the *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, Kuala Lumpur, Malaysia: IEEE, pp. 286-290.

Kearney, W. D. and Kruger, H. A. 2016. Theorising on risk homeostasis in the context of information security behaviour. *Information & Computer Security,* 24(5):496-513.

Kemper, G. 2019. Improving employees' cyber security awareness. *Computer Fraud & Security,* 2019(8):11-14.

Khan, B., Alghathbar, K. S., Nabi, S. I. and Khan, M. K. 2011. Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management,* 5(26):10862-10868.

Khan, H. U. and AlShare, K. A. 2019. Violators versus non-violators of information security measures in organizations — A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce,* 29(1):4-23.

Kokolakis, S. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security,* 64(2017):122-134.

Kroenung, J. and Eckhardt, A. 2015. The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship. *Information & Management,* 52(6):611-627.

Kruger, H. A. and Kearney, W. D. 2006. A prototype for assessing information security awareness. *Computers & Security,* 25(4):289-296.

Kuppusamy, P., Samy, G. N., Maarop, N., Magalingam, P., Kamaruddin, N., Shanmugam, B. and Perumal, S. 2020. Systematic literature review of information security compliance behaviour theories. In Proceedings of the *Journal of Physics: Conference Series*: IOP Publishing, pp. 1-14.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M. and Hohler, B. 2013. Employees' information security awareness and behavior: A literature review. In Proceedings of the *46th Hawaii International Conference on System Sciences (HICSS)*: IEEE, pp. 2978-2987.

Li, H., King, G., Ross, M. and Staples, G. 2000. BS7799: A suitable model for information security management. In Proceedings of the *Americas Conference on Information Systems 2000*, Long Beach, CA, USA: Association for Information Systems, pp. 205-211.

Lundgren, B. and Möller, N. 2019. Defining information security. *Science and Engineering Ethics,* 25(2):419-441.

Mahfuth, A. A. A. 2020. An investigation on the relationship between security knowledge constructs and employee behaviour in organisations. Doctoral thesis, Universiti Tenaga Nasional.

Medeiros, A. S., Martinez, L. F. and Martinez, L. M. 2020. Assessing the determinants of millennials' online protective behavior: How their protection motivation translates into actual use behavior, in Martínez-López, F.J. & D'Alessandro, S. eds. *Advances in Digital Marketing and*

eCommerce: First International Conference. Cham, Switzerland: Springer Proceedings in Business and Economics, pp. 153-162.

Menard, P., Bott, G. J. and Crossler, R. E. 2017. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems,* 34(4):1203-1230.

Miller, C. and Stuart Wells, F. 2007. Balancing security and privacy in the digital workplace. *Journal of Change Management,* 7(3-4):315-328.

Moletsane, T. and Tsibolane, P. 2020. Mobile information security awareness among students in higher education: An exploratory study. In Proceedings of the *2020 Conference on Information Communications Technology and Society (ICTAS)*: IEEE, pp. 1-6.

Moody, G. D., Siponen, M. and Pahnila, S. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly,* 42(1):285-311.

Nguyen, Q. N. and Kim, D. J. 2017. Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives. In Proceedings of the *50th Hawaii International Conference on System Sciences*, Hawaii: University of Hawaii at Manoa, IEEE, pp. 4947-4956.

Ooi, K.-B., Hew, J.-J. and Lin, B. 2018. Unfolding the privacy paradox among mobile social commerce users: A multi-mediation approach. *Behaviour & Information Technology,* 37(6):575-595.

Park, S., Ruighaver, A. B., Maynard, S. B. and Ahmad, A. 2012. Towards understanding deterrence: Information security managers' perspective. In Proceedings of the *International Conference on IT Convergence and Security 2011*: Springer, pp. 21-37.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. 2017. The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security,* 66(2017):40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security,* 42(2014):165-176.

Rogers, R. W. 1975. A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology,* 91(1):93-114.

Samonas, S. and Coss, D. 2014. The CIA strikes back: Redefining confidentiality, integrity and availablility in security. *Journal of Information System Security,* 10(3):21-45.

Scholl, M. 2018. Awareness in information security. *Systemics, Cybernetics and Informatics,* 16(4):80-89.

Schrader, P. and Lawless, K. A. 2004. The knowledge, attitudes, & behaviors approach - How to evaluate performance and learning in complex environments. *Performance Improvement,* 43(9):8-15.

Sommestad, T. and Hallberg, J. 2013. A review of the theory of planned behaviour in the context of information security policy compliance. In Proceedings of the *IFIP International Information Security Conference*, Auckland, New Zealand: Springer, pp. 257-271.

Sommestad, T., Karlzén, H. and Hallberg, J. 2017. The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems,* 59(4):344-353.

Stewart, H. and Jürjens, J. 2017. Information security management and the human aspect in organizations. *Information & Computer Security,* 25(5):494-534.

Taherdoost, H., Chaeikar, S., Jafari, M. and Shojae Chaei Kar, N. 2013. Definitions and criteria of CIA security triangle in electronic voting system. *International Journal of Advanced Computer Science and Information Technology (IJACSIT),* 1(1):14-24.

Tsohou, A., Karyda, M. and Kokolakis, S. 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security,* 52(1):128-141.

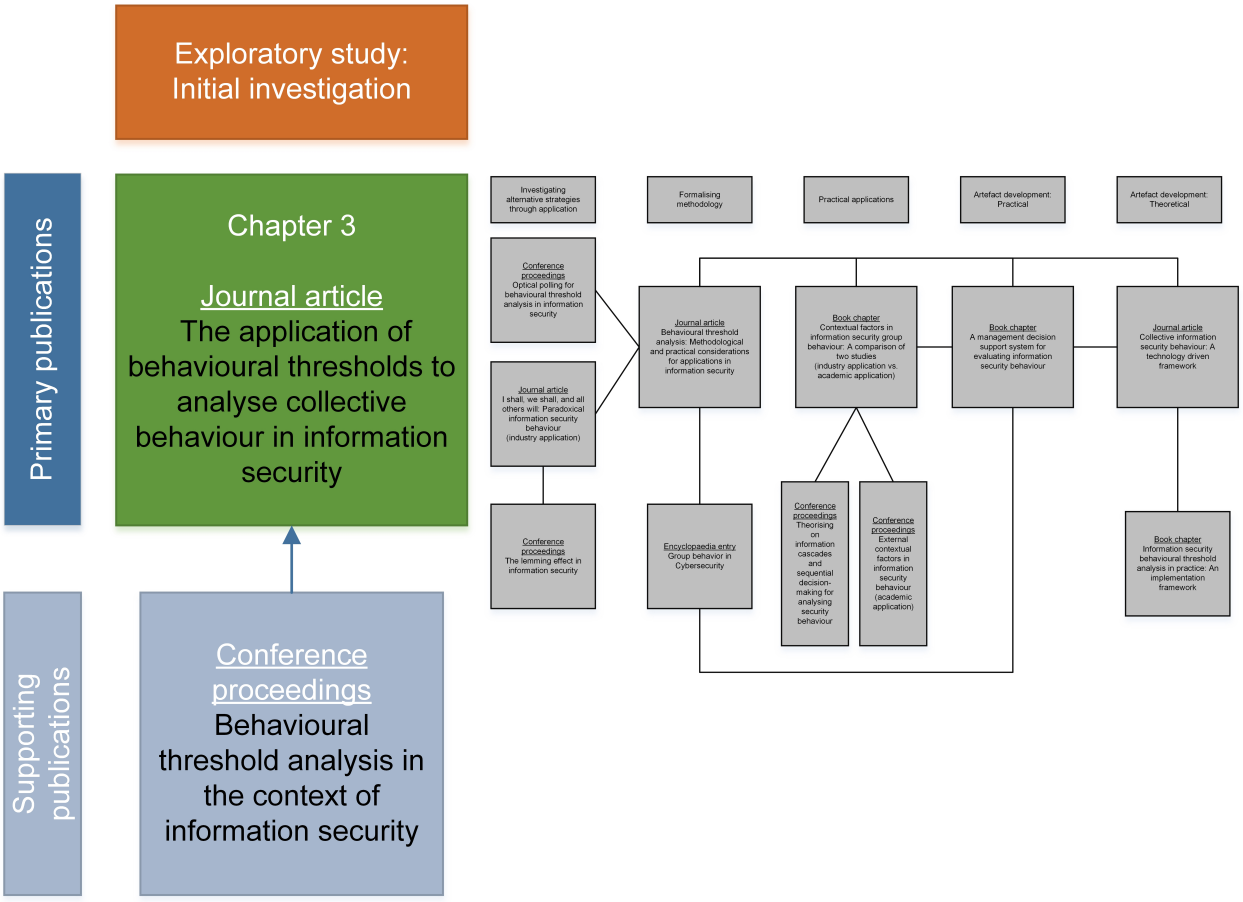
Vafaei-Zadeh, A., Thurasamy, R. and Hanifah, H. 2019. Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior. *Kybernetes,* 48(8):1565-1585.

Van Bavel, R., Rodríguez-Priego, N., Vila, J. and Briggs, P. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies,* 123:29-39.

Van Niekerk, J. F. 2010. Fostering information security culture through intergrating theory and technology. Doctoral thesis, Nelson Mandela Metropolitan University.

Whitman, M. E. and Mattord, H. J. 2011. Principles of information security. Fourth edn. Boston, MA, USA: Cengage Learning.

Chapter 3
-
Article I: The application of behavioural thresholds to analyse collective behaviour in information security



Chapter table of contents

3.1 Preamble to Article I 55

3.2 Emerald journal style requirements 56

3.3 Article I 56

3.3.1 Introduction 57

3.3.2 Contextual background 59

3.3.3 Typical threshold analysis 63

3.3.4 Illustrative example of threshold analysis in the context of information security 64

3.3.5 Future work 67

3.3.6 Conclusion 67

3.3.7 References 68

3.1 Preamble to Article I

The chapter layout in Figure 1.3, Chapter 1, is reiterated at the start of this and each subsequent chapter. The figure is used to help orientate the reader with respect to the coherence of the series of papers and tracks the progress through the thesis. Each of the articles that follow forms part of a chapter of the thesis. These articles that form the core of the chapters are categorised in the accompanying diagram as *primary publications*. Some articles are extensions of previous conference papers that were invited for publication in journals or as book chapters. The original versions of the papers are shown as *supporting publications* on the diagram and are available in the Appendices. One exception to this is Article V. The primary publication to which this supporting publication is connected is not a direct extension thereof, but conceptually the latter can be seen as the natural predecessor, and contributes to the theoretical underpinning of the former. As the reader progresses through the thesis, the current article for the current chapter is highlighted in green on the graphical representation of the chapter layout while a description of the current research phase (possibly comprising multiple publications) is shown in orange. These research phases align with one or more of the research activities of design science research and aim to sketch the background against which each article was written. Furthermore, the articles are preceded by a preamble that provides a narrative that contextualises the publication in the greater scheme of the overarching thesis as well as relating the different articles to one another. Hence, in this chapter, the first of the series of papers is presented. The paper forms part of the *Exploratory study: Initial investigation* phase:

In Article I, the first exploratory application of behavioural threshold analysis in the context of information security is described. The approach was contextualised within the theoretical foundations of the *theory of planned behaviour*, which is commonly used in behavioural information security research. A reflection was provided on how the *threshold models of collective behaviour c*an extend the theory of planned behaviour and, subsequently, how behavioural threshold analysis can leverage its constituents to evaluate security behaviour. The investigation into the suitability of the approach for assessing information security behaviour was conducted as an exploratory study where generic behavioural threshold analysis was presented and then applied by collecting data on the behavioural thresholds of individuals in a group setting. The approach was found to be applicable to this context, but did bring about some challenges and opportunities that can be used to improve upon the initial work to bring the results more in line with the expected patterns that are seen in literature, and the intuitive expectations of the researchers. The paper is concluded with a discussion of the performance of the approach, as well as suggestions for areas for improvement, including data collection, and question or topic

identification and presentation. The findings of the paper subsequently informed the directions for further investigation on how it could be adapted to establish the approach for applications in information security and are addressed in the succeeding articles.

A paper entitled, *Behavioural thresholds in the context of information security*, was presented at the *10th International Symposium on Human Aspects of Information Security & Assurance* held in Frankfurt, Germany from 19-21 July 2016, and published in the related peer-reviewed proceedings[2]. Based on the reviewer reports and evaluation of the presentation during the conference, the paper was identified as being of a high standard and was invited by the editor for publication in a leading security journal, *Information & Computer Security*. An extended version of the original paper was published in Volume 25, Issue 2 of the journal in April 2017 under the title: *The application of behavioural thresholds to analyse collective behaviour in information security*[3]. This extended version is presented here as Article I. The original conference contribution in the proceedings is presented in Appendix B.

3.2 Emerald journal style requirements

The requirements of the journal specified that the *Emerald Harvard* referencing style be used. The article is presented in its final edited and typeset form as it was published in the journal[4]. Information regarding the author guidelines of the journal can be found in Appendix F.

3.3 Article I

Article follows on next page.

[2] Snyman, D. P. and Kruger, H. A. 2016. *Behavioural thresholds in the context of information security*. In Clarke, N. L. & Furnell, S. M. Eds., Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016), Frankfurt, Germany: Plymouth University, pp. 22-32..

[3] Snyman, D. P., & Kruger, H. A. 2017. The application of behavioural thresholds to analyse collective behaviour in information security. *Information & Computer Security*, 25(2):152-164.

[4] Correction – In Article I, Figure 1, an element of the diagram was mislabelled in the published version of the article. The error was corrected in the version of the paper that is included here.

Received 25 March 2017
Revised 25 March 2017
Accepted 5 April 2017

The application of behavioural thresholds to analyse collective behaviour in information security

Dirk Snyman and Hennie Kruger
School of Computer, Statistical and Mathematical Sciences, North-West University, Potchefstroom, South Africa

Abstract

Purpose – The purpose of this study is to perform an exploratory investigation into the feasibility of behavioural threshold analysis as a possible aid in security awareness campaigns.

Design/methodology/approach – Generic behavioural threshold analysis is presented and then applied in the domain of information security by collecting data on the behavioural thresholds of individuals in a group setting and how the individuals influence each other when it comes to security behaviour.

Findings – Initial experimental results show that behavioural threshold analysis is feasible in the context of information security and may provide useful guidelines on how to construct information security awareness programmes.

Practical implications – Threshold analysis may contribute in a number of ways to information security, e.g. identification of security issues that are susceptible to peer pressure and easily influenced by peer behaviour; serve as a countermeasure against security fatigue; contribute to the economics of information security awareness programmes; track progress of security awareness campaigns; and provide a new measure for determining the importance of security awareness issues.

Originality/value – This paper describes the very first experiment to test the behavioural threshold analysis concepts in the context of information security.

Keywords Information security, Human behaviour, Behavioural threshold analysis, Information security awareness programmes, Security culture

Paper type Research paper

1. Introduction

On the terrain of information security research, one of the prevailing themes is that of the human factor. Humans have even been branded to be the weakest link in the fragile information security chain (Soomro *et al.*, 2016; Tsohou *et al.*, 2015; Yildirim *et al.*, 2011). In fact, in a recent summative study of literature pertaining to information security management, Soomro *et al.* (2016) found the human factor to be one that is recurrently identified a nd r esearched a nd i s o ften c lassified un der th emes li ke "h uman as pects in information security" (Safa *et al.*, 2016), "information security awareness" (Tsohou *et al.*, 2015) and "information security culture" (Dhillon *et al.*, 2016).

The influence of this factor continues to have a far-reaching impact on the security and integrity of computerised systems due to the inherent imperfections that humans exhibit when compared to technical layers of security (Berger, 2011; Richardson, 2011; Richardson , 2008). People can be easily influenced by circumstances and they may divulge sensitive information (sometimes unwittingly, other times with specific intent) that could have a detrimental effect on the security and integrity of the systems with which they interact (Richardson, 2011).

Information & Computer Security
Vol. 25 No. 2, 2017
pp. 152-164
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-03-2017-0015

One way to deal with these shortcomings (in terms of information security) is to ensure that security awareness programmes are implemented in organisations. The goal of such programmes is to educate and instruct the members in an organisation about issues regarding information security and to influence their behaviour, or the reigning information security culture, in a positive manner (Tsohou *et al.*, 2015). Information security culture is said to be the system of shared patterns or beliefs, in terms of information security, held by members of an organisation. The security culture of an organisation is governed by a shared system of beliefs, influenced by the members of the organisation (Dhillon *et al.*, 2016).

Having security awareness programmes that function effectively is crucial in managing the information security culture of any organisation. Developing and using these programmes take time and effort which make them costly. Security awareness programmes should, therefore, be tailored to fit the group to ensure that the programmes succeed in their goal. The approach highlighted by Tsohou *et al.* (2015) would be to analyse the behaviour in the organisation through the lens of different behavioural models to determine the reason why the individual, and later the group, behaves in a certain way.

The reasons for the way in which behaviour within an organisation is formed are not always overt, but according to Tsohou *et al.* (2015), behaviour of the individual and the group may be influenced by cognitive and cultural biases. These biases affect the way in which they (the organisation as individuals and as a group) adopt information security regulation and policies. By keeping these factors in mind, security awareness programmes may be optimised.

Granovetter (1978) presents a behavioural model based on the premise that group behaviour is determined by the influence that individuals have on one another. Specifically, how an individual reacts to the actions (or absence of actions) of others (see Section 2.2). This reaction is said to be based on an intrinsic threshold that an individual has to participate, given the number of others who already participate. Such a behavioural model may prove useful to assess security culture and determine how the individual and the group is influenced by peer behaviour (Herath and Rao, 2009). For example, if high personal thresholds for an information security-related topic (like password security) is noted, it would suggest that users are unlikely to be influenced by the behaviour of others, which would indicate that little focus on password security is warranted in a security awareness programme. Conversely, if a low personal threshold is noted, users should be more likely to be influenced by the behaviour of others. Security awareness programmes should, therefore, have their focus on the relevant topics to influence security behaviour in a positive way and should contribute to the economics of security awareness by only including suitable topics in security awareness programmes to limit the high cost (in terms of time and money) usually associated with the development of such programmes. Furthermore, the modern user gets overloaded with security information and has become security fatigued (Furnell and Thomson, 2009) and by tailoring the content of security awareness programmes, security fatigue may be prevented to promote the effectiveness of security awareness programmes.

With this in mind, this paper aims to perform an exploratory investigation into the feasibility of behavioural threshold analysis as a possible aid in developing the right (especially content-wise) security awareness programmes for a given group or organisation. To achieve the abovementioned aim, this paper is structured as follows: Section 2 describes literature from related work pertaining to security awareness programmes, information security behaviour, behavioural thresholds and instruments that can be used to analyse these thresholds. Section 3 demonstrates a typical behaviour threshold analysis. Section 4 presents an illustrative example of threshold analysis, with specific focus on its application

in information security. Section 5 looks towards future directions for this research, and finally, Section 6 summarises the findings of this study.

2. Contextual background

This section shows cursory examples of the related literature, highlighting issues in security awareness programmes, behavioural thresholds, and presents a theoretical background on behaviour in the context of information security.

2.1 Security awareness programmes

Security awareness programmes play an important part in managing the information security culture of an organisation (Tsohou *et al.*, 2015). These programmes convey information about the security policies and possible security threats within an organisation, and they serve as a mechanism to educate users and create awareness about relevant security issues that face the organisation. It is usually assumed that the users within an organisation are prone to risky behaviour in terms of security because they are unaware that their behaviour is risky, and even when informed to the contrary, they are unaware of the potential consequences of their actions.

Tsohou *et al.* (2015) further state that even though there are guidelines and standards that govern the development of security awareness programmes, they often fail because they fail to provide for the way in which users form ideas and opinions on a cognitive level. By not taking this into account, these programmes merely bombard the user with information that does not influence the security behaviour of users as it is supposed to do. For further reading on security awareness programmes, including comprehensive literature surveys, see Safa and Von Solms (2016), Soomro *et al.* (2016) and Lebek *et al.* (2013).

2.2 Behavioural thresholds

Granovetter (1978) (and later Granovetter and Soong (1983)) argues that the preferences, norms or beliefs of an individual are seldom formed without the influence of the environment (especially the interaction with others) in which the individual finds himself. He further argues that these norms can change because of the influence of the behaviour of a group of people, even to such an extent that the behaviour of the individual can change to the exact opposite of said individual's prevailing norms. This phenomenon can occur even without direct confrontation of the individual by any member(s) of the group.

This trigger of paradoxical behaviour may be attributed to humans having an inherent threshold for the acceptance of, and participation in, behaviour in a group setting. For instance, when protesters gather to further a specific cause, emotions and convictions can cause the situation to be volatile. When a core individual or group starts acting violently, the situation can easily escalate to a full-blown riot. Suddenly, all of the (once peaceful) protesters participate in acts of vandalism and the like. For instance, if Person A is a peaceful protester and believes in peaceful resolution of differences; however, he is willing to commit to violence if at least a certain critical mass of others in the protest commit to violence.

This phenomenon can be translated to an organisational setting where, for example, management wants to implement a new information security policy and wants to generate acceptance for the policy amongst the members of the organisation. They need only to influence a critical mass of members and the others will follow in acceptance. Contrariwise, when a certain critical mass of members deviate from the prescriptive policies, there could be a detrimental effect in the overall compliance as the remaining members will once again follow in example, but in a manner that is contraindicated.

A proposed model by Granovetter (1978) aims to analyse the inherent thresholds of the individuals that make up a group and predict the outcome of situations where a critical mass

influences the remainder of individuals. This model is referred to as "behavioural threshold analysis" and is based on circumstances where the actors (members of a group) only have two discrete and opposing avenues of pursuit. Usually, choosing the behaviour in one direction has a supposed positive result and the other has a negative result. The analogy (as explained above) of either participating in a riot or not participating, is used to emphasise these two opposing views, but Granovetter (1978) argues that the model is applicable to any contrasting binary decision. See Granovetter (1978) and Growney (1983) for further analogical situations.

The inherent personal cost versus gain of committing to either of these choices is what determines the individual's threshold pertaining to participation or abstention. The perceived cost of participation differs for each individual that a group consists of. Some individuals require little to no motivation to participate in an activity and can be seen as instigators, while others need to be swayed to join in uncharacteristic activity due to the perceived gain outweighing the cost. Some perceive the cost as being infinitely high and will never join in.

The aim of this model is to describe the outcome of a situation, given the collection and distribution of individuals (each with their own threshold) who are involved therein by predicting the number of individuals opting for each of the opposing behaviours. As mentioned in the Introduction, this model may be implemented as an aid in determining the content of security awareness programmes by analysing the susceptibility of users being influenced by others in terms of information security issues. Using this model as a barometer, only relevant information may be included in security awareness programmes, possibly saving time and money.

2.3 Theoretical framework for information security behaviour

The goal of this section is to contextualise the relationship between behaviour and attitude in terms of this research.

Literature pertaining to information security behaviour, and indeed human behaviour in general, frequently allude thereto that the behaviour of an individual in a certain situation is influenced by the attitude that the individual has towards the situation or so-called "attitude object" (Kroenung and Eckhardt, 2015; Stedman, 2002; Fazio, 1990). Positive attitudes towards a specific attitude object lead to positive behaviour, while a negative attitude leads to a negative behaviour in relation to the attitude object (Stedman, 2002).

This relationship between attitude and behaviour has been formalised over some years. Many theories and models have been developed to study behaviour in various situations. Kearney and Kruger (2016) summarise the most prevalent theories as the following: the theory of reasoned action (TRA); the theory of planned behaviour (TPB); the general deterrence theory; and the protection motivation theory. Of the aforementioned, TPB (which is an extension of TRA) draws on the attitude of an individual to predict the intention that the individual has to perform a specific behaviour (Ifinedo, 2012; Bulgurcu *et al.*, 2010). The reported link between behaviour and attitude is also in line with another early and influential model, which aims to describe the relationship between attitude and behaviour. This model is called the MODE (m**o**tivation and opportunity as d**e**terminants) model which was presented by Fazio (1990). The MODE model indicates that under the right circumstances, attitude can be a direct precursor for behaviour. The TPB forms the basis for this study and is graphically depicted in Figure 1.

The highlighted area shows the domain for this research within the existing model. As explained in Section 1, this paper aims to investigate behavioural threshold analysis, and based on the link between attitude and behaviour (as mentioned above), attitude cannot be

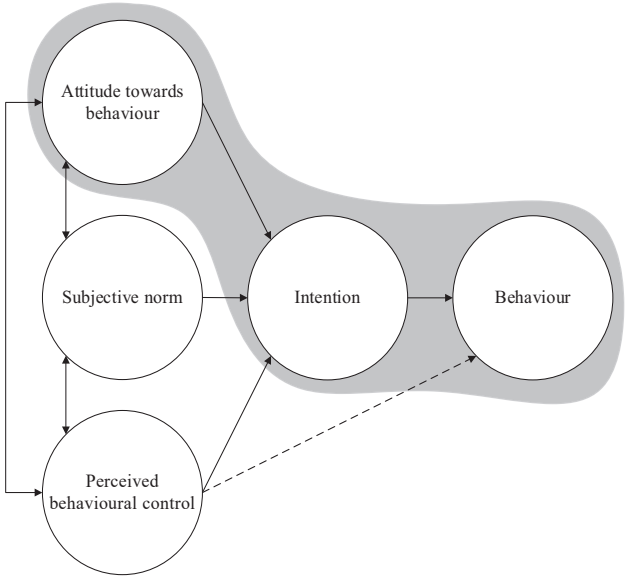


Figure 1.
TPB

Source: Adapted from Ajzen (1991)

separated from behaviour. This is evident in the manner in which behavioural thresholds (see Section 2.2) are determined: firstly, before any analysis is done, the attitudes within a group are observed (if enough people perform an action, I will also perform the action). After the attitudes have been tabulated and analysed, a specific behaviour (action being performed or abstained from) may be predicted. To further contextualise this research within the domain of behavioural theories, Figure 2 extends the shaded area of Figure 1 to show the relationship between attitude, behaviour, behavioural threshold analysis and security awareness programmes.

The connections between the elements in Figure 2 show that the attitude towards a behaviour and the intent to perform a behaviour can be measured to determine the related behavioural thresholds. These thresholds can then in turn be leveraged to determine which security awareness topics should be included in security awareness programmes, which is also the ultimate goal of this research project.

Measuring attitude in an assuredly accurate manner may present some problems. Frangopoulos *et al.* (2014) mention some common issues pertaining to bias when respondents answer questionnaires – which is a common data collection tool and also used in this study – that could have a negative impact on the subject being measured. Social desirability is a bias that is driven by respondents having a pre-conceived notion of the "correct" or "expected" answer (Kearney and Kruger, 2016; Fisher, 1993). The answers given are not a reflection of the truth or status quo, but rather a version of events that reflects actions that are deemed socially acceptable. This is especially applicable in terms of behavioural threshold analysis because of the sensitive nature of questions or statements like, in general, "I will cheat on an exam if enough other people do so" and more specifically, in terms of information security, "I will share my password with others if enough people do it". The tendency will be to say that one will never cheat or share passwords because of a perceived social taboo on these actions, even if this is in direct contradiction with one's actual actions.

Other issues are that different people also have different attitudes, influenced by many different factors like age, gender, education level, occupation, work environment, etc. This means that when people are questioned about their attitude at a different time or under

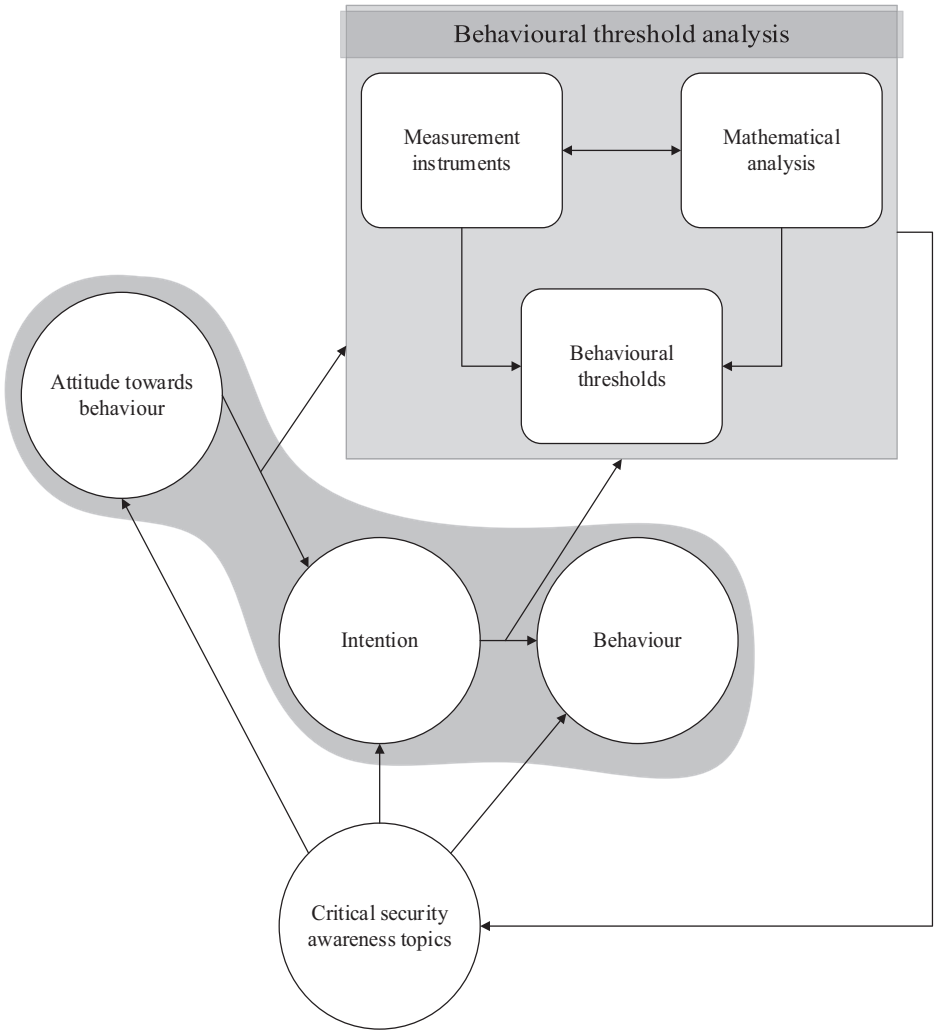


Figure 2.
Conceptual model for behavioural threshold analysis in information security

different circumstances, they might provide altered or even opposing answers due to external influences. Different information security topics or subjects (e.g. passwords and email security) may also elicit different attitudes. Even within an individual, there may exist different attitudes towards different information security topics due to the perceived risk or reward associated with complying with the guidelines for a specific topic (Kroenung and Eckhardt, 2015).

The abovementioned issues need to be addressed to ensure the validity and integrity of an analysis of attitudes and behaviour towards information security. This paper is of an exploratory nature and is the first report of an ongoing project. Therefore, methods to address these issues form part of the future work as described in Section 5. The following section describes the typical analysis of recorded thresholds based on the analysis as presented by Growney (1983).

3. Typical threshold analysis

Growney (1983) posits that, to obtain the individual threshold values from a group, a simple standard questionnaire can be used. The individuals in a group are requested to truthfully respond to a set of questions about two discrete outcomes of a situation in which the individuals as part of a group may find themselves. The individuals are asked to complete a

value for x in 2(b) of Figure 3. The value quoted represents the inherent threshold for the individual in question.

After the responses are received from the respondents, the responses can be tabulated and represented in a graph format. Threshold analysis can then be performed on the observed values to predict the outcome of the behaviour of the group under observation. Observe the following set of cumulative thresholds (Table I). These thresholds were obtained for an imaginary group of people in an imaginary setting as if they had completed a questionnaire like the one in Figure 3. Let the two mutually exclusive outcomes as mentioned earlier be Outcome A (negative) and Outcome B (positive).

The thresholds tabulated in Table I represent an individual's threshold to participate in an action (Action A) that will lead to Outcome A. In other words, how many individuals have to perform Action A before the individual, whose threshold is being noted, will join in and also perform Action A. Consider the number of individuals with a given threshold of 20. These 15 individuals will be inclined to perform Action A when 20 or more people already participate. The cumulative frequencies (Column 3) indicate that there are 30 people in total with the threshold of 20 or less, which means that the 15 people with the threshold of 20 will join in Action A. The participating group will continue to grow as long as the thresholds in Column 1 are exceeded by the cumulative frequencies in Column 3.

Questionnaire

1. Choose one of the following outcomes that is preferable:
   a. Outcome A
   b. Outcome B
2. Regardless of the outcome selected above, respond to the following statements:
   a. I will never participate in Action A
   b. I will participate in Action A when at least x number/percent of group members choose to participate in Action A.

Figure 3.
Threshold questionnaire

Source: Growney (1983)

Thresholds	No. of individuals with given threshold	Cumulative frequencies of individuals with a threshold ≤ given threshold
0	0	0
10	15	15
20	15	30
30	10	40
40	30	50
50	10	80
60	0	90
70	0	90
80	0	90
90	0	90
100	0	90
No threshold	10	

Table I.
Threshold analysis

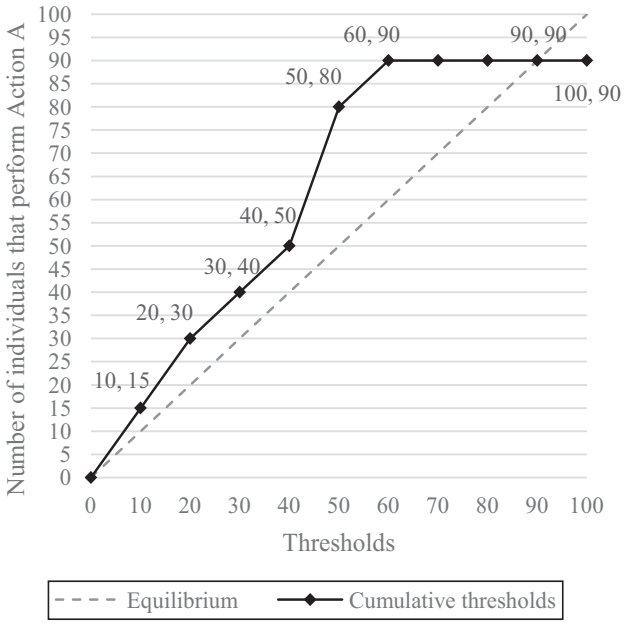
Source: Growney (1983)

The complete behavioural threshold analysis is based on the comparison of all the individual behaviour thresholds – noted across the group in question – to a uniform distribution of thresholds said to be the equilibrium. A graphic representation of Table I is presented in Figure 4. To simplify the analysis, all values have been expressed as percentages and thresholds adjusted to intervals of 10 (Growney, 1983; Granovetter, 1978).

With reference to Figure 4, when observing the threshold line segments to either the left or right of an intersection with the equilibrium line, the gradients of these line segments describe the stability of the group's behaviour against deterioration (heading towards Outcome B) or escalation (heading towards Outcome A). When the line segment to the left of an equilibrium intersection has a gradient of less than one, the equilibrium that has been reached is said to be stable against decrease (towards B), and a segment with a gradient of less than one to the right, stable against increase (towards A). If both conditions of line segment with gradients less than one are met, the equilibrium is said to be stable and the group will remain in its current state; otherwise, there will be a movement towards one of the extreme outcomes (A vs. B). Upon inspection of the resulting graph (Figure 4), an upward trend with a positive gradient is identified up to the (60, 90) co-ordinates. Thereafter, a gradient of 0 (horizontal line segments) is noted for the remainder of the graph. When equilibrium is reached at the intersection (90, 90), the conditions for a stable equilibrium are reached and no further deterioration or escalation is possible. The following section will present an illustrative example to show how the principles of behavioural threshold analysis are applied in the context of information security.

4. Illustrative example of threshold analysis in the context of information security

To meet the aim of this study, a threshold analysis is to be performed in terms of information security to gauge the effectiveness thereof as a tool for the development of security awareness programmes. The example mentioned in this section is still in an exploratory phase. It was the very first experiment to test the behavioural threshold analysis concepts in



Source: Growney (1983)

Figure 4.
Threshold analysis example

the context of information security. The experiment was carried out with students as a test group, and the initial results, which are used here only as an illustration, will be used to improve the security questions that are asked, as well as refine the experimental process as a whole.

4.1 Data collection

The questionnaire that was used for data collection for this research was based on the questionnaire that is presented in Section 3. Questions were added to supplement the questionnaire to determine basic demographic information such as gender, age, etc. To test the questionnaire, it was distributed to a group of first-year engineering students at a South African university. Distribution and capturing of the students' responses was facilitated by hosting the questionnaire on Google Forms. Out of a possible 70 students, 22 had responded, resulting in a response rate of 31.4 per cent. Of these 22 students, 13 identified themselves as male and 9 as female. An example of the questionnaire is presented below in Figure 5. The section of the questionnaire that contains questions about demographic information is not shown due to space considerations. Because of the exploratory nature of this research, it was opted to use a simple information security aspect for behavioural threshold analysis. Passwords were used as the basis for the questions, as all students need to use passwords on a daily basis and should be familiar enough for them to relate to. Students were asked whether they would share their passwords if enough other students opt to do so and if so, how many students need to share their passwords before they would also share their passwords. The sections in the questionnaire below were presented one at a time, based on the responses received.

Initial pilot runs of this questionnaire proved troublesome with students being unsure of how to answer the questions relating to their password-sharing behaviour, specifically question 2(A) as it was not clear to respondents that they needed to nominate a threshold value resulting in a majority of unusable responses. The measurement instrument still needs refinement to ensure the results obtained are representative of the security behaviour in the group. The choice of what is to be measured should also be re-evaluated as passwords (which form the basis for the behavioural threshold questionnaire) might be one aspect of information security that the respondents are too familiar with. They may be security fatigued due to overexposure to awareness campaigns which taints their answers to the questionnaire. This prompted a redesign of the presentation of the questions about their security behaviour. It was noted that the manner in which the questions are structured in this questionnaire (Figure 5) may seem reversed when compared to the example in Section 3 and that seen in literature. This is due to Growney (1983) proposing that issues with responses on

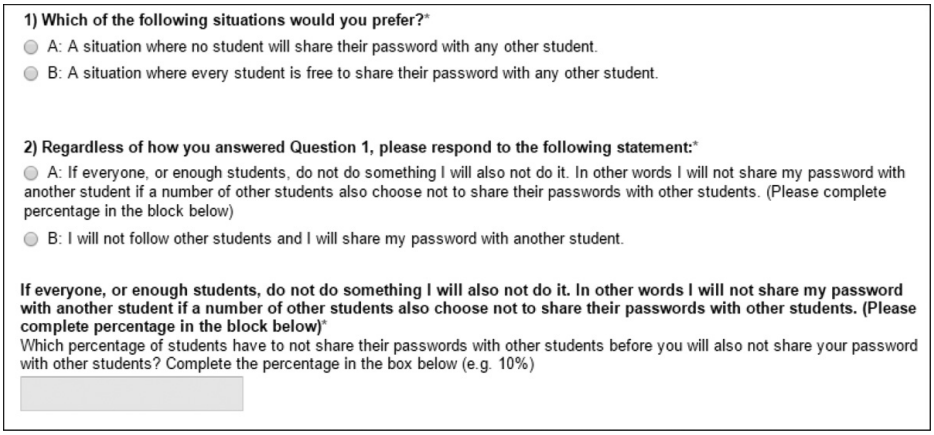


Figure 5.
Behavioural threshold questionnaire

the questionnaire, where the question was not understood by the respondents, may be solved by reversing the order in which the different outcomes are presented. This leads to interpretable results that can be displayed in an analogical manner of the way in which behaviour threshold analysis may be implemented in an information security behaviour setting. The questions on information security behaviour, specifically on passwords, still need to be re-evaluated and refined to ensure operability in a real-world analytical setting. The following section presents the results of the group behaviour threshold analysis for the above-mentioned questionnaire.

4.2 Results

Figure 6 shows the results of the responses received from the questionnaire from Section 4.1. The resulting graph shows a positive gradient up to the (10, 9.09) coordinates where the graph intersects the equilibrium line. The line segment to the left of the intersection with the equilibrium line has a gradient of 0.454 (less than one), which indicates stability against decrease. The line segment to the right of the intersection with the equilibrium line has a gradient of 0 (less than one) which, in turn, indicates stability against increase. Equilibrium is reached at the intersection and the conditions for a stable equilibrium are met and no further deterioration or escalation is possible.

When this is interpreted in terms of information security and the questions posed in the questionnaire, there will be an increase in participation to the point where almost 10 per cent of the students are influenced to join in and share their passwords with others. This number should remain stable, as there is not enough momentum for this trend to catch on to the other students. This is due to the equilibrium being reached at a point where there are no more growth opportunities where the self-reported thresholds of the students are exceeded and students will not be influenced to join in. The stability in password-sharing behaviour that is noted from the analysis may now be used to determine whether "passwords and password

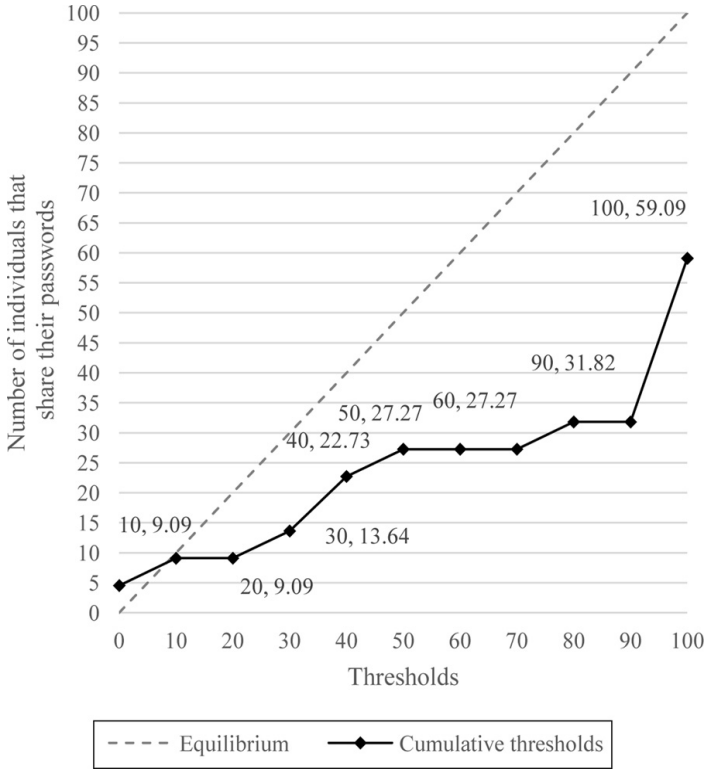


Figure 6.
Results for threshold analysis

confidentiality" is a suitable subject to include in security awareness programmes for this specific group. Depending on other considerations in information security that an organisation might have and need to address, they might decide that 10 per cent of users sharing their passwords are a problem that needs addressing immediately (rather than any other current security matters) and opt to include password education in security awareness programmes. Conversely, they may decide that other matters are more pressing than the sharing of passwords and because of the stability (i.e. the problem is not a growing one), they may opt to leave password education out of a security awareness programme for possible inclusion at a later date.

This initial analysis of security behaviour by using behavioural threshold analysis is still in its infancy, but shows promise as a tool for measurement, analysis and prediction of security behaviour and awareness. However, there are still problems which would need to be addressed. These problems are to be addressed as future work and is summarised in the following section.

5. Future work

Section 2.3 highlights some key issues that have to be kept in mind when measuring attitudes and behaviour, amongst others, social desirability, differing attitudes due to biographic differences between individuals, difference in personal attitudes when measured under different circumstances and also difference in personal and individual attitudes towards different security topics. For the most part, future work comprises of determining methods that may be used to mitigate the effect of the abovementioned issues. These include the investigation on how attitude is measured using psychological instruments (questionnaires). Determine how social desirability may be measured and, if found to be present, provided for when using questionnaires. Questionnaires are often used when measuring attitude in terms of information security, but they are known to be prone to social desirability. Pattinson *et al.* (2016) suggest that a repertory grid approach might deliver better, non-biased results even if the approach might be tedious. They further suggest that a combination of these two approaches may improve the accuracy of self-reporting instruments. The viability of repertory grids and the combination thereof with questionnaires to measure behavioural thresholds are to be investigated. Using a repertory grid, in turn, prompts an investigation into identifying suitable information security topics for measuring behavioural thresholds, e.g. passwords, email security, etc. A literature review of recent important or high-ranking information security threats (Berger, 2011; Richardson, 2011; Richardson, 2008) should provide a basis for determining topics. And finally, extending this exploratory study to include responses from industry to obtain real-world data that can be analysed to see how the behavioural threshold analysis approach performs.

6. Conclusion

This paper presents an original inquiry into the application of behavioural thresholds and group dynamics in analysing the human factor of information security. The initial experimental results show that behavioural threshold analysis is feasible in the context of information security and may provide useful guidelines on how to construct information security awareness programmes.

The threshold analysis method may contribute to security awareness in the following ways:

- By helping to determine which security issues are easily susceptible to peer pressure or easily influenced by peer behaviour. If such topics can be identified, it means that these are the topics that should be concentrated on in security awareness campaigns.

- By identifying the key issues on which to concentrate in security awareness programmes, the threshold analysis method may serve as a countermeasure against security fatigue.
- It may provide a positive contribution to the economics of security awareness, by helping to save time and money.
- The threshold analysis method can be used later on, after interventions by means of security awareness campaigns, in a follow-up to track progress of security awareness levels. If 90 per cent of the users said they will follow others in doing something that is against information security policies, but in the follow-up, only 10 per cent say they will follow other and also do something against information security policies, an improvement can be noted. This improvement may indicate success in the security awareness programmes.
- Finally, the threshold analysis method gives a new way to measure the importance of security awareness issues in an organisation.

References

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

Berger, U. (2011), *CSI/FBI Computer Crime and Security Survey: 2011-2012*, Computer Security Institute, New York, NY.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Dhillon, G., Syed, R. and Pedron, C. (2016), "Interpreting information security culture: an organizational transformation case study", *Computers & Security*, Vol. 56 No. 1, pp. 63-69.

Fazio, R.H. (1990), "Multiple processes by which attitudes guide behavior: the MODE model as an integrative framework", *Advances in Experimental Social Psychology*, Vol. 23 No. 1, pp. 75-109.

Fisher, R.J. (1993), "Social desirability bias and the validity of indirect questioning", *Journal of Consumer Research*, Vol. 20 No. 2, pp. 303-315.

Frangopoulos, E.D., Eloff, M.M. and Venter, L.M. (2014), "Human aspects of information assurance: a questionnaire-based quantitative approach to assessment", *Proceedings of the 8th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014), University of Plymouth, Plymouth*, pp. 217-229.

Furnell, S. and Thomson, K. (2009), "Recognising and addressing 'security fatigue'", *Computer Fraud & Security*, Vol. 2009 No. 11, pp. 7-11.

Granovetter, M. (1978), "Threshold models of collective behavior", *American Journal of Sociology*, Vol. 83 No. 6, pp. 1420-1443.

Granovetter, M. and Soong, R. (1983), "Threshold models of diffusion and collective behavior", *Journal of Mathematical Sociology*, Vol. 9 No. 3, pp. 165-179.

Growney, J.S. (1983), "I will if you will: individual thresholds and group behavior – applications of algebra to group behavior", *Modules in Undergraduate Mathematics and Its Applications – Tools for Teaching*, COMAP Inc., Bedford, MA, pp. 108-137.

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95.

Kearney, W.D. and Kruger, H.A. (2016), "Theorising on risk homeostasis in the context of information security behaviour", *Information & Computer Security*, Vol. 24 No. 5, pp. 496-513.

Kroenung, J. and Eckhardt, A. (2015), "The attitude cube – a three-dimensional model of situational factors in IS adoption and their impact on the attitude – behavior relationship", *Information & Management*, Vol. 52 No. 6, pp. 611-627.

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. (2013), "Employees' information security awareness and behavior: a literature review", *Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS), IEEE, Wailea, Maui*, pp. 2978-2987.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., Calic, D. and Furnell, S. (2016), "Assessing information security attitudes: a comparison of two studies", *Information & Computer Security*, Vol. 24 No. 2, pp. 228-240.

Richardson, R. (2011), *15th Annual 2010/2011 Computer Crime and Security Survey*, Computer Security Institute, New York, NY.

Richardson, R. (2008), *CSI Computer Crime and Security Survey*, Computer Security Institute, New York, NY.

Safa, N.S. and Von Solms, R. (2016), "An information security knowledge sharing model in organizations", *Computers in Human Behavior*, Vol. 57 No. 1, pp. 442-451.

Safa, N.S., Von Solms, R. and Furnell, S. (2016), "Information security policy compliance model in organizations", *Computers & Security*, Vol. 56 No. 1, pp. 70-82.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Stedman, R.C. (2002), "Toward a social psychology of place predicting behavior from place-based cognitions, attitude, and identity", *Environment and Behavior*, Vol. 34 No. 5, pp. 561-581.

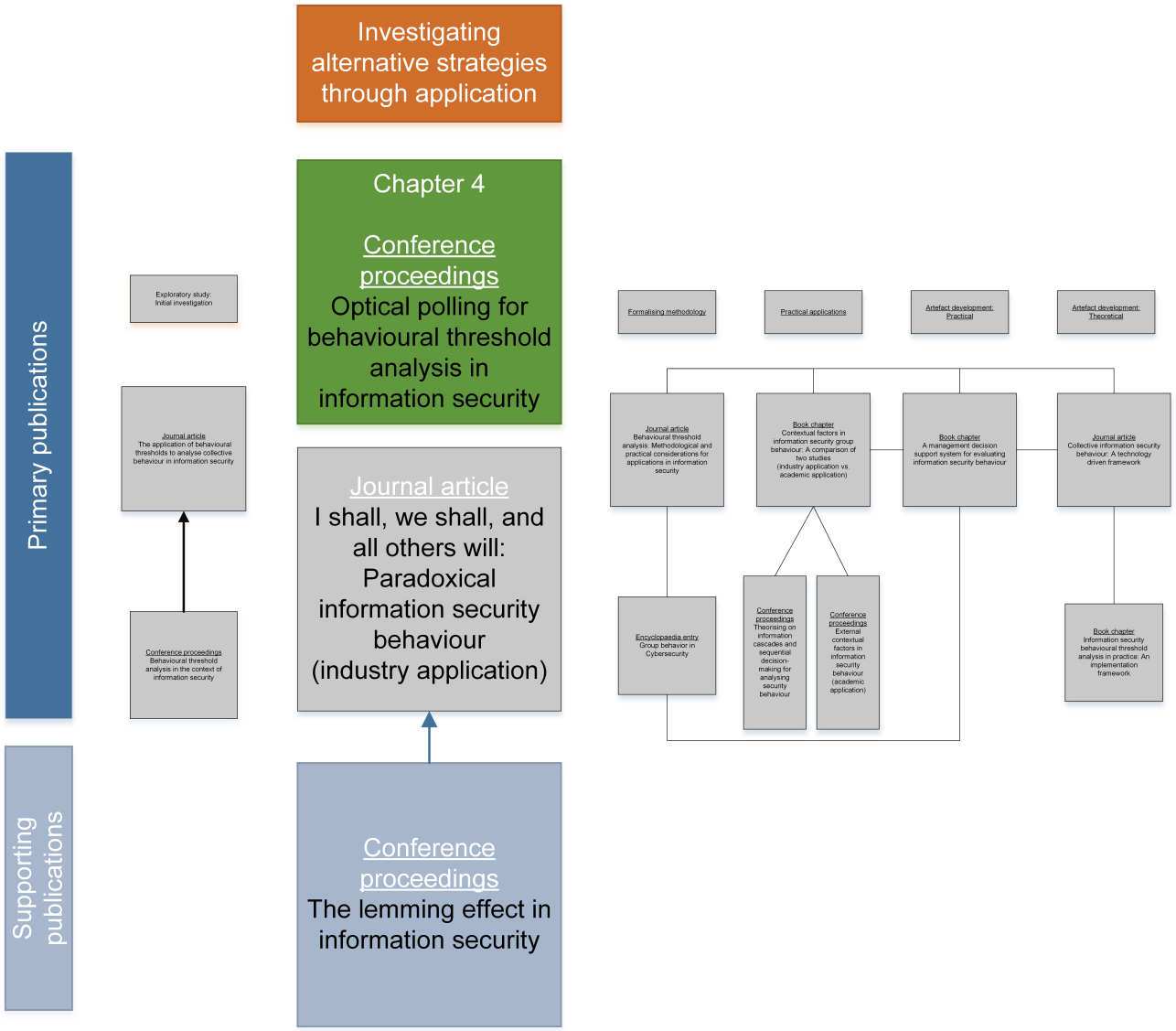
Tsohou, A., Karyda, M. and Kokolakis, S. (2015), "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs", *Computers & Security*, Vol. 52 No. 1, pp. 128-141.

Yildirim, E.Y., Akalp, G., Aytac, S. and Bayram, N. (2011), "Factors influencing information security management in small-and medium-sized enterprises: a case study from Turkey", *International Journal of Information Management*, Vol. 31 No. 4, pp. 360-365.

Corresponding author
Hennie Kruger can be contacted at: hennie.kruger@nwu.ac.za

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**

Chapter 4
-
Article II: Optical polling for behavioural threshold analysis in information security



Chapter table of contents

4.1 Preamble to Article II 72

4.2 IKE'17 conference proceedings style requirements 73

4.3 Article II 73

4.3.1 Introduction 74

4.3.2 Background 75

4.3.3 Methodology 76

4.3.4 Discussion 79

4.3.5 Conclusion 79

4.3.6 References 80

4.1 Preamble to Article II

Following the initial investigation by means of an exploratory study in the previous chapter, the second phase describes investigating *alternative strategies through application* phase. In short, this involves making changes to the generic behavioural threshold analysis approach and evaluating whether the changes contribute positively to the outcomes of such exercises. The current phase encompasses two publications in which different strategies that were applied in practice are described. The first thereof is presented here and the second in the following chapter.

One of the shortcomings of the generic behavioural threshold analysis approach, as applied to information security in Chapter 3, Article I, was identified as the method of data collection, *i.e.,* how the behavioural threshold data is gathered from the participating members of an organisation (respondents). In this section, Article II is presented as an attempt to help mitigate some of the underlying issues.

Behavioural threshold analysis, as applied here in information security, aims to assess behaviour about topics that could be considered to be of a sensitive nature. This includes behaviours such as password sharing, incident reporting, *etc*. Questions on sensitive topics have been shown in literature to elicit untruthful responses from respondents where they respond in a manner that they believe the researcher wants to see or deems appropriate, even if this is not true. This social desirability bias is well known in behavioural research. Research in this domain is reliant on the accuracy and overall trustworthiness of the data that are obtained from the respondents in question.

Another challenge is that behavioural threshold questionnaires comprise relatively many questions. Overwhelming respondents with too many questions often leads to questionnaire fatigue. This hampers response rates (respondents simply do not continue with a questionnaire until the end) and can also lead to respondents completing a questionnaire by answering all the questions by selecting the same response, “drawing patterns” with responses, *etc*.

The article posits optical polling as a method that can lessen the negative effect mentioned above. Optical polling is a method whereby a group of people who are together in a physical space, such as a meeting room or lecture hall, can be surveyed simultaneously in real time. It involves participants responding to questions by means of Likert scale-style responses, *i.e.,* responses that range from 1 to 4. The respondents are each handed a card resembling a QR-code at the start of a session. The card and its relative orientation is used to respond to the questions that are asked by a facilitator who in turn uses the camera function of a mobile device to obtain the responses by reading the cards in the room. The investigation that is described in the article suggests that the approach works well to help address the issues mentioned above.

Article II is entitled *Optical polling for behavioural threshold analysis in information security*[5]. It was presented in 2017 at the peer-reviewed *16th International Conference on Information & Knowledge Engineering (IKE'17)* as part of the annual *World Congress in Computer Science, Computer Engineering & Applied Computing (CSCE'17)* hosted in Las Vegas, Nevada, USA from 17-20 July 2017. The article was published in the conference proceedings.

4.2 IKE'17 conference proceedings style requirements

The conference required papers to be formatted in the Institute of Electrical and Electronics Engineers (IEEE), two-column format, using the IEEE numbered reference style. The article is presented in its final edited and typeset form as it was published in the conference proceedings. Information regarding the author guidelines of the conference can be found in Appendix G.

4.3 Article II

Article follows on next page.

[5] Snyman, D. P., & Kruger, H. A. 2017. *Optical polling for behavioural threshold analysis in information security*. In Arabnia, H.R., Deligiannidis, L., Hashemi, R., Tinetti, F.G. Eds., Proceedings of the 16th International Conference on Information and Knowledge Engineering (IKE'17), Las Vegas, USA, pp. 39-45.

Optical Polling for Behavioural Threshold Analysis in Information Security

Dirk Snyman, Hennie Kruger
School of Computer-, Statistical- and Mathematical Sciences
North West University,
Potchefstroom, South Africa.
e-mail: {dirk.snyman, hennie.kruger}@nwu.ac.za

***Abstract*—In terms of information security research, human attitude and behaviour are commonly sought to be assessed and addressed. These aspects remain complex and difficult to understand and control in order to efficiently manage them. Many psychological and sociological models exist to describe and test human behaviour but they are all reliant on data. This research presents a novel approach for data collection for the specific application of behavioural threshold analysis. Optical polling is found to be a viable alternative to traditional data collection methods which provides good quality data. It addresses some of the issues associated with behavioural threshold analysis and information security research in general.**

Keywords—information security; optical polling; behavioural threshold analysis; data collection.

I. INTRODUCTION

Research pertaining to information security often aims to understand the factors that drive the behaviour of individuals in their everyday interactions with information technology systems [1-3]. Human behaviour is often fickle and unpredictable which makes the management thereof a problematic endeavour. The business risk associated with information security behaviour (namely financial or data loss) necessitates the need for better understanding by management on how and why people do what they do to ultimately provide for different eventualities, or ideally act in a pre-emptive manner to avoid these eventualities from occurring at all. One of the common controls that are put in place to help prevent the above-mentioned losses include the development and deployment of information security policies [4]. These policies aim to govern the interaction between humans and systems in a manner that reduces the associated risks by limiting behaviour that might lead to risky actions. The main issue with policies, however, are that they are only effective when followed to the letter. Individuals tend to develop averse attitudes to policies due to their constricting nature [5] where, for instance, a less secure shortcut to completing a task exists but are contrary to procedures specified by policy. They therefore often opt to disregard policies in part or in their entirety in exchange for the ease or speed conveyed by the risky behaviour [4]. Furthermore, disregard for policies may also be due to ignorance about them rather than resistance towards them [6]. If an individual is oblivious to policies, following them becomes impossible.

To remedy the latter situation where ignorance is the cause of failing policies is relatively simple. By introducing security awareness programs employees can be educated about the existence and contents of information security policies and taught good information security practices [1, 3]. The former, where attitude is to blame, is far more complicated to address. Security awareness programs may help in re-affirming the already known intricacies of said policies, but without a specific focus on addressing behaviour and correcting the underlying attitude such programs may fail. The individual might just become security fatigued due to the possibly repetitive nature of programs that lay emphasis on the same tired topics [7]. Once the audience of such programs have become fatigued, it may lose its efficacy to promote healthy information security practices. The attitude that an individual has towards a situation influences the behaviour that the individual will exhibit when confronted with the specific situation and has been formalised into behaviour models (see [8, 9]). Given this link between attitude and behaviour it is evident that influencing the former, will influence the latter. It should be noted that before an attitude can be influenced, it should first be determined what the existing attitude is in order to determine a course of action.

One approach to bring information security attitude and behaviour together is through behavioural threshold analysis [10]. The application of behavioural threshold analysis as a means of measuring information security attitudes of individuals in a group setting was first presented by Snyman and Kruger [11]. One of the key issues highlighted by this study was the unique requirements of a measuring instrument that would be appropriate in behavioural threshold analysis. This current study will investigate and comment on an alternative data collection method, specifically for behavioural threshold studies, to address the shortcomings of existing measuring instruments. Section II presents a brief overview of behavioural threshold analysis in the context of information security and will also point out some of the specific key issues pertaining to data collection.

Existing instruments for measuring attitude are, although widely used, not without problems [2, 6-9, 11]. Based on these common problems, Crossler *et al.* [6] state that the methods of measuring data relating to information security should be improved. Subsequently Pattinson *et al.* [2] review and compare two standard data collection methods commonly used for measuring attitude. These methods were analysed in terms of ease of implementation and the overall quality of the results obtained by using each method. The two techniques are standard self-reporting (online) questionnaires and repertory grid technique interviews. They conclude that when trying to measure attitude an approach that combines these two methods might be advantageous. In an attempt to combine these methods

ISBN: 1-60132-463-4, CSREA Press ©

and draw from their respective strengths, this study posits evaluating the feasibility of an optical polling data collection method to obtain information on individual attitudes with a specific focus on gathering information security data for behavioural threshold analysis.

The remainder of the paper is organised in the following manner: **Section II** provides the background for the study and describes the related literature on data collection methods for attitude and behaviour in information security. **Section III** presents the methodology for this study as well as results obtained. **Section IV** provides a discussion of the suggested data collection method and **Section V** concludes the paper and presents an overview of planned future work.

II. Background

In an earlier and related study that forms part of the same larger research project, Snyman and Kruger [11] presented the first application of behavioural threshold analysis as an instrument for analysing the human factor of information security. The behavioural threshold approach was first presented by Granovetter [10] in an attempt to provide a model that could be used to predict the outcome of circumstances where people are assembled in a group setting. The proposition for the model is that each individual in a group has an innate attitude toward the actions of others in the specific group. When the individual is confronted with either partaking in or refraining from a specific activity in the group setting the decision is said to be based on the perceived number of others that are already participating in the activity. This innate attitude towards the action, given the knowledge of the number of current participants, is presented as the behavioural threshold of the individual in the context of Granovetter's [10] model. When the number of participants of the activity exceeds that of the individual's threshold, the individual will participate in the activity. This could then be used to determine the number of eventual participants in the specific activity, given the dispersion of the individuals that comprise the group and their own thresholds that determine their participation.

Snyman and Kruger [11] conducted an initial inquiry into employing behavioural threshold analysis for information security. The pilot study that was conducted indicated that behavioural threshold analysis is a feasible approach in terms of information security and determining topics for security awareness programs among others (see [11] for more applications of behaviour threshold analysis in information security). There are, however, some issues that were raised that are to be addressed in future work if behavioural threshold analysis for information security is to properly succeed. Some of the key issues that were identified in the pilot study, with specific reference to behavioural threshold analysis research, were that:

1) Data collection for behavioural threshold analysis requires a unique method of questioning. The initial question in [11] was posed in such a manner that respondents[1] had to nominate a percentage of other group members that were sharing their passwords with others before the respondent would also share their password. This lead to respondents misunderstanding the question and indicating any random percentage value which lead to unexpected aggregated results;

2) The choice of the topic (password security [11]) that was used for collecting behavioural threshold data influences the manner in which respondents answer the question due to their familiarity (and also individual outlooks) with the topic and its recommended practices. For behavioural threshold analysis it is imperative to identify suitable topics upon which questions are based. Topics on which respondents are already security fatigued may not yield useful results for threshold analysis;

3) The influence that biographic differences and circumstances of individuals might have on their reported attitudes. Behavioural threshold analysis measures attitudes in a group setting. The distribution of individuals that make up the group directly influences the attitudes of others in the group and ultimately determine the outcome of group participation;

4) The problem of social desirability and the impact that it might have on the accuracy of the results that are obtained from the application of this model. Social desirability is the supposed predisposition of a person to, when presented with a questionnaire, answer in a manner they would deem socially acceptable [8, 9, 11]. This desire to not offend social decorum leads to answers that reflect that which the person deems acceptable, instead of mirroring the actual events that the person is being asked about. In the context of behavioural threshold analysis, social desirability plays a deeper roll than only influencing the responses on a questionnaire. In its essence behavioural threshold analysis measures the influence of the group on the individual. If an individual suffers from social desirability they may demonstrate an uncharacteristic willingness for group participation with a low threshold. This is because the participant wants to fit in with the group's social dynamic to be accepted. However when an outsider like a researcher questions them about their threshold for participation they might exaggerate their threshold to seem socially acceptable from the researcher's perspective. This phenomenon might bias the behaviour threshold analysis to understate the eventual outcome that is being investigated and would need to be managed.

Finally, 5) the manner in which questions and possible answers are presented to respondents in a questionnaire might have an effect on the answers they elicit by causing a bias. This could include the ranking of attitudes that a participant has by using traditional Likert scales vs. questions that require direct answers as discussed in 1) above. Traditional Likert scales are based on an uneven number of possible answers, e.g. a five or seven point scale [12]. This presents the respondent with the option to express neutrality by selecting a response exactly in the middle of the scale. For behavioural threshold analysis a neutral answer does not convey any proper information on the personal threshold of a respondent. Traditional scales of reporting are therefore not suited to express either participation or abstinence. Self-reporting questionnaires are thought to cause different

[1] Note on terminology: *Respondent* is used to refer to an individual that completes questionnaires, while *Participant* refer to an individual in an interview or group setting.

biases and also introduce social desirability as previously mentioned [13]. Behavioural threshold analysis in the context of information security is currently unknown to the conventional respondent. With this in mind, traditional questionnaires might not convey enough background or structure for a respondent to confidently reply in the expected fashion. Mechanisms would need to be employed to restructure the approach and guide a respondent through the process.

Pattinson *et al.* [2] confirm the occurrence of social desirability and other issues in questionnaires when comparing different data collection methods for measuring attitudes for information security research. They statistically analyse the outcomes of two different approaches, namely questionnaires and the repertory grid interview technique, and found that both the techniques have merit under different circumstances. Questionnaires provide a way to facilitate quick and easy dissemination of questions to many respondents with the possibility of a large amount of data being acquired, but as mentioned above, questionnaires are prone to biases. The repertory grid technique for interviews is shown to reduce social desirable responses and other biases, but are tedious and time consuming to implement due to the small number of participants that can be accommodated at any given interview as well as interview length. They may however lead to better quality results when compared to questionnaires. Pattinson *et al.* [2] then proceed to advise a combination of the two techniques when attempting to measure attitude. The main difference between these two approaches is self-reporting (when using questionnaires) contrasted with facilitator led reporting (repertory grid technique interviews) [2]. Combining these methods would then require some sort of supervised self-reporting where a facilitator or interviewer would guide the reporting process (as with repertory grid technique interviews) while still maintaining the volumes of responses that one would expect from using a questionnaire to some extent.

In an attempt to combine the two approaches mentioned above and to address the issues 1) to 5) mentioned before, this research employs an optical polling platform for attitude data acquisition. According to a collection of patents, optical polling is the acquiring of feedback from participants by means of a camera and real-time image processing [14, 15]. Each participant is given an object (usually a paper-based encoded pattern) by means of which the participant can provide one of a set of pre-defined responses. The objects are then recognised by a computer system which logs the nominated responses that each participant provides. Very little research on using optical polling for data acquisition for any general research purposes, and indeed none for information security research, currently exists. De Thomas *et al.* [16] and Lai *et al.* [17] describe the use of optical polling as a mechanism for testing student participation and knowledge and getting student feedback, while some individual unpublished lecture and seminar notes also allude to audience interaction with optical polling methods [18-20]. The main advantage of optical polling would be that many participants can be guided through answering a set of questions by a facilitator that is present in the room. This meets the requirements, as set out above, for combining the common data collection techniques. Furthermore, it also helps to address some of the issues in data collection for behavioural threshold analysis e.g. the real-time feedback from participants in order to clarify any uncertainties that may arise due to their understanding of questionnaire items, and may help to limit the effects of social desirability. Another advantage is that due to the interactive nature of optical polling (i.e. facilitated sessions), the questions on behavioural thresholds can be better structured to guide participants in responding in a structured manner, rather than expecting a direct answer on a relatively complex question with little or no context. Other advantages that are specific to behavioural threshold analysis is discussed in Section IV.

The following section describes the methodology that was used to test optical polling as a data collection tool for behavioural thresholds in information security.

III. Methodology

A. Using an optical polling method

The optical polling method that was selected for this research is the Plickers[2] platform [16-20]. Plickers are free to use and can accommodate up to 63 participants. The Plickers website provides functionality to set up multiple choice questions that are answered during the facilitated questionnaire session. The questions are shown on a projector to the participants via the Plickers website where the current question is selected from a mobile device (e.g. a smartphone or tablet) running the Plicker application. The participants then use a Plicker card to nominate their answer to the specific question. Figure 1 shows an example of a typical Plicker card.

Fig. 1. Example of a Plicker card

Note the numbers and letters around the edges of the encoded pattern on the card in Figure 1. The number indicates the card number in the series of cards and shown in Figure 1 is card 1 of 63. Responses are recorded against the specific card number, which in turn (depending on the needs of the researcher) can be linked to a specific participant. The letters indicate the desired response from the participant where the answer (A, B, C or D) is selected by rotating the card so that the corresponding letter is

[2] Plickers available at www.plickers.com

at the top of the card. The card shown in Figure 1 indicates that the answer selected is "A".

When selecting their answer to a question, the participants hold up their cards, taking care that the entire card is visible to the facilitator. The facilitator in turn, takes the mobile device mentioned above and points the device camera towards the group of participants. The live feed from the camera is presented in a real-time, augmented reality fashion showing the number of responses as well as a cursory summary of responses to the facilitator. A hovering indicator is shown next to the card through the view finder when a card has been scanned. The website is then updated to reflect which card number has answered the question and which card's responses are still outstanding. The website can also show a summary of responses to the attending participants.

The general advantages that are conveyed by using optical polling are that social desirability might be reduced as with the repertory grid technique interviews [2]. Questions would most likely not be misinterpreted [11] as any uncertainties may be discussed with the facilitator during the interactive session which in turn should lead to better quality results. The facilitated sessions can accommodate up to 63 participants which is an improvement over the individual interviews described by Pattinson *et al.* [2]. While a facilitated session does mean time spent on the interaction with participants it should be much less than the total time that would be invested in individual interviews. The advantages that this optical polling method encompasses for behavioural threshold analysis is presented in Section IV.

Disadvantages include that participants all have to be present for the facilitated session where the optical polling is conducted. This corresponds to one of the drawbacks [2] of repertory grid technique interviews and is contrary to one of the benefits of self-reporting online questionnaires where respondents can complete the survey at any geographical location and at any time that suit them. The possible number of responses for a specific question is limited to four. As stated above, the available responses are only a choice of responses A-D. This might limit the sensitivity of the responses where more options are needed, especially for Likert scale based questions where a common practise is to use as wide a scale as possible, but narrowing the scale under certain conditions is also commonly done and should not pose an insurmountable problem [12]. Due to the limitation on the type and number of responses it is not possible to conduct any research that require open ended questions when using optical polling in the manner in which it is implemented here. These limitations are not necessarily detrimental for research on behavioural thresholds and can even be beneficial. By limiting the responses to four possible options, participants are compelled to take a stance on the question that is posed to them as there is no choice for a moral middle ground that is often offered by the uneven number of options in classic Likert scales [12]. This stance would typically be for or against a specific information security behaviour.

The following section describes the detail of data collection for behavioural threshold analysis by using optical polling.

B. Data collection

In order to test the feasibility of optical polling as a method for collecting data for information security behaviour research, a questionnaire on information security behavioural threshold questions [11] was posed to a group of participants using Plickers in the manner described in the previous section.

A facilitated questionnaire session was conducted with 35 students enrolled for honours level computer science and information systems at a South African university. The voluntary nature of participation in this research meant that only 23 students elected to participate in the session. To ensure anonymity, the Plicker cards were distributed randomly among the participants with no specific linking of participants to the cards. To be able to track answers on a per participant basis, each card was identified on the Plicker system as only "Participant1" and "Participant2" and so on without any knowledge by the researchers on the eventual user of the card. The session was preceded by an instructional tutorial on the use of Plickers including a trial run of responses on a gender identification question.

Behaviour threshold analysis requires a very specific style of questionnaire to elicit the required responses from participants [21]. Based on the questionnaire used in [11] and based on the understanding gained from the pilot study some changes were made to the approach to adapt the questionnaire to be used in an optical polling setup. Rather than opting for a participant to nominate their threshold value as a percentage as in [11], the participant rates their level of inclination in intervals of threshold values. The behavioural threshold question was based on the use of dubious websites as an example of naïve and accidental internet use [2, 5]. Figure 2 shows the questionnaire that was used in its entirety.

Percentage of others that use torrent sites	How inclined would you be to use torrent sites, given the percentage (%) of others in your group that use torrent sites?			
	Never	Somewhat inclined	Strongly inclined	Always
0—10%	1	2	3	4
11—20%	1	2	3	4
21—30%	1	2	3	4
31—40%	1	2	3	4
41—50%	1	2	3	4
51—60%	1	2	3	4
61—70%	1	2	3	4
71—80%	1	2	3	4
81—90%	1	2	3	4
91—100%	1	2	3	4

Fig. 2. Example of complete behavioural threshold question

The questionnaire in Figure 2 had to be further adjusted to be implemented in an optical polling environment. Each threshold interval was shown to the participants in isolation in order to structure and facilitate the process. Figure 3 shows an example of one of the behavioural threshold interval sub-questions as posed to the participants via the Plickers website during the facilitated session.

ISBN: 1-60132-463-4, CSREA Press ©

If 71-80% of the honours class makes use of torrent sites, how inclined would you be to use torrent sites?

1=Never, 2=Somewhat inclined, 3=Mostly inclined, 4=Always

A:1 B:2 C:3 D:4

Fig. 3. Example behavioural threshold question

The responses that were recorded for the behavioural threshold analysis were answered on a scale of 1-4 which corresponds with the options A-D on the four sides of a Plicker card. An answer of 1 indicates that the participant will have no inclination towards participating in using torrent sites given the indicated number of others that use them, while 4 indicates that the participant is inclined to always participate, given the number of others already participating. Ten versions of the sub-question in Figure 3 was presented with a new 10 % interval for the behavioural threshold value (see Section II and [11]) nominated for each sub-question in order to test all threshold value intervals from 0-100%. This resulted in ten behavioural threshold sub-questions in total. The series of behavioural threshold sub-questions was supplemented by a further eight questions [22] to determine the level of social desirability expressed by the participants in answering the behavioural threshold questions. By measuring the level of social desirability, certain adaptations can be made to the answers of the participants to reflect the true version of events, rather than the reported one. The facilitated questionnaire session, including the introductory instruction, trial question and social desirability questions, took around 20 minutes to complete.

C. Data analysis and interpretation

After completing the facilitated questionnaire session, the resulting responses were tabulated (see [11]) in order to construct a graphic representation for analysing the behavioural thresholds of the participants. The individual thresholds are determined when a participant is willing to participate, given the number of current participants. By nominating a value of either 2 and lower or 3 and higher, the participant indicates willingness to participate or abstain. It is therefore necessary to translate all responses to their extremes, i.e. a response of 2 is translated to the "Never" end of the spectrum to 1 and a response of 3 is translated to a 4 at the "Always" end of the spectrum [11]. This would, however, prove problematic if an uneven number of possible responses were presented to a participant by means of a five point Likert scale where participants have the possibility to choose a neutral response where classification could not be easily achieved. Given this binary classification of responses, and given the four responses that are possible using the Plicker cards, this approach seems to be well suited for the task. After the binary classification of responses were completed, the answers were analysed on a per-respondent basis to determine the behavioural threshold for each participant. The remaining eight questions that were used to measure the level of social desirability were scored and interpreted as instructed in [22]. Nine of the 23 participants exhibited a high level of social desirability. The responses for these participants were adjusted to one notch higher than the self-reported level of inclination to participate. The following sub-section shows the results for both the unadjusted behavioural threshold analysis as well as the analysis where the thresholds were adjusted for social desirability.

D. Results

Snyman and Kruger [11] discuss the method of behavioural threshold analysis in terms of information security in detail and therefore this section will only mention the specifics pertaining to this research. Figure 4 shows the resulting graphical representation of the cumulative thresholds as reported by the participants using Plickers as an optical polling platform.

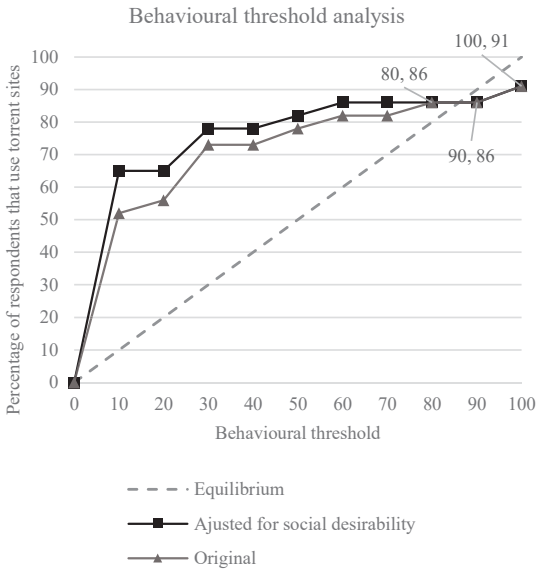


Fig. 4. Behavioural threshold analysis

Based on the original reported figures as designated within Figure 4, a strong initial number of participants with a low threshold for using torrent sites is shown. Over 50% of the respondents indicated they will participate in using torrent sites when only 10% of the group are already participating. The number of participants in the group is likely to continue growing until an equilibrium is reached. The equilibrium point where the graph intersects the equilibrium line is both stable against decrease and stable against further increase, with the preceding and subsequent line segments having a gradient (m) that is less than one ($m=0$ in both cases) [10, 21]. This indicates that given the distribution of individual thresholds, the behaviour of using torrent sites is likely to grow until about 86% of the individuals in the group take part in the behaviour. Once this point is reached the number of participants should become dormant and remain stable, but without an external intervention it will also not show any decline.

Section III-C described a series of questions which were presented to the participants to test the level of social desirability exhibited when answering the behavioural threshold questions. Figure 4 also shows the resulting graph for the adjusted thresholds to correct the responses of the nine participants showing high levels of social desirability. The leftmost part of

the graph shows a higher number of participants exhibiting lower thresholds than initially indicated. This means that more participants are willing to use torrent sites when a lower number of the group are using the torrent sites. To the right of the graph where the equilibrium line is intersected, the resulting equilibrium remains the same as with the original thresholds which were not adjusted for social desirability. This shows that the outcome remains the same but the escalation of the number of partaking participants is quicker than the original threshold analysis indicated. The unchanged outcome, even after adjustment, might indicate that the influence of social desirability might not have been as high as expected. This might be due to the manner in which the data was collected, i.e. by using optical polling as the data collection method.

In the penultimate section (Section IV), a discussion is given on the results presented here.

IV. Discussion

The results obtained by using data collected via optical polling for behavioural threshold analysis seems promising. The cumulative behavioural thresholds presented in the previous section follow the expected conformation when graphically depicted. In the typical plot of cumulative behavioural thresholds, the majority of the reported thresholds reside above the uniformly distributed thresholds which forms the equilibrium line [10, 21]. A stable equilibrium can only be reached when the intersection with the equilibrium line is from above as the gradient of the adjacent line segments cannot be less than one if the intersection comes from below. The latter can indicate a situation where the influence of the group on the individual is negligible as the number of group members exhibiting a behaviour never exceeds their personal threshold [21].

Section III shows results that are somewhat in contrast to the earlier results presented in [11] where the graphic depiction shows only a small allocation of the reported thresholds above the equilibrium line with the bulk falling below it. In [11], equilibrium is reached early on and the problem of password sharing becomes stable with 10% of the group being likely to exhibit this behaviour. These results [11] are said to be an analogical example of the application of behavioural threshold analysis for information security behaviour. This was due to the deviation of the results from the expected form and was attributed to the issues highlighted in Section II.

Using optical polling in this research leads to results that better resemble the expected outcomes from literature than that of [11]. The most notable difference between the two studies is that [11] made use of a self-reporting online questionnaire, while the optical polling method was used in this research. It appears that by changing the data collection method to a hybrid approach as suggested by Pattinson et al. [2], an improvement of the quality of the data that were collected is evident. It simultaneously helps address some of the issues mentioned in Section II: The misunderstanding of the question being presented to individuals. All of the participants can hear the instructions as issued by the facilitator. This ensures that all participants have a uniform understanding of the questions and the process. Participants could directly ask for clarification during the facilitated session if anything was still unclear which means that the question will be answered in the manner and context expected by the researcher; secondly the issue of social desirability seems to be (at least partly) improved. When measuring the social desirability of participants, it was noted that some of them are rated high and are unlikely to supply responses that are truthful. Nonetheless the outcome of the behavioural threshold analysis (at least in this instance) seems unaffected; and finally, optical polling provides a new way in which to structure and present questions to participants which is particularly useful in addressing the unique requirements for behavioural threshold analysis. Forcing a participant to only choose participation or abstinence with the four point scale of the optical polling platform, the issue of neutral answers can be overcome which leads to better interpretability of the data. It helps in organising the data collection process in such a fashion as to assist the participant in understanding and contextualising the questions and guide their responses along the lines of what the researcher would expect. It helps participants answer what they should (the question), rather than what they think they should (their interpretation of the question). The final section concludes this research paper and indicates future directions for optical polling as a data collection method for behavioural threshold analysis.

V. Conclusion

This report shows the first investigation into using optical polling as an innovative data collection method for use in behavioural threshold analysis. The goal of this research was to test the feasibility of the approach and was done by implementing optical polling in the data collection phase of a behavioural threshold analysis experiment in the domain of information security. The motivation for this research was determined by a former study [11] in an ongoing larger project on information security behavioural threshold analysis research.

Optical polling addresses some of the common data collection issues for information security research, but more importantly it addresses some of the issues that are unique to behavioural threshold analysis (see Sections II and VI). The results of behavioural threshold analysis that were obtained when using optical polling for data collection closely resemble that which is expected from literature. This indicates that optical polling solves some of the data quality complications that were experienced in earlier behavioural threshold analysis experiments.

As with any other data collection approach, optical polling is not an infallible solution and cannot be seen as a silver bullet to address all the problems relating to behavioural threshold analysis. For traditional information security research, some general issues remain unanswered. For instance where it is physically impossible to have the participants together in one venue due to geographical or scheduling issues, the optical polling approach would not be suited. In this instance a self-reporting (possibly online) questionnaire would remain the instrument of choice. Also where more in-depth interviews with individual participants are required (e.g. for qualitative research), repertory grid interviews remain the preferred data collection mechanism. The problems which are specific to behavioural threshold analysis which still remained unanswered

are indicated for inclusion in future work. This includes an investigation to determine the suitability of the information security topic that is used in questioning to determine behavioural thresholds. Choosing the correct topics remain cardinally important in ensuring the legitimacy of the behavioural thresholds that are measured; and finally the current studies on behavioural threshold analysis in information security and related data collection will be extended to include real-world applications thereof in an industry setting in order to extensively test these concepts.

REFERENCES

[1] S. Furnell, N. Clarke, M. R. Pattinson, and G. Anderson, "How well are information risks being communicated to your computer end-users?," *Information Management & Computer Security,* vol. 15, pp. 362-371, 2007.

[2] M. Pattinson, K. Parsons, M. Butavicius, A. McCormac, and D. Calic, "Assessing Information Security Attitudes: A comparison of two studies," *Information & Computer Security,* vol. 24, pp. 228-240, 2016.

[3] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers & security,* vol. 24, pp. 124-133, 2005.

[4] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," *European Journal of Information Systems,* vol. 18, pp. 151-164, 2009.

[5] D. Calic, M. Pattinson, P. K., M. Butavicius, and A. McCormac, "Naïve and Accidental Behaviours that Compromise Information Security: What the Experts Think " in *Tenth International Symposium on Human Aspects of Information Security & Assurance*, Frankfurt, Germany, 2016, pp. 12-21.

[6] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *computers & security,* vol. 32, pp. 90-101, 2013.

[7] S. Furnell and K. Thomson, "Recognising and addressing 'security fatigue'," *Computer Fraud & Security,* vol. 2009, pp. 7-11, 2009.

[8] R. J. Fisher, "Social desirability bias and the validity of indirect questioning," *Journal of Consumer Research,* vol. 20, pp. 303-315, 1993.

[9] W. D. Kearney and H. A. Kruger, "Theorising on risk homeostasis in the context of information security behaviour," *Information & Computer Security,* vol. 24, pp. 496-513, 2016.

[10] M. Granovetter, "Threshold models of collective behavior," *American Journal of Sociology,* vol. 83, pp. 1420-1443, 1978.

[11] D. P. Snyman and H. A. Kruger, "Behavioural thresholds in the context of information security," in *Tenth International Symposium on Human Aspects of Information Security & Assurance*, Frankfurt, Germany, 2016, pp. 22-32.

[12] I. E. Allen and C. A. Seaman, "Likert scales and data analyses," *Quality progress,* vol. 40, p. 64, 2007.

[13] E. D. Frangopoulos, M. M. Eloff, and L. M. Venter, "Human Aspects of Information Assurance: A Questionnaire-based Quantitative Approach to Assessment," in *Eighth International Symposium on Human Aspects of Information Security & Assurance*, 2014, pp. 217-229.

[14] N. R. Amy and S. R. Amy, "Optical polling platform methods, apparatuses and media," US Patent 9,098,731 B1, issued August, 4, 2015.

[15] W. F. Thies, A. C. Cross, and E. B. Cutrell, "Audience polling system," US patent 2,014,004,092,8 A1, issued February, 6, 2014.

[16] J. R. de Thomas, V. López-Fernández, F. Llamas-Salguero, P. Martín-Lobo, and S. Pradas, "Participation and knowledge through Plickers in high school students and its relationship to creativity," in *UNESCO-UNIR ICT & Education Latam Congress 2016*, Bogota, Colombia, 2016, pp. 113-123.

[17] C.-H. Lai, S.-H. Huang, and Y.-M. Huang, "Evaluation of Inquiry-based Learning with IRS in the Technique Course: A Pilot Study in Taiwan Industrial High School," in *44th Annual Conference of the European Society for Engineering Education*, Tampere, Finland, 2016.

[18] J. Bacon and B. Ward. (2015, 2017-03-07). *The Horizon Report 2015 with Audience Participation Using Paper Clickers* [Presentation slides]. Available: http://scholarspace.jccc.edu/cgi/viewcontent.cgi?article=1129&context=c2c_sidlit

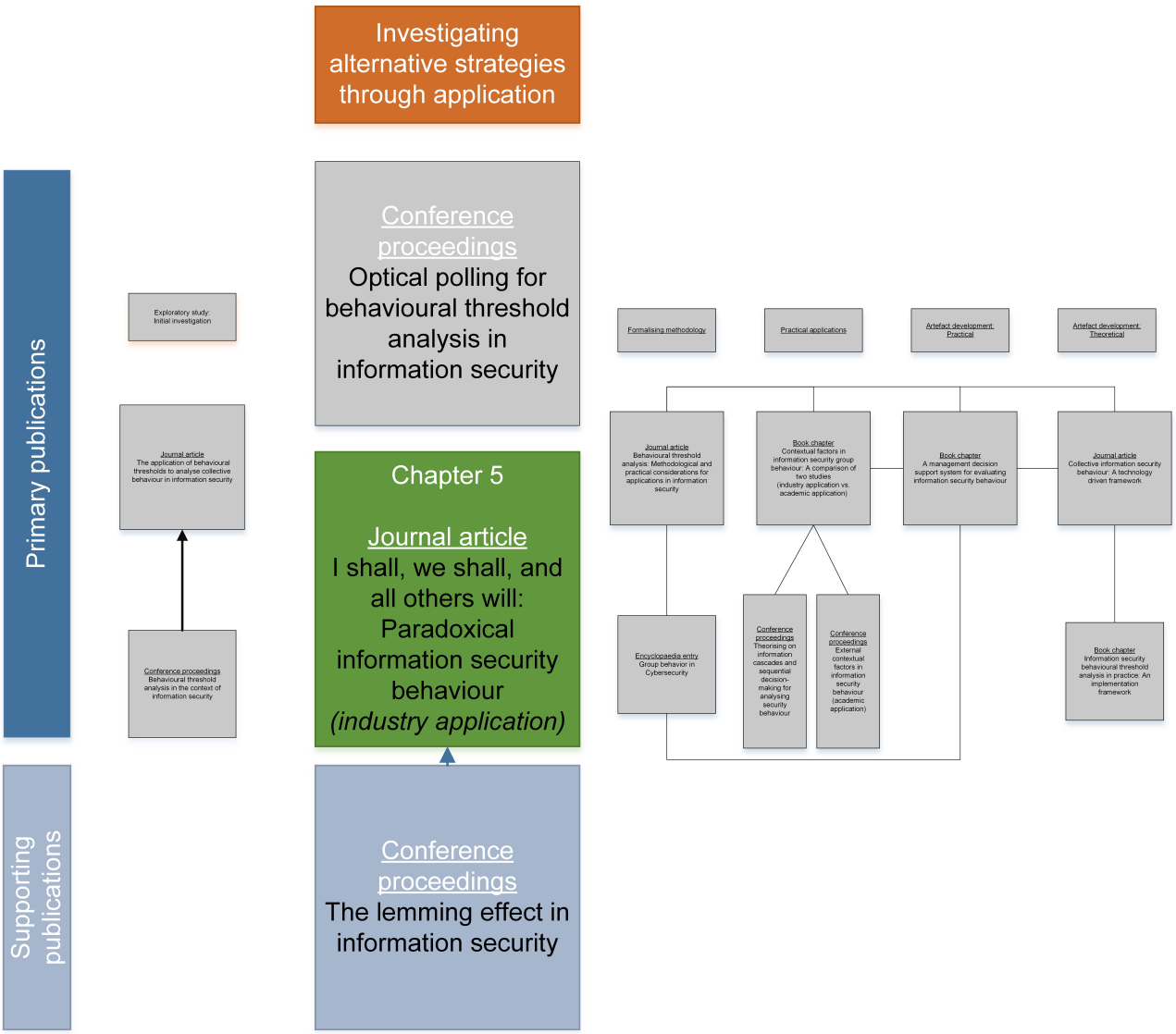
[19] L. J. Darcy and S. James. (2015, 2017-03-07). *Take IT to the Next Level: Moving from Item Teaching to Authentic Instruction* [Presentation slides]. Available: http://www.doe.virginia.gov/instruction/english/professional_development/institutes/2015/elementary/darcy_and_james/presentation.pdf

[20] M. Taylor. (2016, 2017-03-07). *Raise your Cards-A look at Plickers in an Adult Learning Environment* [Presentation slides]. Available: http://scholarspace.jccc.edu/context/c2c_sidlit/article/1205/type/native/viewcontent

[21] J. S. Growney, "I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior," ed: Modules in Undergraduate Mathematics and Its Applications - Tools for Teaching, 1983, pp. 108-137.

[22] J. J. Ray, "The reliability of short social desirability scales," *The Journal of Social Psychology,* vol. 123, pp. 133-134, 1984.

Chapter 5
-
Article III: I shall, we shall, and all others will: Paradoxical information security behaviour



Chapter table of contents

5.1 Preamble to Article III 83

5.2 A note on the authors 84

5.3 Emerald journal style requirements 84

5.4 Article III 84

5.4.1 Introduction 85

5.4.2 Behavioural threshold analysis 87

5.4.3 Application of behavioural threshold analysis 88

5.4.4 Results 91

5.4.5 Discussion 96

5.4.6 Conclusion and future work 98

5.4.7 References 98

5.1 Preamble to Article III

Continuing the second phase of the research (*Investigating alternative strategies through application*), this chapter comprises the subsequent attempt to improve on the quality of the data that is used to support behavioural threshold analysis in information security. The focus of the previous article was on enhancing the data collection method, *i.e.,* optical polling, to obtain better data on which to base behavioural threshold analysis. In this article, the unique and specialised requirements for a behavioural threshold analysis measurement instrument and the importance of identifying the correct information security topics to evaluate are reiterated. Drawing once more from literature for guidance, information security focus areas are identified and tailored questions are developed for the specific application of behavioural threshold analysis. Other studies have found that the presentation of the questions has an influence on how the respondents perceive the questions and ultimately how truthfully they respond to these questions. The premise is that correctly framing the questions can help alleviate the occurrence of the social desirability bias. It remains, however, a possibility that a respondent still does not answer in a manner that reflects his/her true inclinations towards following the example of security group behaviour. To this end, a formal scheme for evaluating social desirability is described and included in the approach to allow researchers to control for social desirability in the responses.

Given the aforementioned, Article III in this chapter incorporates the data collection recommendations from Article II, Chapter 4, and addresses the question framing issues that were identified in Article I, Chapter 3, into the first full-scale application of behavioural threshold analysis in an industry setting. The research exercise was conducted with 63 respondents at a utility company in a departmental setting to firstly, assess the current state of information security in the organisation for six identified security focus areas, and secondly, to test the amalgamation of new ideas to enhance the approach. A reflection is provided on the success of the exercise and the specific implications for the organisation, as well as the implications for behavioural information security in general.

Article III was first published in the peer-reviewed conference proceedings of the *International Symposium on Human Aspects of Information Security & Assurance*. This 11th instalment of the conference was held in Adelaide, Australia from 28-30 November 2017. The paper was entitled *The lemming effect in information security*[6] and is available in Appendix C. The conference chairs once more identified the work as novel and of a high standard and again invited the contribution to be extended for publication in the *Information & Computer Security* journal (Volume 26, Issue 3)

[6] Snyman, D. P., Kruger, H. A., & Kearney, W. D. 2017. *The lemming effect in information security*. In Clarke, N. L. & Furnell, S. M. Eds., Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017), Adelaide, Australia, pp. 91-103..

under the title *I shall, we shall, and all others will: Paradoxical information security behaviour*[7] in April 2018.

5.2 A note on the authors

These two papers include a third author, Dr WD Kearney, who, at the time of writing and publication, was an industry partner and extraordinary professor in the former School of Computer, Statistical, and Mathematical Sciences at the North-West University. Dr Kearney assisted with the measurement instrument application and data collection activities within the targeted organisation.

5.3 Emerald journal style requirements

The requirements of the journal specified that the *Emerald Harvard* referencing style be used. The article is presented in its final edited and typeset form as it was published in the journal. Information regarding the author guidelines of the journal can be found in Appendix F.

5.4 Article III

Article follows on next page.

[7] Snyman, D. P., Kruger, H. A., & Kearney, W. D. 2018. I shall, we shall, and all others will: Paradoxical information security behaviour. *Information & Computer Security*, 26(3):290-305.

The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/2056-4961.htm

Received 26 March 2018
Revised 26 March 2018
Accepted 17 April 2018

I shall, we shall, and all others will: paradoxical information security behaviour

Dirk P. Snyman
School of Computer, Statistical and Mathematical Sciences, North-West University, Potchefstroom, South Africa

Hennie Kruger
Department of Computer Science, North-West University, Potchefstroom, South Africa, and

Wayne D. Kearney
North-West University, Currambine, Australia

Abstract

Purpose – The purpose of this paper is to investigate the lemming effect as a possible cause for the privacy paradox in information security.

Design/methodology/approach – Behavioural threshold analysis is used to test for the presence of the lemming effect in information security behaviour. Paradoxical behaviour may be caused by the influential nature of the lemming effect. The lemming effect is presented as a possible cause of the privacy paradox.

Findings – The behavioural threshold analysis indicates that the lemming effect is indeed present in information security behaviour and may lead to paradoxical information security behaviour.

Practical implications – The analysis of the lemming effect can be used to assist companies in understanding the way employees influence each other in their behaviour in terms of security. By identifying possible problem areas, this approach can also assist in directing their information security education endeavours towards the most relevant topics.

Originality/value – This research describes the first investigation of the lemming effect in information security by means of behavioural threshold analysis in practice.

Keywords Information security, Human behaviour, Behavioural threshold analysis, Lemming effect, Privacy paradox

Paper type Research paper

1. Introduction

Humans play an integral part in all the phases of technology utilisation; from the initial development to the intended use of technology, the human factor is an inexorable aspect that needs to be managed on many levels. One of the more prominent factors where humans play a vital role is in the protection of technological systems (Evans *et al.*, 2016). This protection of systems is twofold: First, humans implement technological security that is developed to protect systems from unauthorised access and intrusion. Systems become enveloped in a cocoon of technology so that all but those who are authorised may gain entry. Second, those who are duly authorised to have access are entrusted to keep their access private so that no other may intrude upon that which is theirs to guard. On the first account, the security of systems is well thought-out. The protections are methodical, well-designed and near

Information & Computer Security
Vol. 26 No. 3, 2018
pp. 290-305
© Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-03-2018-0034

impossible to penetrate. It is on the second account where the true vulnerability of systems lies. The human is untrustworthy and relinquish their control over their own small, albeit very important, part of the system's security defences at the drop of a hat. Often, this is unwittingly, the human is fooled into relinquishing control to another. Other times the human is set on abusing their access for personal gain.

This interaction has prompted an avenue of research that aims to study the phenomenon of the human and its relation to information security. Human aspects of information security studies often aim to investigate the underlying behaviour of the users that interact with information technology systems (Pham *et al.*, 2017).

However, human behaviour does not provide a consistent variable to measure. Quite often, behaviour is unpredictable and does not seem to conform to expectations. For a specific human, their behaviour and, more specifically, reasons for behaviour are not always clear, even to themselves. Studies indicate that the individual's intention and attitude towards behaviour does not always lead to the same behaviour (Egelman and Peer, 2015) and that the eventual behaviour can be contradictory to what their intention was (Barth and de Jong, 2017). This discrepancy between the intention and/or attitude and the behaviour they ultimately exhibit is often called the privacy paradox (Hallam and Zanella, 2017; Kokolakis, 2017; Egelman *et al.*, 2016). Even in an early study of users' internet experience, Brown (2001) has already noted the paradox in how privacy and security is maintained, both online and offline. Though an individual's privacy is important to them, they would still be willing to sacrifice their privacy for very little benefit. This paradox is also observed in other information security behaviours and not only in matters of privacy as its name suggests, e.g. not reporting security incidents when it is known that reporting is expected.

In a study on group behaviour, Granovetter (1978) noted that paradoxical behaviour can be linked to the influence that group behaviour has on an individual. In terms of information security, Snyman *et al.* (2017) have conceptualised this influence as an occurrence of the so-called "lemming effect". The lemming effect refers to the propensity of individuals to follow the behaviour of a group blindly even when the behaviour is assuredly dangerous (Wiedermann *et al.*, 2014). The term is derived from the behaviour of lemmings (small rodents) that are purported in popular culture to follow migration behaviour of the group blindly, even walking off cliffs in droves only to fall to their deaths. In terms of information security, this would involve individuals following the group example in their information security behaviour.

Even though many previous studies exist that investigate information security behaviour (Crossler *et al.*, 2013; Warkentin *et al.*, 2011) and many behavioural theories (i.e. protection motivation theory, theory of planned behaviour, theory of reasoned action, etc.) have been developed that are often used as basis for these studies (Sommestad *et al.*, 2014), there still seems to be room for further exploration. For instance, Dang-Pham *et al.* (2017) argue that these previous studies chiefly focus on individualistic cognition of employees and supply limited contextual details. Furthermore, results and findings are also subject to the theoretical assumptions of the theories used in the studies (Dang-Pham *et al.*, 2014).

Given the importance of information security and the apparent shortage on approaches that include contextual details, this paper reports a practical application to evaluate the lemming effect as a possible explanation for the privacy paradox by including the context of co-workers instead of focusing on individual cognition on its own. The method that is used to study the lemming effect is based on the application of threshold models of collective behaviour (Granovetter, 1978) and was influenced by the theory of planned behaviour (Snyman and Kruger, 2017a). This method is applied to a large utility corporation in Australia.

The use of behavioural threshold analysis in information security has not been applied in practice before. This paper forms part of a larger research project where the feasibility of behavioural thresholds in information security is investigated. Snyman and Kruger (2017a, 2016) initiated the use of behavioural threshold analysis in information security by testing the approach in their exploratory research. They presented the proof of concept as a feasible approach to information security behaviour analysis. This was succeeded by a study on effective data collection methods for threshold analysis (Snyman and Kruger, 2017b). These studies serve as the basis for this research and were used as iterations to refine the process and methodology of behavioural threshold analysis in information security. This current paper differs from the aforementioned initial exploratory research therein that this is the first report on the first application of behavioural threshold analysis in information security to be put into practice.

The remainder of the paper serves to describe the process and is structured as follows: Section 2 presents an introductory background on behavioural threshold analysis. Section 3 describes the application of behavioural threshold analysis in information security, with specific reference to the methodology and experimental setup. The results, which were obtained for the experiment described in Section 3, are presented in Section 4 and discussed in Section 5. Finally, Section 6 concludes this report and looks towards future directions for this research.

2. Behavioural threshold analysis

The concept of behavioural thresholds, as well as threshold analysis, will only be revisited briefly in this section to serve as background information as the concepts were already presented in detail in the previous papers. For a more in-depth review, see Snyman and Kruger (2016).

The foundational idea of behavioural thresholds as presented by Granovetter (1978) is that each individual in a group possesses an internal decision-making mechanism for following group behaviour. This mechanism weighs the personal cost versus gain of participation in the group behaviour, given the number of other group members that are already engaged in the behaviour. The mechanism expresses the willingness to participate as the number of other group members who should already be participating in the behaviour before the possible gains outweigh the cost for the individual. This is called the individual's behavioural threshold. When it is known to the individual that more group members are participating in the group behaviour than the number represented by their personal threshold, they will also participate in the group behaviour. This corresponds to the lemming effect that was mentioned in the Introduction. Granovetter (1978) explains the working of the mechanism using an analogy as follows: within a group of workers in an organisation, a rumour might start circulating. An individual might pay little attention to the credibility of the rumour if it is heard from only one source. When more sources impart the same rumour to the individual, the rumour gains credibility because the number of sources is larger than before. The individual's internal mechanism then determines that if the credibility reaches a critical threshold, i.e. enough sources share the rumour, the individual will also believe and circulate the rumour. The individual's threshold has been exceeded and they will take part in the group action. Therefore, the individual has theoretically succumbed to the lemming effect. The individual might act in a manner that is contrary to their better judgement because they simply cannot help but follow the group example. In the same way, the lemming effect causes the same paradoxical behaviour in information security, e.g. if enough members of a group share their passwords with other members and the number exceeds an individual's threshold for participation, the individual

will also share their password with others even when they know that they are not supposed to. An individual that acts in contradiction of their own good sense is a typical example of the privacy paradox.

To show the working of the model in action and illustrate the advantages thereof, the model was applied in practice, and the following section presents the methodology that was followed.

3. Application of behavioural threshold analysis

The behavioural threshold analysis exercise was conducted with 63 respondents from a large utility corporation. From the existing structures at the corporation, three groupings of employees were identified, i.e. permanent staff, contractors and management. Participation in this study was voluntary and the questionnaire had a specific consent section in line with acceptable practice. All information supplied by the respondents was strictly anonymous. Ethical clearance for the exercise was obtained from the human resources department and the CEO. Each respondent completed an online questionnaire on their willingness to perform certain information security actions, given the number of others whom also perform the actions.

The application of behavioural threshold analysis to analyse group behaviour in information security presents a unique challenge in terms of the measurement instruments used to gather the relevant behaviour data (Snyman and Kruger, 2017b). This is both in terms of the topics of information security questions that are posed to respondents and how these questions are presented typographically. For the purposes of this application, six questions were posed to the respondents (Table I).

The questions were based on focus areas and topics identified from the human aspects in information security questionnaire (HAIS-Q) (Parsons *et al.*, 2017; Parsons *et al.*, 2014). The six focus areas that are shown are neither exclusive nor extensive but serve to illustrate the suitability of a focus area and related question for behavioural threshold analysis. Depending on the intention of the specific behavioural threshold analysis exercise that is to be conducted, different suitable focus areas (for instance, mobile computing) may be identified. For instance, the first focus area and related question in Table I is in contrast to the others, as it describes positive behaviour, i.e. volunteering for information security training. This focus area and question was added as a control to test the willingness of the

Table I. Information security questions for behavioural threshold analysis

Focus area	Information security behaviour threshold question
1. Security training	How inclined would you be to also complete voluntary information security training, given the percentage of staff that have completed voluntary information security training?
2. Social media use	How inclined would you be to also spend excessive work time on social media, given the percentage of staff that spend excessive work time on social media?
3. Incident reporting	How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?
4. Internet use	How inclined would you be to also access dubious websites from devices connected to your company network, given the percentage of staff that regularly access dubious websites from devices connected to your company network?
5. Email use	How inclined would you be to also open any unfamiliar email attachments, given the percentage of staff that normally open any unfamiliar email attachments?
6. Password management	How inclined would you be to also share passwords, given the percentage of staff that share their passwords?

respondents to follow others in their behaviour if there was no negative connotation to performing the behaviour. Furthermore, the focus areas of the HAIS-Q are divided into questions that address different aspects of the themes. The password management focus area has questions on "password sharing", "re-using passwords" and "strong passwords" (Parsons *et al.*, 2017). Depending on whether a study has an interest in these specific aspects, they may also be included. However, special attention should be given to the number of questions that are included as each question necessitates ten new responses. Owing to the number of responses, adding an extra question places a relatively higher burden on the respondent in comparison with traditional questionnaires. The number of questions is also contrasted to traditional approaches where multiple questions are used to test a given aspect (Sekaran and Bougie, 2010). The nature of this model only allows for one question per aspect: Will you participate if enough others do?

Each of the questions from Table I was answered on a scale of inclination for participation in the specific information security activity, given the percentage of other group members that are known to partake in the activity. An example is presented in Table II.

It should be noted that the sample size in this exercise does not follow traditional style for questionnaires which can be summarised as "the more the better". Because of the unique nature of behavioural threshold analysis, it is specifically done in smaller groups. The members of the group have to be aware of the habits and behaviour of others in order to answer the questions about their own thresholds (Growney, 1983). When sample sizes become too large (i.e. start to extend beyond the natural boundaries of organisational departments) the group members no longer have the awareness that is crucial for the correct application of the model and the probability of incorrect answers increases.

As mentioned earlier in Section 2, the threshold for an individual is the number (percentage) of others that have to exhibit a specific behaviour before they will join in. If a respondent indicated that they would be somewhat inclined to participate, given the percentage of the group that do so, that percentage was taken as their individual threshold. This was noted for each respondent, and the aggregate of all the respondents' thresholds was used for the behavioural threshold analysis results (Section 4).

In the earlier, related studies, it was noted that the results might have been affected by social desirability and was ascribed to the sensitive nature of the information security questions being asked, as well as how familiar the respondents were with the topics (Snyman and Kruger, 2017a, 2017b, 2016). Social desirability refers to the tendency that

Table II.
Example of a complete behavioural threshold question

Percentage of staff that ignore security incidents by not reporting them (%)	How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?			
	Never	Somewhat inclined	Strongly inclined	Always
0-10	1	2	3	4
11-20	1	2	3	4
21-30	1	2	3	4
31-40	1	2	3	4
41-50	1	2	3	4
51-60	1	2	3	4
61-70	1	2	3	4
71-80	1	2	3	4
81-90	1	2	3	4
91-100	1	2	3	4

many respondents have to answer questions in a manner that they think to be acceptable rather than truthful (Fisher, 1993). It was therefore deemed necessary to control for this phenomenon to obtain a more accurate view on the predicted group behaviour. A series of additional questions was given to the respondents after completion of the behavioural threshold questionnaire to determine the level of social desirability that they exhibit. The questions to measure social desirability were based on a standardised 33 question measurement instrument which was developed by Crowne and Marlowe (1964) and later shortened to eight questions by Ray (1984). These eight questions were used to measure social desirability in this research. They are presented in social desirability questions (Ray, 1984) below.

3.1 Social desirability questions

Q1. Are you always courteous, even to people who are disagreeable?

Q2. Are you always a good listener, no matter whom you are talking to?

Q3. Are you quick to admit making a mistake?

Q4. Have there been occasions when you took advantage of someone?

Q5. Do you sometimes try to get even rather than forgive and forget?

Q6. Do you sometimes feel resentful when you do not get your own way?

Q7. Are you always willing to admit when you make a mistake?

Q8. Have you sometimes taken unfair advantage of another person?

The social desirability questions are simply answered with Yes, No or Unsure. Depending on the specific question either Yes or No will be awarded a score of one or three respectively. Unsure is always scored two. The scores for all of the questions are added together for a score out of a possible 24. The higher the score, the higher the likelihood is that the respondent's answers were influenced by social desirability. For the purposes of this study, only the extreme score of 24 is taken to mean that the respondent was not truthful in the way in which they answered the questions. If a respondent was deemed untruthful, their answers on the information security questions were adjusted towards a higher level of inclination for participation (Table II). The level of willingness for participation was adjusted one level higher, i.e. if a respondent with a social desirability of 24 selected their inclination of participation as *somewhat inclined (2)* it was adjusted to *strongly inclined (3)*. This would mean that the individual's threshold for participation is taken at a lower percentage in the cases where the behaviour is seen as a negative information security action. The reverse holds true for positive information security behaviours where the respondents might overstate their willingness for participation. In these cases, the threshold for participation is taken at a higher percentage. For all of the questions in this study, both the adapted and the original thresholds are considered to illustrate the effect of the adaptation.

The information security behavioural threshold analysis exercise was executed as explained above and following an analysis of the collected data, the results are presented in the following section.

4. Results

This section shows the aggregation of the information security behavioural threshold analysis results that were obtained from the respondents for each of the questions in Table I. The results are presented in a graph format. These graphs represent a plot of the cumulative behavioural thresholds for a corresponding question plotted against a uniform distribution of thresholds called the equilibrium line. The shape of the behavioural threshold graph and the intersection with the equilibrium line allows for an interpretation that may predict a percentage of members of the group that may eventually participate in the relevant information security behaviour. It should be noted that a detail analysis of all the nuances conveyed by the graph is omitted and only the crux of the analysis is presented. An overview of other measures and analyses (e.g. information conveyed by gradient measurement of the graph) is presented in Snyman and Kruger (2017a).

From the result for the six questions in Table I, it is possible to classify their outcome as being either one of three distinct cases. The cases are representative of situations where:

(1) Individuals tend to follow the positive information security behaviour of others because of low thresholds for participation. The lemming effect therefore has a high impact.

(2) Individuals are easily influenced to follow the negative information security behaviour of others; in other words, individuals exhibit low thresholds for participation and therefore a high lemming effect is present.

(3) Individuals are not easily convinced to follow the bad information security behaviour of others; in other words, where individuals exhibit high thresholds for participation.

The lemming effect in this case is low. The results are presented one by one in this order.

4.1 Following positive behaviour (low threshold – high lemming effect)

Figure 1 shows the cumulative results for the groups' individual thresholds towards question 1 from Table I (hereafter referred to as *Q1*):

Q1. How inclined would you be to also complete voluntary information security training, given the percentage of staff that have completed voluntary information security training?

Information security training (*Q1*) is an example of a positive influence that members of the group have on one another in the context of information security training. The steep incline and rapid growth in the cumulative behavioural thresholds indicates a high willingness (i.e. low thresholds) in the members of the group to follow the example of others to also participate in voluntary information security programs. The intersection with the equilibrium line indicates that if the status quo is sustained that the percentage of members that voluntarily participate in security training programs is likely to grow until 93 per cent of the group takes part. The situation is then unlikely to change, as the distribution of thresholds reaches satiety at this point.

By including an example question on positive information security behaviour, the lemming effect can be considered in two directions. From the number of respondents that indicate that they will follow positive behaviour, the instinct of the model is ratified, i.e. they are willing to follow behaviour, even if they were not necessarily inclined to the behaviour in the first place.

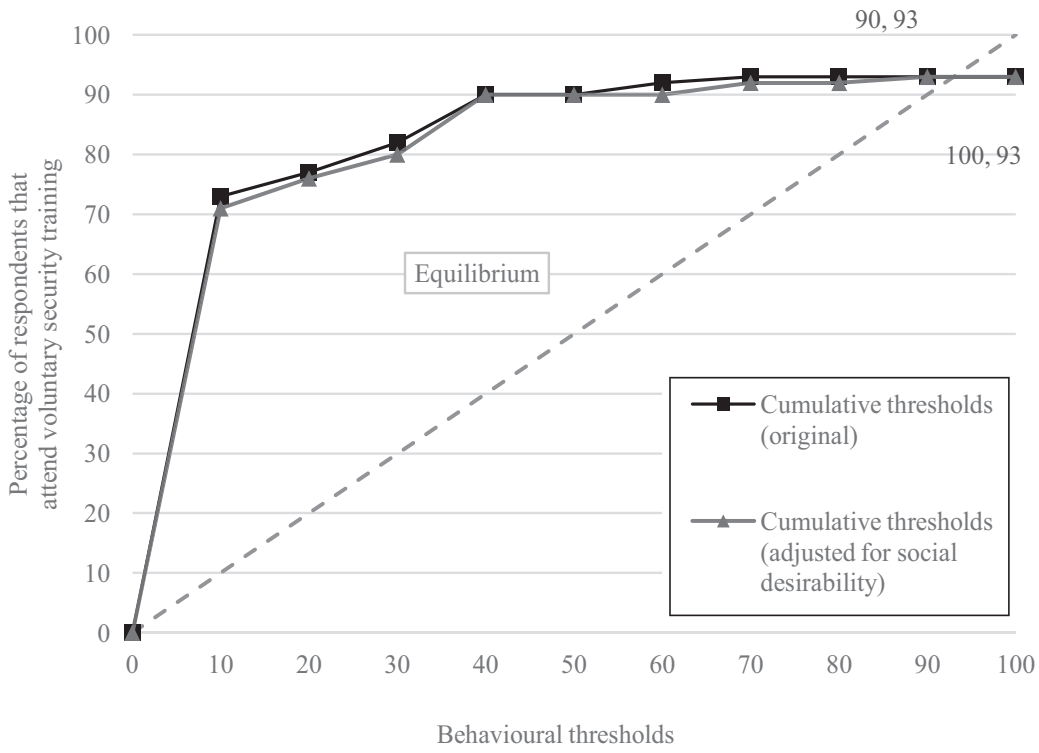


Figure 1. Distribution of behavioural thresholds for information security training (*Q1*)

4.2 Following bad behaviour (low threshold – high lemming effect)

The paradoxical information security behaviour in this category is illustrated by the results for two of the questions. First, in the case of social media use:

Q2. How inclined would you be to also spend excessive work time on social media, given the percentage of staff that spend excessive work time on social media?

Second, for incident reporting:

Q3. How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?

The recorded thresholds for participating in-group behaviour were noted to be low and individuals are therefore likely to follow the group in its behaviour. These are examples where the influence of the group would be considered negative. Participation in the behaviour is not recommended as a good practice to promote high levels of information security.

Figures 2 and 3 show the cumulative behavioural threshold graph for the responses to the two questions above.

The willingness for participation of the group in using both excessive work time for social media and ignoring security incidents is moderate (i.e. they have low to medium thresholds for participation). The thresholds indicate that a number of the individuals are probably going to participate in the group behaviour. In Figure 2, the social media use behaviour (*Q2*) reaches an equilibrium state with only around 12 per cent of the group participating. This distribution of thresholds satisfies the requirements for equilibrium and the participation rate is unlikely to change unless there is some external influence, like an intervention, that changes the group dynamic. This analysis is based on the original thresholds as reported by the participants.

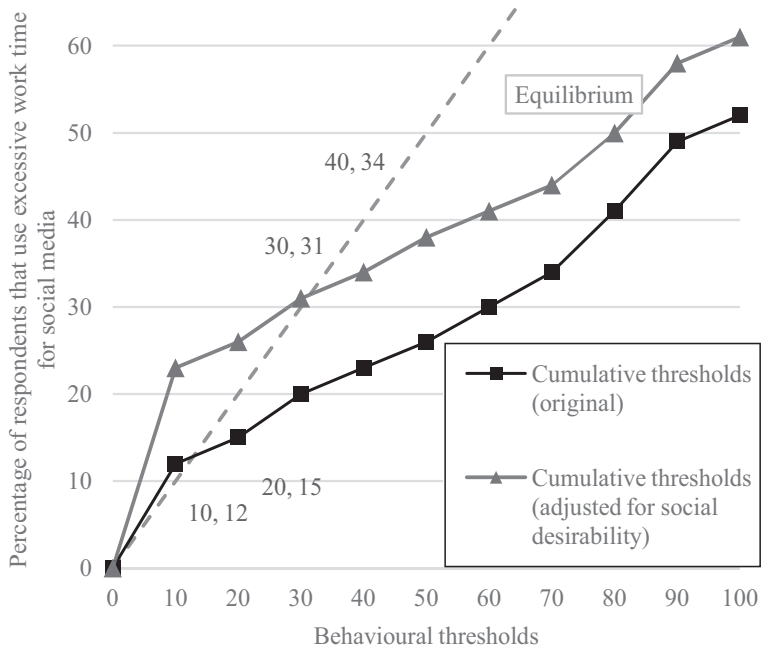


Figure 2.
Distribution of behavioural thresholds for social media use (*Q2*)

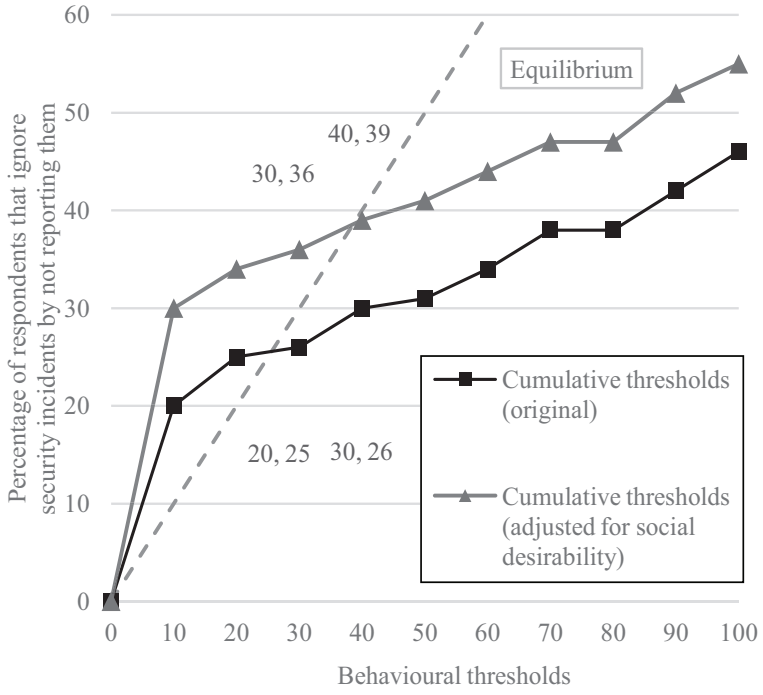


Figure 3.
Distribution of behavioural thresholds for incident reporting (*Q3*)

When the effect of social desirability is considered, the rate of participation stabilises at 31 per cent of the group participating.

Similar to the pattern noted for *Q2*, the graph for incident reporting (*Q3*) indicates that participation in the group behaviour should be around 26 per cent of the group participating. Correcting for social desirability changes the outlook where participation in the behaviour stabilises with 39 per cent of the members of the group participating.

This number of participants in both these behaviours may be considered problematic even though the participation rates do not predict a majority of the group participating. The individuals show low thresholds for both the questions, and the lemming effect appears to be high. Individuals with low thresholds are likely to follow the bad example of others in contradiction to their existing knowledge of right and wrong. This kind of behaviour is in accordance with the premise of the privacy paradox. Topics on social media and incident reporting might be reviewed by the corporation and its importance reaffirmed through security awareness campaigns.

4.3 Rejecting bad behaviour (high threshold – low lemming effect)

The remaining three questions illustrate this final category: First,

Q4. How inclined would you be to also access dubious websites from devices connected to your company network, given the percentage of staff that regularly access dubious websites from devices connected to your company network?

In the second instance:

Q5. How inclined would you be to also open any unfamiliar email attachments, given the percentage of staff that normally open any unfamiliar email attachments?

The third and final question is:

Q6. How inclined would you be to also share passwords, given the percentage of staff that share their passwords?

In all the three questions, the individuals demonstrate high thresholds. The lemming effect is low and is therefore of little consequence in these behaviours.

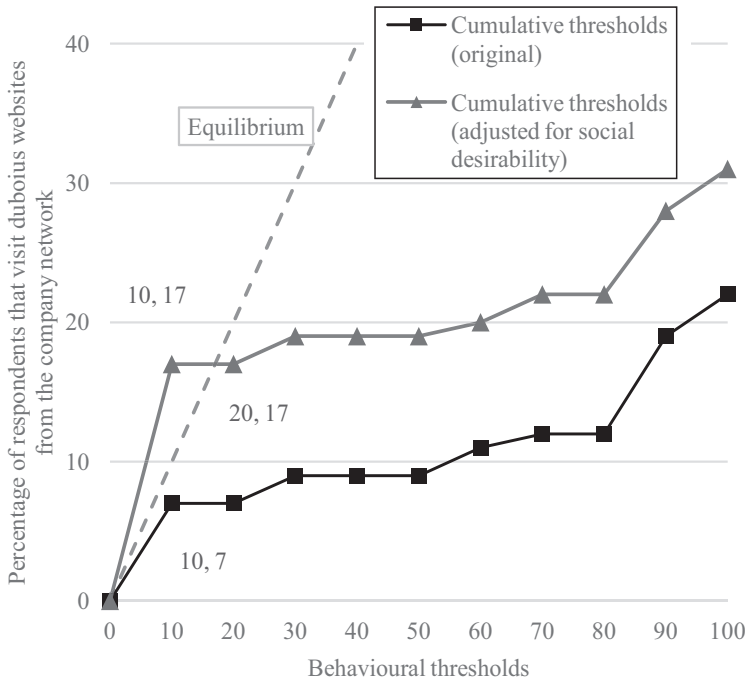


Figure 4. Distribution of behavioural thresholds for internet use (*Q4*)

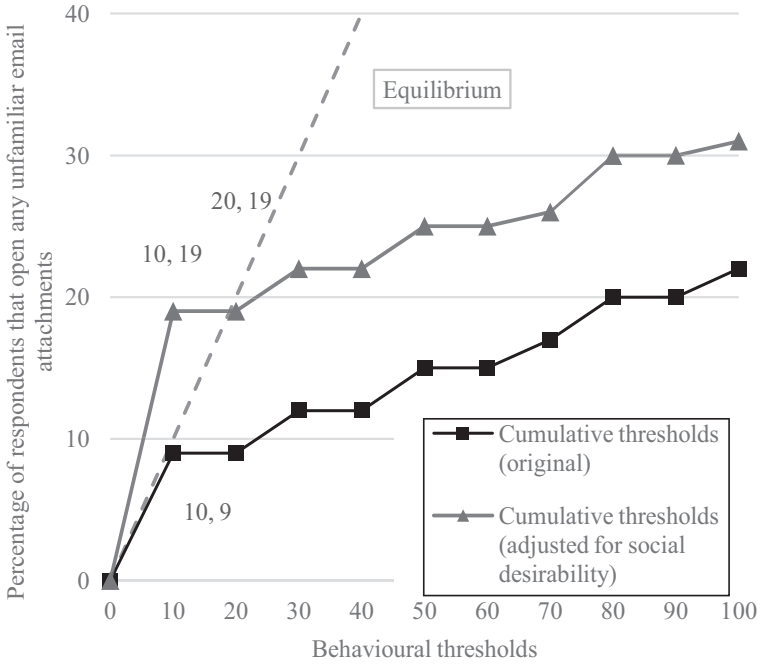


Figure 5.
Distribution of behavioural thresholds for email use (*Q5*)

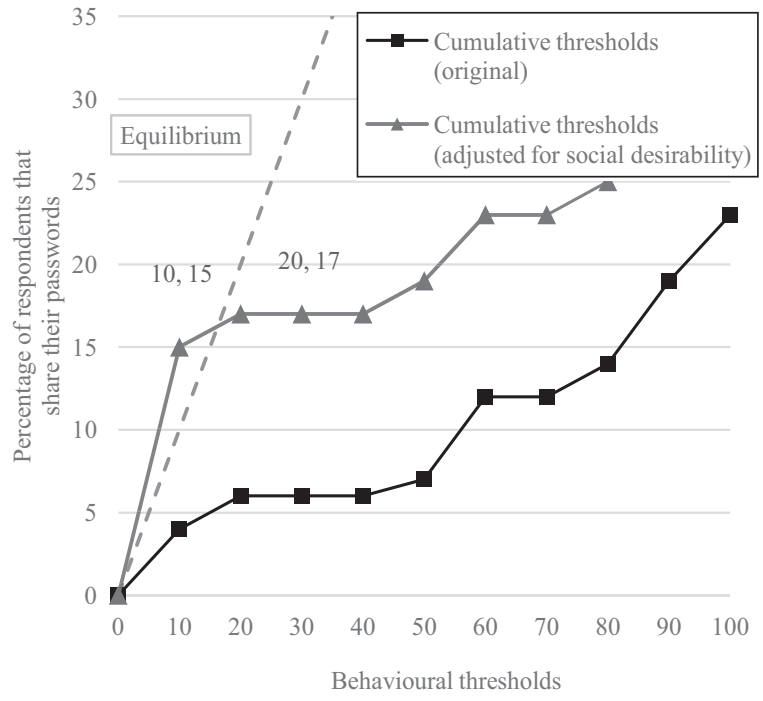


Figure 6.
Distribution of behavioural thresholds for password management (*Q6*)

The cumulative threshold plots in Figures 4, 5 and 6, based on the original responses for each behaviour, never intersect the equilibrium line. This is because of the very high personal thresholds that each of the individuals in the group has against participating in the group behaviour.

Whenever there is no intersection with the equilibrium line, the group behaviour is said to be in decline. The behaviour will never reach a stable state which indicates that there will be no uptake by the group, other than an unsuccessful instigator, in

participating in the behaviour. The behaviour should also ultimately decline among the instigators because of the non-conformance of the group. The lemming effect should therefore work in reverse and convince the instigators to change their behaviour for the better. Such an occurrence of non-equilibrium is also called a "dying problem" (Growney, 1983).

Considering the effect of social desirability, the outlook changes somewhat. The adjusted behavioural thresholds plot intersects the equilibrium line with 17 per cent of the group participating in accessing dubious websites from the corporation network. Similarly, the behaviour reaches equilibrium with participation rates of 19 and 17 per cent for *Q5* and *Q6*, respectively.

This discrepancy indicates that there may be more individuals that are inclined to participate in these behaviour than what was reported. The overall trend for their behavioural thresholds, however, remains high. The relatively low percentages for participation indicate that these behaviours are less likely to occur than category one behaviours. Inclusion of topics relating to *Q5* and *Q6* in security awareness programs might be reconsidered in favour of more pressing issues. By leaving out topics in which the worker corps is already aware of might help to prevent security fatigue and ensure that the topics that are included in the training are reflected on with the required reverence.

5. Discussion

Based on the results that are reported in Section 4, this section provides a twofold overview. A discussion is presented in terms of issues relating to this specific research exercise and then remarks of a more general nature relating to behavioural threshold analysis and the privacy paradox caused by the lemming effect is presented.

5.1 Specific remarks

The group that was surveyed in this study is shown to be well versed in good information security behaviour. They furthermore exhibit a willingness to be team players in positive behaviour that promotes information security. Despite the predominantly positive results, there are still some security topics where the negative influence of the lemming effect is observed.

Although only six information security focus areas (each with one related question) are covered in this study, the results show significant findings, and definitive recommendations can be made. Three categories of results were postulated. The first category describes the willingness of individuals to follow positive security behaviour of others. This result was illustrated by the question on voluntary information security training (*Q1* in Figure 1). The individuals exhibit low thresholds for participation, i.e. they will readily also participate. It follows logically that individuals would be willing to follow the example of positive behaviour and therefore the result indicates that the model is intuitively correct.

The second category is where thresholds for participation are low and a strong lemming effect is present, i.e. individuals are willing to follow the negative group behaviour. Examples of this category are social media use (*Q2*) and incident reporting (*Q3*) where low thresholds and the strong influence of the group lead to paradoxical information security behaviour. The lemming effect causes individuals to act in a manner that is contradictory to their better judgement. It was observed that 31 per cent (*Q2*) and 39 per cent (*Q3*) of the group is likely to be inclined to participate in negative information security practices. These focus areas, particularly incident reporting, are generally not as frequently addressed as the

more conventional focus areas, e.g. password management and email use. It is therefore to be expected that the levels of awareness for these focus areas should be lower and that the individuals should more easily follow the example of others. This expectation is sensible and, given the corroborating results for this category, once more suggests that the logic and intuition of the model is sound. It is therefore advisable to introduce a specific focus on these behaviours in information security awareness programs, the percentages should see a decrease. The results for this category have shown that the group is willing to participate in such programs, even doing it voluntarily. This should contribute to the success of security awareness programs that are conducted in the corporation.

The final category is defined as individuals having high personal thresholds for participation, and the lemming effect is not pronounced enough to have a measurable effect. In the related information security focus areas, the individuals are not swayed to participate in negative group behaviour. This category and the accompanying high thresholds were observed for internet use (*Q4*), email use (*Q5*) and password management (*Q6*). The low lemming effect does not lead to paradoxical behaviour in these cases. Password, internet, and email risks are topics that are typically well known. It can be assumed that they are regularly addressed by management. It should then be reasonable to expect that the individuals should be resistant against participation. The results show that the higher levels of awareness in these cases lead the individuals to reject participation in these behaviours. By rejecting the behaviour, the individuals act as they were expected to. This further serves to confirm that the intuition of the model is based on verifiable reasoning and that behavioural threshold analysis gives good results.

It was also interesting to note that the respondents exhibit high levels of social desirability. The average social desirability score for the participants was measured at 19/24. Such a high score indicates that there is a high probability that the respondents did not answer the questionnaire in a completely truthful manner. High social desirability might indicate that the respondents overstated their positive information security behaviour and understated the negative behaviour that they would rather present in a better light. This can be attributed to the sensitive nature of the information security topics included in the questionnaire. The individual might also already be aware of expected behaviour and answers in accordance thereto.

5.2 General remarks

The results show that the individual in a group is likely to follow the majority example in specific cases with reference to group information security behaviour. This indicated that the lemming effect is indeed present and, when analysed, can be useful to help evaluate group information security behaviour. This helps to understand the privacy paradox and provide a possible explanation for its occurrence. A high lemming effect indicates that an individual should easily follow the behaviour of others. The individual might be aware that the behaviour should not be followed, but following the group becomes more important because of the group exceeding the individual's threshold for participation.

Behavioural threshold analysis provides a formal measure to capture contextual information for an individual's security behaviour concerning the behaviour of co-workers. This context provides a broader view on information security behaviour than the traditional focus on individual cognisance. By measuring the lemming effect and predicting probable group behaviour, it provides a tool to identify possible risk areas. The identified risks can help focus the efforts of information security awareness programs. Focussed awareness programs will also help individuals to

focus on their behaviour as to avoid the privacy paradox. A concerted effort to reflect on their training before acting could indeed provide heightened levels of information security.

Given the positive contributions of behavioural threshold analysis, there are some points that still warrant careful consideration. Collecting data for behavioural threshold analysis poses a unique challenge to elicit useful answers from respondents. As mentioned earlier, the sensitive nature of information security questions often leads to high levels of social desirability. By tailoring the data collection instrument for this specific application, the occurrence of social desirability can be somewhat addressed. Furthermore, the uniqueness of the instrument does not allow it to be tested for statistical validity and reliability as with traditional questionnaires. This is because of the specific manner in which the questions are structured to determine the respondent's behavioural threshold. The answers that the respondents provide may also vary to a large degree where they are often completely willing to follow the behaviour of others or completely opposed to it. Another factor to keep in mind is the relative levels of influence that different members of the group have. An individual might be more inclined to follow the example of friends or prominent figures as opposed to just another employee they barely know.

6. Conclusion and future work

This paper presented the first application of information security behavioural threshold analysis to measure the lemming effect in practice. The lemming effect is shown to be a possible cause for the privacy paradox because of the influence of group behaviour on the individual. Given the number of factors that have an influence on this analysis, the results should be handled carefully. Further research into these topics is warranted. Consideration might be given to other social theories that explain the influence of a group on an individual such as social capital theory and social cognition theory. The aforementioned notwithstanding, the results indicate the presence of the lemming effect in information security behaviour and that the effect can be measured with the use of behavioural threshold analysis as presented in this research. Furthermore, the results give a good indication of the levels of security awareness of the group in question and helps determine areas in which awareness still needs development. In conclusion, it is therefore in the light of the lemming effect and the privacy paradox that because one individual initiates a behaviour (I shall), more individuals will join in (we shall) and participation grows until all the members of the group also participate (all others will).

References

Barth, S. and De Jong, M.D. (2017), "The privacy paradox – investigating discrepancies between expressed privacy concerns and actual online behavior – a systematic literature review", *Telematics and Informatics*, Vol. 34 No. 7, pp. 1038-1058.

Brown, B. (2001), "Studying the internet experience", *Technical Report (HPL-2001-49)*, HP Laboratories, Bristol.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers & Security*, Vol. 32, pp. 90-101.

Crowne, D.P. and Marlowe, D. (1964), *The Approval Motive*, Wiley, New York NY.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2014), "Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach", *25th Australasian Conference on Information Systems (ACIS), Auckland, New Zealand*.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2017), "Applications of social network analysis in behavioural information security research: concepts and empirical analysis", *Computers & Security*, Vol. 68, pp. 1-15.

Egelman, S. and Peer, E. (2015), "Scaling the security wall: developing a security behavior intentions scale (Sebis)", *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, ACM*, pp. 2873-2882.

Egelman, S., Harbach, M. and Peer, E. (2016), "Behavior ever follows intention? A validation of the security behavior intentions scale (SEBIS)", *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ACM*, pp. 5257-5261.

Evans, M., Maglaras, L.A., He, Y. and Janicke, H. (2016), "Human behaviour as an aspect of cybersecurity assurance", *Security and Communication Networks*, Vol. 9 No. 17, pp. 4667-4679.

Fisher, R.J. (1993), "Social desirability bias and the validity of indirect questioning", *Journal of Consumer Research*, Vol. 20 No. 2, pp. 303-315.

Granovetter, M. (1978), "Threshold models of collective behavior", *American Journal of Sociology*, Vol. 83 No. 6, pp. 1420-1443.

Growney, J.S. (1983), "I will if you will: individual thresholds and group behavior – applications of algebra to group behavior", *Modules in Undergraduate Mathematics and Its Applications – Tools for Teaching, COMAP, Bedford, MA*, pp. 108-137.

Hallam, C. and Zanella, G. (2017), "Online self-disclosure: the privacy paradox explained as a temporally discounted balance between concerns and rewards", *Computers in Human Behavior*, Vol. 68, pp. 217-227.

Kokolakis, S. (2017), "Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon", *Computers & Security*, Vol. 64, pp. 122-134.

Parsons, K., Mccormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers & Security*, Vol. 42, pp. 165-176.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., Mccormac, A. and Zwaans, T. (2017), "The human aspects of information security questionnaire (HAIS-Q): two further validation studies", *Computers & Security*, Vol. 66, pp. 40-51.

Pham, H., Brennan, L. and Richardson, J. (2017), "Review of behavioural theories in security compliance and research challenge", Cohen, E. (Ed.), *Proceedings of the Informing Science and Information Technology Education Conference, Vietnam*, Informing Science Institute, Santa Rosa, CA, pp. 65-76.

Ray, J.J. (1984), "The reliability of short social desirability scales", *The Journal of Social Psychology*, Vol. 123 No. 1, pp. 133-134.

Sekaran, U. and Bougie, R. (2010), *Research Methods for Business: A Skill Building Approach*, John Wiley & Sons, Hoboken, NJ.

Snyman, D.P. and Kruger, H.A. (2016), "Behavioural thresholds in the context of information security", *Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016), Plymouth University, Frankfurt*, pp. 22-32.

Snyman, D.P. and Kruger, H.A. (2017a), "The application of behavioural thresholds to analyse collective behaviour in information security", *Information and Computer Security*, Vol. 25 No. 2, pp. 152-164.

Snyman, D.P. and Kruger, H.A. (2017b), "Optical polling for behavioural threshold analysis in information security", *The International Conference on Information and Knowledge Engineering (IKE'17), CSREA Press, Las Vegas*, pp. 39-45.

Snyman, D.P., Kruger, H.A. and Kearney, W.D. (2017), "The lemming effect in information security", *Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017), Plymouth University, Adelaide*, pp. 91-103.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management & Computer Security*, Vol. 22 No. 1, pp. 42-75.

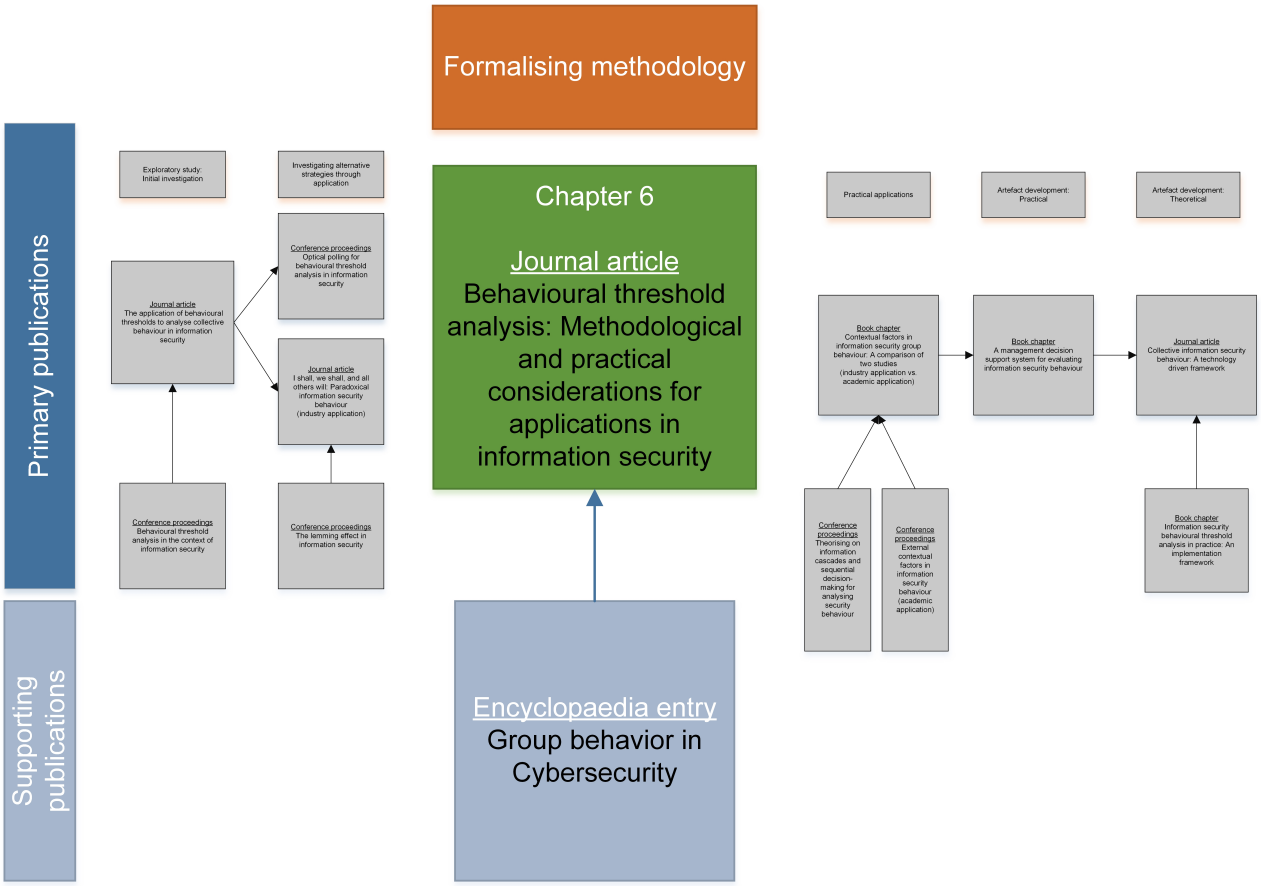
Warkentin, M., Johnston, A.C. and Shropshire, J. (2011), "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention", *European Journal of Information Systems*, Vol. 20 No. 3, pp. 267-284.

Wiedermann, W., Niggli, J. and Frick, U. (2014), "The lemming-effect: harm perception of psychotropic substances among music festival visitors", *Health, Risk & Society*, Vol. 16 No. 4, pp. 323-338.

Corresponding author
Hennie Kruger can be contacted at: hennie.kruger@nwu.ac.za

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**

Chapter 6
-
Article IV: Behavioural threshold analysis: Methodological and practical considerations for applications in information security



Chapter table of contents

6.1 Preamble to Article IV 103

6.2 Taylor & Francis journal style requirements 104

6.3 Article IV 104

6.3.1 Introduction 105

6.3.2 Related work 107

6.3.3 Information security behaviours 110

6.3.4 Example information security questions for behavioural threshold analysis 111

6.3.5 Illustrative case studies 113

6.3.6 Proposed methodology 115

6.3.7 Validation 117

6.3.8 Reflection 119

6.3.9 Conclusion 120

6.3.10 References 121

6.1 Preamble to Article IV

As described in the Research Design section in Chapter 1, design science research is concerned with the creation of artefacts that contribute to the creation of new knowledge that benefit the scientific body of evidence. As such, part of this research is to develop artefacts to this effect. Distinction is made between two classes of artefact in this research, *i.e.,* practical and theoretical artefacts. A practical artefact refers to an instantiation of the underlying theory and which contributes to the practice of the specific research field, *e.g.* a software implementation or system. In comparison thereto, a theoretical artefact can be a novel contribution to the field that does not take a practical form, but contributes new knowledge and formalises practical processes, *e.g.* a new methodology (as described in this chapter) and framework (Chapter 10) that are developed in this study.

In the article in this chapter, the focus shifts from the aforementioned first applications of behavioural threshold analysis in information security and the exploratory nature thereof, to properly establishing the method. This leads in the new research phase of *formalising methodology*. Behavioural thresholds are a novel and unique way to assess information security group behaviour. As such, no set of guidelines exist to guide applications and the accompanying data collection. By formalising the methodology and creating guidelines for successfully implementing the approach in practice, the method is made available to a wider audience of information security researchers and practitioners alike. This contributes to the body of knowledge of behavioural information security and is therefore the first of the two theoretical artefacts in this research. It allows others to use the methods as is and, ideally, expand on this work.

In this light, an analysis of the specialised requirements for such a measurement instrument is presented in Article IV and concrete recommendations on the content and presentation of information security topics are made in this context. This includes both the wording and orthography of the related questions and how they are presented. The orthography of the eventual presentation of the measurement instrument presented in this chapter draws on the principles of repertory grid interviews. An example of the resulting measurement instrument is presented in Appendix K. Literature has shown that the presence of an interviewer causes research participants to be more truthful in their responses to interview questions. However, given the nature of behavioural threshold analysis, such an interview approach is not feasible but some of the fundamental principles do translate well into the unique requirements that the application of the threshold approach demands. Once again, in this article, the researcher draws on the experiences gleaned through the work presented in the previous chapters to formalise the methodology and practical strategy for applications of behavioural threshold analysis in

information security. The preceding articles in Chapters 3-5 are formally assessed as case studies. These serve as the basis for the recommendations for an established methodology and future applications in practice. Article IV was submitted to *Behaviour & Information Technology* and accepted for publication in its 38th Volume, 11th Issue, after successfully clearing the peer-review process. The ensuing paper, entitled *Behavioural threshold analysis: Methodological and practical considerations for applications in information security*[8] was published in January of 2019.

6.2 Taylor & Francis journal style requirements

The requirements of the journal specified that the *Taylor and Francis Custom Citation* referencing style be used. The article is presented in its final edited and typeset form as it was published in the journal[9]. Information regarding the author guidelines of the journal can be found in Appendix H.

6.3 Article IV

Article follows on next page.

[8] Snyman, D. P., & Kruger, H. A. 2019. Behavioural threshold analysis: Methodological and practical considerations for applications in information security. *Behaviour & Information Technology*, 38(11):1-19.

[9] Correction – In Article IV, the captions for Figures 4 and 5 were switched in the published version of the article. The error was corrected in the version of the paper that is included here.

BEHAVIOUR & INFORMATION TECHNOLOGY
2019, VOL. 38, NO. 11, 1088–1106
https://doi.org/10.1080/0144929X.2019.1569163

Taylor & Francis
Taylor & Francis Group

Check for updates

Behavioural threshold analysis: methodological and practical considerations for applications in information security

Dirk Snyman and Hennie Kruger

School of Computer Science and Information Systems, North-West University, Potchefstroom, South Africa

ABSTRACT

The application of behavioural threshold analysis to analyse group behaviour in information security presents a unique challenge in terms of the measurement instruments and methodology used to gather relevant attitude data. This paper presents an analysis of the specialised requirements for such a measurement instrument and makes methodological recommendations on the content and especially presentation of information security topics in a measurement instrument for this context. A comparison between existing methods and the specific requirements for threshold analysis is presented and serves as the main rationale for the suggested methodology. The recommended methodology and subsequent measurement instrument were implemented and experimentally tested in case studies to gauge their feasibility. Applications of behavioural threshold analysis in information security that follow the recommended methodology suggested in this article performed satisfactorily and elicits cause for further real-world experimentation.

ARTICLE HISTORY
Received 18 May 2018
Accepted 24 December 2018

KEYWORDS
Measurement instrument; behavioural threshold analysis; information security; behaviour; attitude

1. Introduction

Human aspects remain an important component of information security. Measuring and quantifying the human aspect, however, remains a difficult task (Connolly et al. 2016). A new proposed approach to analyse information security behaviour based on the attitudes of individuals in an organisation, is the behavioural threshold analysis technique (Snyman and Kruger 2016). The general application of behavioural threshold analysis on group behaviour was first presented by Granovetter (1978). Forming part of a larger research project, initial exploratory studies on the application of behavioural threshold analysis in information security show that this approach may help to determine attitudes and behaviours of individuals in a group setting on specific information security topics in order to help evaluate the risk associated with these topics (Snyman and Kruger 2016, 2017a). Furthermore, behavioural threshold analysis was also determined to be helpful in the construction of information security awareness programmes and also helps gauge the level of saturation that these awareness programmes have within an organisation. The inextricable connection between attitude and behaviour was once more confirmed in the application of behavioural threshold analysis for information security topics in the earlier studies (Ifinedo 2012; Snyman and Kruger 2016, 2017a; Sommestad and Hallberg 2013). The analyses in the mentioned studies suggest solutions to the unique problems in terms of the questions that have to be asked to individuals to determine their attitude towards specific information security topics. These attitudes are used to construct a collective representation of the ultimate behavioural thresholds within an organisation for the specific topic under assessment. The exploratory studies mentioned above have been previously conducted on the application of behavioural threshold analysis in the context of information security and has determined its value as an instrument to analyse collective behaviour. What remains absent is that there has not been a specific concentration on information security focus areas and the related information security questions that have to be asked for each focus area to determine individual thresholds.

Behavioural threshold analysis presents a unique challenge and differs from conventional information security awareness research and as such has very specific needs for the type of related security questions and how these questions are presented (Snyman and Kruger 2016, 2017a). For instance, typical behavioural threshold analysis requires a mechanism to elicit individual threshold values expressed as a percentage or number of group members. Specifically, for information security

CONTACT Dirk Snyman dirk.snyman@nwu.ac.za School of Computer Science and Information Systems, North-West University, 11 Hoffman Street, Internal box 107, Building G3 - Office G03, Potchefstroom 2531, South Africa

© 2019 Informa UK Limited, trading as Taylor & Francis Group

research, these threshold values are in terms of sensitive information security behaviours. The method of response available to the respondent is also a unique issue in behavioural threshold analysis. It remains to be determined whether threshold values should be answered in a direct response, or whether the thresholds should be presented as intervals with respondents indicating levels of agreement.

Question structure is another factor and includes how the question is worded, presented and set out. The sensitive nature of the questions leads to social desirability being a specific problem that needs to be kept in mind when determining which topics to include in questioning and how questions are presented. Another specific issue is asking the minimum number of questions but retaining the maximum coverage of risk types. Special attention to the questions that are asked is moreover due to the requirement that people need to be aware of other people's information security behaviour (Growney 1983). This means that only certain kinds of question can be asked and not just any of the information security questions that have been previously determined. Therefore, specific attention has to be given to questions about information security behaviour that is not conducted in secret where others will not know about the behaviour, but rather behaviour that is conducted openly where others can be aware thereof.

From the argument above, the specialised prerequisites for a specific methodology for creating a measurement instrument for behavioural threshold analysis is evident and is formalised in the following problem statement:

> *Due to the unique requirements of an information security threshold application, traditional information security measurement instruments are insufficient and need considerable adaptation to determine behavioural thresholds.*

Existing approaches to behavioural threshold analysis have been tested in earlier work by applying them in information security (Snyman and Kruger 2017a). From the earlier work, the opportunity to improve upon the existing method became evident. This indicates that there is a definitive gap in the current state of research where this study can make a valuable contribution.

Therefore, the current research aims to answer the following research question:

> *Can a unique information security behavioural threshold measuring instrument be developed that will address the special nature and requirements of a behavioural threshold analysis methodology in the context of information security?*

In order to guide the study to answer the research question above, it is divided into the following three sub-questions that address the unique requirements of behavioural threshold analysis in the context of information security:

- *How should sampling be conducted for behavioural threshold analysis in information security?*
- *Which aspects should be considered in terms of question design for behavioural threshold analysis in information security? and*
- *Which factors should be provided for to ensure the validity of data collection for behavioural threshold analysis in information security?*

The aim will be achieved by formulating and motivating some basic information security questions to measure attitude (and behaviour) in some common information security focus areas. Specific reference will be made to the presentation of these questions to respondents and the requirements of behavioural threshold analysis. The research that is presented in this paper specifically differs from the previous work in that the initial inquiries aimed to test the feasibility of the behavioural threshold analysis approach for information security. The approach was found to provide promising insights and now this study presents part of the process to fine-tune the methodology to contribute to its maturity. The main contribution of this research is that it provides a methodology for the construction of a measurement instrument for behavioural threshold analysis for applications in information security.

The structure of the remainder of this paper is presented as follows: In **Section II**, a cursory background is given on the human aspect in information security, as well as behavioural threshold analysis and its application in information security. In **Section III**, an overview of the most prominent forms of information security behaviour is presented. In **Section IV**, some examples of specific questions for behavioural threshold analysis are provided, while in **Section V**, case studies are presented to illustrate their use. The proposed methodology is presented in **Section VI**. Exercises that validate the proposed methodology are described in **Section VII.** Finally, in **Section VIII** a reflection on the study is presented and in **Section IX** the findings of this research are summarised and future directions for the application of behavioural threshold analysis in the context of information security are anticipated.

2. Related work

As explained in Section I, this research forms part of a series of articles in an overarching research project on behavioural threshold analysis and its application in the field of information security. As such, only a high-level overview of the related human aspects in information technology and general behavioural threshold concepts is provided in this section.

2.1. The human aspect in information technology

Human aspects in information security have been identified as one of the core aspects (alongside organisational and technical facets) that form part of the process to ensure the fidelity and protection of information systems within an organisation (Safa, Von Solms, and Futcher 2016). For the most part, technical and organisational issues pertaining to information security have been thoroughly thought through and addressed and continue to be effectively managed in organisations (Scholl, Leiner, and Fuhrmann 2017). The human aspect, however, is still to be as successfully managed as these other core aspects. This is due to a relative ineptitude of organisations and their managing structures to identify and control the human factor, as it is a complex and ever-changing phenomenon. The human factor within an organisation is often said to be directed by the collective organisational culture that is based on the attitudes, norms and behaviours of the individuals that make up the organisation (Ashenden 2008). This is also the case with information security culture, which is driven by the same collective outlook that the individuals in an organisation express towards information security policies and practices (Da Veiga and Martins 2017; Dhillon, Syed, and Pedron 2016). Their communal attitude towards policies and other security measures often determines whether these controls can be effectively implemented to protect the information assets of the organisation or could, on the other hand, cause them to fail. Attitude is a common antecedent for behaviour (Ajzen 1991; Fazio 1990) and as such the topic of attitudes in information security has received much attention in recent studies (Cuganesan, Steele, and Hart 2018; Ifinedo 2012; Nguyen and Kim 2017; Snyman and Kruger 2016; Sommestad et al. 2014). Attitude towards compliance with information security policies should determine the eventual actions that the individuals in a group perform, either following or disregarding these policies. The corroboration of the link between attitude and behaviour has been formalised by the expression thereof in terms of theoretical models.

One of the better-known models is the theory of planned behaviour, first described by Ajzen (1991). This model shows the influence that the attitude towards behaviour has on an individual's intentions, which is ultimately expressed in his/her behaviour. The theory of planned behaviour has been used to contextualise many studies in information security behaviours and attitudes (Al-Omari, El-Gayar, and Deokar 2012; Ifinedo 2012; Pattinson et al. 2016; Snyman and Kruger 2017a; Sommestad and Hallberg 2013). Another influential model for attitude and behaviour in information security is the knowledge, attitude and behaviour model (Kaur and Mustafa 2013; Kruger and Kearney 2006; Parsons et al. 2014). An example of this model would be the knowledge that a person has about information security policies influencing his/her attitude about information security topics, which in turn determines the actions (behaviour) that the person takes when confronted with information security challenges. Measuring attitude (linked to behaviour) in terms of information security remains a challenging endeavour. Two of the more common approaches to measuring attitudes is by using self-reporting questionnaires, such as the HAISQ (Parsons et al. 2014; Parsons et al. 2017) and the use of repertory grid technique interviews (Pattinson et al. 2016; Pattinson et al. 2015).

2.2. Behavioural threshold analysis

The idea of behavioural threshold analysis stems from the initial model presented by Granovetter (1978) in which the collective behaviour of a group of people is said to be based on the individual's attitude towards participating in a group activity, given his/her awareness of the proportion of others in the group that participate in the activity. The attitude is said to be expressed in terms of the number of members in the group that have to participate in a certain action before the individual will be inclined to also partake. This is said to be the individual's threshold for participation (Granovetter 1978). The behavioural threshold model can theoretically be applied to any situation where a group is confronted with a contrasting decision, for instance the spreading of a rumour. If a rumour is heard by an individual X from one person in a group, he/she might discard the information as being untruthful due to an inherent level of naiveté or lack of evidence. Contrarily, if the rumour is heard from enough other persons in the group (i.e. individual X's threshold of participants in spreading the rumour is exceeded), individual X will accept the rumour and also start spreading it due to the perceived credibility the number of members of the group that spread it add to the rumour.

Group behaviour in information security can also be expressed as two contrasting courses of action, i.e. a binary decision (Snyman and Kruger 2017a) and therefore presents the opportunity to implement behavioural threshold analysis. Based on the collective information security activities of the members in a group, and the individual's attitude (threshold level) towards also participating in those activities, a prediction of the eventual information security actions of the group can be made. This prediction is based on the analysis of the individual thresholds according to the behavioural threshold analysis model. The analysis, using the model, is only possible when the individual thresholds for information security actions of the members of a group are known (Granovetter 1978). As such, a mechanism of eliciting threshold information from the members is needed. The aforementioned threshold value of an individual is directly determined by the individual's attitude towards participation in the group action.

Growney (1983) suggests a questionnaire as the instrument for gathering the individual thresholds from a group for any group activity situation. The questionnaire is structured in a very specific way where respondents choose their preferred outcomes and nominate their own threshold values for participation. The questionnaire was used in an earlier, related study (Snyman and Kruger 2016) to test the application of the behavioural threshold model for information security. Figure 1 shows an example information security question similar to the one, which was presented to respondents in Snyman and Kruger (2016) in the format, which was suggested by Growney (1983).

The respondents were tasked with nominating their threshold value for sharing their passwords with others. The threshold was expressed as a percentage of group members that would need to share their passwords with others before the respondent would also do so. The results obtained for the initial experiments in Snyman and Kruger (2016) did not follow the expected trends seen from literature. This indicated that there are some problems with the measurement instrument in its current form.

In an attempt to improve the behavioural threshold approach for information security, the results from Snyman and Kruger (2016) were critically analysed in another related study (Snyman and Kruger 2017b) and some key issues were identified that need to be addressed to help improve the feasibility of the behavioural threshold analysis approach in this context. Snyman and Kruger (2017b) investigated a novel alternative to the questionnaire as the measurement instrument for information security thresholds by employing an optical polling method for data collection. The suggested optical polling method could address some of the issues, but under certain circumstances, it would remain beneficial to employ a questionnaire as the instrument of choice (for instance different geographical locales, etc.). Issues that were identified that are specific to questionnaires on behavioural thresholds in information security and are relevant to this research are reiterated here for context and motivation for the aim of this study. Data collection for behavioural threshold analysis requires a unique method of questioning. The initial questionnaire wording and structuring created confusion, which led to respondents misunderstanding the question and answering incorrectly, possibly due to the following causes:

- For behavioural threshold analysis (especially when applied to information security), the topics that are used in questioning need to be suitable and well thought out. The choice of the topic (password security) that was used previously might have failed to yield the expected results due to the familiarity that respondents could have had with recommended practices for the topic;

Questionnaire

1. Choose one of the following outcomes that is preferable:
   a. A situation where no student will share his/her password with any other student.

   –OR–

   b. A situation where every student is free to share his/her password with any other student.
2. Regardless of the outcome selected above, respond to one of the following statements:
   a. I will never share my password with another student.

   –OR–

   b. I will share my password with another student when at least ***x*** percent of students shares their passwords. (nominate a value for ***x***)

Figure 1. Behavioural threshold questionnaire adapted from Growney (1983).

– Due to the sensitive nature of the typical information security topic, respondents tend to either over-, or understate their attitudes towards the behaviour of others who deal with these subjects. They wish to portray a version of themselves that is more socially acceptable than their actual self. This tendency is called social desirability (Fisher 1993) and it is especially important in a setting where the influence of members in a group on each other is expected. A group setting in itself is essentially a social situation, regardless of whether the group is an organisational or friendly one. Individuals' perceived social identities and group membership determine that they would be very susceptible to social desirability, presenting themselves as they would want to be perceived in an attempt to fit in with the group (Tanis and Postmes 2005).

The effect of the social desirability bias, albeit in a general sense, is seen in the work of Dahlgren and Hansen (2015) in the tourism sector. They report that respondents gave biased answers when asked questions about their opinion of a country when they perceive that the interviewer has the same nationality as said country. The bias is attributed to respondents *not wanting to offend* the interviewer. If the country and nationality are not the same, they tend to be more honest because their social perception dictates that the interviewer will not feel offended in this instance. See also the works of Van de Mortel (2008) on social desirability in health research, and Dodou and De Winter (2014) on social desirability in online, offline and paper surveys.

Similarly, in terms of behavioural thresholds, social desirability is expected to lead to *lower* thresholds for *actual* participation, i.e. the individual should easily comply with the group even if the behaviour is undesirable. This would be due to the intrinsic pressure experienced by the individual to *fit in with* or to *not offend* the group. Consequently, the individual *does as the group does* in terms of its information security behaviour. On the other hand, when *asked* about participating in undesirable behaviour, the individual is likely to report a *high* threshold indicating he/she would not be swayed by the group. The individual knows that *doing as the group is doing*, in terms of bad practices, is not what is expected of him/her. They report that the individual will not easily follow the example as to *not offend* or *conform to the expectations* of whosoever sees his/her responses. This paradox of actual versus reported behaviour is problematic for the interpretation of threshold values. Mechanisms to control for the effect of social desirability should be investigated;

– Behavioural threshold analysis in the context of information security is currently unknown to the conventional respondent. With this in mind, traditional questionnaires might not convey enough background information on exactly what is expected from respondents. In addition, the structure of the questionnaire might not provide enough guidance for a respondent to reply confidently in the expected fashion. Mechanisms would need to be employed to restructure the approach and guide a respondent through the process and in doing so prevent responses that do not fit the expected patterns; and finally
– The nature of the topic on which the questions are based should be such that the behaviour of an individual is known to other members of the group. Behavioural threshold analysis is reliant thereon as an individual's threshold is based on the behaviour of the group around him/her and if the individual is not aware of other's behaviour he/she cannot be influenced and cannot express an inclination to follow their example. This implies that any behaviour that is not practised in the open, or at least practised without specifically being hidden by the members in the group, is not suitable as a topic for behavioural threshold analysis (Granovetter 1978). Most likely behaviour with specifically harmful intentions would be done in secret. By contrast, behaviour that is not known to the perpetrator to be detrimental may not be hidden due to no perceived wrongdoing or threat. This has the implication that not all information security questions from literature can be used without ensuring the question conforms to this specification. This does not preclude the use of existing questions, but simply that special consideration should be given to the underlying behaviour about which the question asks.

In summary, these issues mentioned above indicate the direction for the investigation that is presented in this paper. It furthermore serves to reaffirm the premise that the measurement instrument cannot follow the existing trends and the underlying methodology will have to differ in most aspects. The traditional approaches need to be revisited in order to address these issues to fit the unique requirements for behavioural threshold analysis. In the following section, how information security behaviour is currently classified and implemented in information security research and how behavioural threshold analysis questions can be determined are described. Special attention is given to the requirements for behavioural threshold analysis, namely what topics are suitable for behavioural threshold analysis in information security and how the questions on a

questionnaire should be presented to obtain trustworthy results. Attention is given to the overtness of the behaviour and whether the behaviour would typically be performed with the explicit knowledge of others.

3. Information security behaviours

In order to ascertain suitable information security topics for behavioural threshold analysis, it is imperative to look at information security topics and questions in general and how they are expressed and handled in literature. Specific attention is given to whether the specific behaviours from literature conform to the specifications as set out above.

Pattinson et al. (2016) define information security behaviour as simply: '*… the full spectrum of behaviours* [actions] *by people who make significant use of computers as part of their job.*' Based on an earlier study by Pattinson and Anderson (2007), these behaviours are categorised into three discrete types of information security behaviour that are 'deliberate risk-averse behaviours', 'Naïve and accidental behaviours', and 'Deliberate risk-inclined behaviours'. Some examples of these behaviours are also presented by Pattinson and Anderson (2007) and include: Always logging off when computer is unattended (deliberate risk-averse), opening unsolicited e-mail attachments (naïve and accidental), and writing and disseminating malicious programmes (deliberate risk-inclined).

This classification is based on a mapping of a larger taxonomy for information security behaviours that was introduced by Stanton et al. (2005). Their taxonomy was constructed by interviewing information security experts about their experience with positive and negative information security behaviours within different organisations. After refactoring the original behaviours by merging similar behaviours into groups, a six-element taxonomy was constructed, which categorises information security behaviours on two features, namely intent and skill. Intent looks towards the eventual outcome that was envisioned by the person performing the specific behaviour, i.e. a positive or negative eventuality for the organisation. Skill refers to the level of technical proficiency that is required to execute the behaviours. Each behaviour is then expressed with a rating of one (low) to five (high) for both skill and intention. Interestingly it was noted that the higher the intentionality of the behaviour, the higher the required skill level for the behaviour became (Stanton et al. 2005).

The categories for information security behaviour by Pattinson et al. (2016), that were referred to earlier, were mapped from the taxonomy suggested by Stanton et al. (2005). They identify 'naïve and accidental behaviours' as their category of interest for a comparison of data collection methods for information security attitudes. This provides the direction for using the same kind of 'naïve and accidental behaviours' as the basis for behaviour threshold analysis. In comparison, the other two categories are either mostly unsuited for this research ('deliberate risk-inclined behaviours') or still indicated for inclusion in future work ('deliberate risk-averse behaviour'). 'Deliberate risk-inclined behaviours' are behaviours that, for the most part, require a high level of skill. Furthermore, seeing that these behaviours are deliberate, they are known by the offender to be behaviour that is not acceptable as good information security practice. Such behaviours are therefore most likely done in secret and those that practise them are very unlikely to let others in their organisation find out what they are doing, let alone admit to the behaviour on a research survey. Recall that behavioural threshold analysis requires the members of a group to be aware of the actions of others for the model to be applied. Therefore, 'deliberate risk-inclined behaviours' are excluded from this research. The other end of the spectrum involves 'deliberate risk-averse behaviours', which are behaviours that are considered beneficial to the overall well-being of an organisation's information security and culture. These behaviours will likely be practised overtly, without the individual wanting to hide his/her actions. Other members of the specific group would therefore be aware of this behaviour and the behaviour should also have an influence on their collective behaviour. Inclusion of risk-averse behaviours in behavioural threshold analysis falls beyond the scope of this paper but is planned for inclusion at a later stage.

Furthermore, 'deliberate' information security behaviours are typically covered by information security policies, which would make their analyses a question of policy compliance (Al-Omari, El-Gayar, and Deokar 2012; Ifinedo 2012; Vance and Siponen 2012). For this specific study, the focus is on 'naïve and accidental behaviours'. By implication, the naïve individual may not have knowledge of existing policies that exist to govern his/her behaviour and cannot therefore comply with guidelines that the individual does not know exist. Furthermore, even if the individual does have knowledge of policies he/she may still be deceived due to his/her naiveté regarding, for instance phishing attacks. Accidental behaviour may also be performed by individuals who are well versed in policy matters. A seemingly harmless action might cause a security vulnerability by accident. Retrospective to behavioural threshold analysis for information security topics, policies may be inferred from the results specifically to guide future behaviour in conjunction with security awareness programmes. This,

however, falls outside the scope of the current research and is indicated as possible future work.

When an individual is unaware (i.e. naïve) that his/her behaviour is unwanted, that individual will most likely exhibit 'naïve and accidental behaviours' without much thought to consequences of what should happen if the behaviour is known. Members of the group should therefore be aware of each other's naïve and accidental actions. These behaviours are also of such a nature that they could be harmful to an organisation's information security and fidelity (Pattinson et al. 2016). A relatively low skill level is required for behaviour that falls into this category, which means that most individuals in a group should be able to perform these actions. Furthermore, Parsons et al. (2014, 2017) also used naïve and accidental behaviour as the basis for the development of the HAIS-Q (Humans Aspects of Information Security Questionnaire). The HAIS-Q is used as an aid in determining specific topics for behavioural threshold analysis in information security, with the difference that the topics are expressed in a manner that is conducive to the unique requirements set out for threshold analysis. In the following section, example questions for behavioural threshold analysis when it is applied in the context of information security are presented.

4. Example information security questions for behavioural threshold analysis

An annual survey of international information security threats is conducted by PricewaterhouseCoopers to inform business leaders of information security risks. In the report 'The Global State of Information Security Survey' (PWC 2017) it is stated that there is an awareness among company executives of the possible consequences of cyberattacks. Nevertheless, almost half (48%) of the companies which were surveyed do not have structures in place to address general information security awareness among employees. Furthermore, 54% of these companies do not have incident-response strategies. While it is acknowledged that these shortcomings should first and foremost be addressed at an executive level, there is a resulting gap in the typical employee's awareness and general information security hygiene. This lack of awareness and skills is sure to have an influence on their eventual information security behaviour.

The Human Aspects of Information Security Questionnaire (HAIS-Q) is a measurement instrument, developed by Parsons et al. (2014), to quantify the information security weaknesses that are perpetuated by humans. The instrument was tested for validity and reliability and can be considered as one of the better established and mature instruments for assessing security awareness. The modular nature of the HAIS-Q allows the instrument to be adapted for testing awareness for specific aspects of information security that are of interest (Parsons et al. 2017). To this end, the HAIS-Q is divided into information security focus areas, each with a specific set of related behaviours. With the specifics of behavioural threshold analysis in mind, the HAIS-Q was used as a basis for determining a series of questions for the construction of a measurement instrument specifically for the application of threshold analysis for information security behaviour. These behaviours were chosen to also be representative of typical problematic information security areas that are identified in information security audits and surveys as mentioned above.

Table 1 shows example information security questions for behavioural threshold analysis, based on the focus areas and associated security behaviours ('naïve and accidental'), which were identified from the HAIS-Q. The questions were formulated in the style required for behavioural threshold analysis and were subsequently included in case studies on the implementation of behavioural threshold analysis in information security.

The HAIS-Q describes more focus areas with themes, such as mobile devices and information handling (Parsons et al. 2017) that are not included in Table 1. After due consideration of the specific contexts in which the case studies and further validation studies were to be conducted, only the five focus areas in Table 1 were selected for inclusion in the experimental phases of this research. It should be noted, however, that depending on the requirements of the specific behavioural threshold study, one might include more of the focus areas and include multiple associated

Table 1. Example questions based on focus areas and behaviours from HAIS-Q.

	Focus area	Information security behavioural threshold question
1.	Password management	How inclined would you be to also share passwords, given the percentage of colleagues who share their passwords?
2.	Social media use	How inclined would you be to also spend excessive work time on social media, given the percentage of colleagues who spend excessive work time on social media?
3.	Incident reporting	How inclined would you be to also ignore security incidents by not reporting them, given the percentage of colleagues who ignore security incidents and do not report them?
4.	Internet use	How inclined would you be to also access dubious websites from devices connected to your company network, given the percentage of colleagues who regularly access dubious websites from devices connected to your company network?
5.	E-mail use	How inclined would you be to also open any unfamiliar email attachments, given the percentage of colleagues who normally open any unfamiliar email attachments?

questions for each focus area. Caution should be exercised when deciding on adding multiple focus areas or questions in order not to overburden the respondents with lengthy questionnaires that take excessive time to complete. The number of responses that are required per question adds significantly to the burden that is placed on the respondent. Traditional questionnaires employ multiple questions to test one facet of interest (for example, incident reporting) in order to address consistency in the questionnaire (Sekaran and Bougie 2010). Once again, the unique requirements for behavioural threshold analysis necessitate a divergent approach. The model allows for only one question per facet that is to be tested.

The wording for the questions is based on the requirements for behavioural threshold analysis. In this case, a respondent indicates his/her level of inclination to join in the corresponding behaviour when different percentages of the group are participating in the behaviour (i.e. the threshold for participation). The inclination is expressed on a four-point Likert scale, and the corresponding percentage of participants in the group is presented in intervals of 10%. Table 2 presents an example of how one of these questions would be presented in its entirety. Each question is presented as a grid of possible thresholds and respondents would have to nominate a response for each threshold interval resulting in ten responses per question. The suggested layout draws from the recommendations of Pattinson et al. (2016) that a combination of repertory grid interviews and traditional questionnaires is advisable for information security behaviour research. The responses for the threshold intervals are required in order to conduct the mathematical analysis and prediction of the group behaviour. It is therefore recommended that a balance be found between the coverage of topics and the number of questions asked.

Table 2. Example of a complete behavioural threshold question.

Percentage of colleagues who spend excessive work time on social media	How inclined would you be to also spend excessive work time on social media, given the percentage of colleagues who spend excessive work time on social media?			
	Never	Somewhat inclined	Strongly inclined	Always
0–10%	1	2	3	4
11–20%	1	2	3	4
21–30%	1	2	3	4
31–40%	1	2	3	4
41–50%	1	2	3	4
51–60%	1	2	3	4
61–70%	1	2	3	4
71–80%	1	2	3	4
81–90%	1	2	3	4
91–100%	1	2	3	4

In Section II, it was remarked that social desirability is a problem when using questionnaires for data collection, with specific implications for behavioural threshold analysis. Mechanisms for measuring the levels of social desirability that a respondent exhibits date back some time. Most influential is the work of Crowne and Marlowe (1964) who developed a fully-fledged instrument to measure whether a respondent is answering truthfully or whether social desirability has tainted his/her response. The Marlowe-Crown social desirability scale is a 33-item questionnaire that presents a respondent with statements that could be deemed socially positive and others that are socially negative. Respondents are asked to respond only whether the statement is true, or false, pertaining to them personally. A set of expected responses to the questions is predetermined, coded as true for 18 of the scenarios and 15 for false. The expected responses are based on whether a truthful respondent would answer true to statements that would place him/her in a bad light socially. The responses are scored, and the level of social desirability can be determined as either high or low. Due to the number of questions that are included in the Marlowe-Crowne scale, shortened versions of the scale have been proposed (Reynolds 1982) and later validated (Ray 1984) to convey a reliable account of a respondent's level of social desirability. The short social desirability scale, which was validated by Ray (1984) consists of only eight questions answered by only Yes, No or Unsure. Each of these responses is coded and scored based on the specific question. These eight questions were included in the subsequent case studies, supplementing the five information security questions (see Appendix A).

The premise, at least for behavioural threshold analysis, is that a respondent who exhibits high levels of social desirability would nominate threshold values that are higher than their actual thresholds, e.g. that he/she would share his/her password when 31–40% of others in their group share their passwords. The truth is that a respondent may in fact share his/her password when only 11–20% of others in the group do so. The thresholds for a respondent who shows social desirability could conceivably be adapted downwards by a conservative margin (e.g. one threshold interval or 10%). This should lead to representations of the personal thresholds within a group being more trustworthy and allow the eventual collective behaviour of the group to be predicted with better accuracy.

From the discussion in this section, it becomes evident that the proposed questionnaire differs considerably from the typical information security behaviour questionnaires. Furthermore, the analysis and interpretation of the responses are also treated differently in that a

specialised mathematical analysis of the results is performed rather than the traditional statistical methods that are commonly used in the analysis of traditional questionnaires. In Section V, two illustrative case studies where these questions were implemented, and provision was made for the occurrence of social desirability are described.

5. Illustrative case studies

Two case studies were completed to validate the choice of behavioural threshold analysis questions for group behaviour in information security, as well as the method for presenting the questions to respondents. Before the case studies are presented, a note on the sample sizes that are reported for each of the case studies: As mentioned earlier in Sections I, II, and III, the behavioural threshold analysis approach requires individuals to be aware of the behaviour of the other members of the group (Growney 1983). It stands to reason that an employee will only be aware of the behaviour of individuals that he/she comes into contact with on a regular basis, i.e. another person in the same organisational group or department. On the other hand, global tendencies in information security behaviour might be propagated through media or other public information sources, which in turn creates an awareness that transgresses organisational boundaries. Analysing these large-scale trends falls outside the scope of the model. In this instance, global trends are overlooked in favour of more immediate behaviours in an organisational setting. Therefore, in order to judge the immediate group influence and behaviour accurately, only the relevant group members should be included in the exercise. When including members from outside the individual's frame of reference in terms of behavioural examples, the model might become skewed and the results less reliable. The required awareness therefore dictates that the sample sizes are specifically kept small. This is another example of the uniqueness of the behavioural threshold analysis model and how it differs substantially from the other established approaches to measure information security behaviour.

5.1. Case study 1 (Snyman and Kruger 2016)

The first case study was conducted with a group of 22 first-year engineering students at a South African university. The information security question that was used in this instance was based on password management and was presented in the format of Figure 1:

> I will share my password with another student when at least x percent of students share their passwords (nominate a value for x). (Focus area: Password management)

The information security question along with some questions on biographic information was distributed to the group via Google Forms. The structure of the question was presented in such a manner that the respondent had to nominate a value for x by typing in the relevant percentage value. In this case study no questions on social desirability were asked and no adjustment of the nominated thresholds was done. The case study was intended to be an initial test to see how a skeleton questionnaire would fare for behavioural threshold analysis. After the cumulative results for the nominated behavioural thresholds were calculated, the resulting graph in Figure 2 was obtained.

The graph represents an aggregate of the thresholds of the individuals, given the percentage of group members who share their passwords. For instance, the point (20,10) indicates that 10% of individuals will share their passwords when 20% of the group do so. The graph did not follow the expected trends. The expectation was that individuals would have low thresholds for password sharing, i.e. they would be willing. The group of students was observed throughout a semester during practical programming classes in a shared computer laboratory. They need a network username and password to access the workstations in this environment. Password sharing was often observed to occur when one student's credentials have expired or were forgotten. Resetting the expired credentials would entail a visit to an IT helpdesk in another building some distance away. So, in order to save time another student would simply supply their credentials so that a classmate is able to access a workstation to complete the assignment that is due by the end of the practical session.

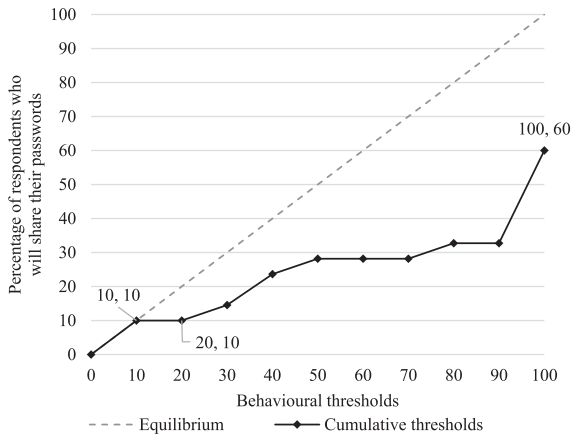


Figure 2. Behavioural threshold analysis for case study 1 (Focus area: Password management).

The network credentials in question are also used for authentication with other network resources, such as printers, network storage, e-mail server, learning management system, financial and academic statements, etc. If another user is privy to one's credentials, he/she can therefore access any and all resources for which the credentials are authorised. Whether the risks are known and understood by the students is not clear, but through the above-mentioned observation, it was known that the group was quite comfortable with sharing its passwords among the members and it is a practice that was done on a regular basis (even though the practice is not recommended).

The notion of password sharing among students is supported by Shay et al. (2010), who conducted research on behaviour and attitudes relating to passwords. They found that 33% of the undergraduate students that they surveyed were engaging in password-sharing behaviour. Another, more recent, study on password behaviour, reports an even higher password-sharing rate of between 50–60% for a non-homogenous sample in a South African context (Butler and Butler 2018). Since the case study was performed in a South African context, this result should also be indicative of what could be expected in terms of the results for password sharing from case study 1.

The two main reasons that were identified for the unexpected results were, either the respondents do not understand the question and how to answer it correctly, or respondents chose to misrepresent their actions by not answering the question truthfully because they are aware that password sharing is frowned upon, i.e. they display high levels of social desirability. A combination of social desirability and misinterpretation was thought to be the most likely cause for the results not conforming to the expected standard. For a detailed interpretation of the graph and related recommendations, see Snyman and Kruger (2016). Taking its direction from the lessons learnt in the first case study, a second case study was completed as described in the following sub-section below.

5.2. Case study 2

A second case study was conducted as part of the current study to improve upon the two issues that were identified from the first case study, i.e. question format and social desirability. Another question was selected and a new online questionnaire (once more facilitated through Google Forms) was constructed and a more guided approach to threshold selection was followed based on the recommendations of this research. The questionnaire was completed by 16 staff members at a university within a departmental setting. The layout and the question in Table 2 was used, i.e. a grid layout (inspired from that of a repertory grid) where a respondent would have to rank his/her level of inclination for participation in the behaviour that was described in the question, given the percentage of others that perform the behaviour. The question is reiterated below and is an example of social media use:

> How inclined would you be to also spend excessive work time on social media, given the percentage of colleagues who spend excessive work time on social media? (Focus area: Social media use).

Even though the question seems to be about work time management, there are underlying information security risks associated with social media use that are addressed (e.g. sharing of sensitive company information). The information security question was supplemented with the eight social desirability questions as described in Section IV. The inclination level mentioned above was tested for each of the threshold intervals. For this case study, it was decided that the first level of inclination that represents a willingness to participate in the action would be used to determine the threshold value for the individual respondent, i.e. answering at least that he/she was 'Somewhat willing' to participate in the behaviour. Helfinstein, Mumford, and Poldrack (2015) argue that the influence of group behaviour on an individual is great enough that that individual would follow group actions based only on the perception that others in the group are doing it, without much proof that they indeed perform the actions. This colloquially coined *lemming effect*[1] may be strong enough to cause the individual to act in a manner that is contrary to his/her own convictions (Helfinstein, Mumford, and Poldrack 2015). The results obtained for the second case study are presented in Figure 3. The graph closely follows the expected trends from literature.

Initially, around 31% of individuals expressed relatively low thresholds to use excessive work time for social

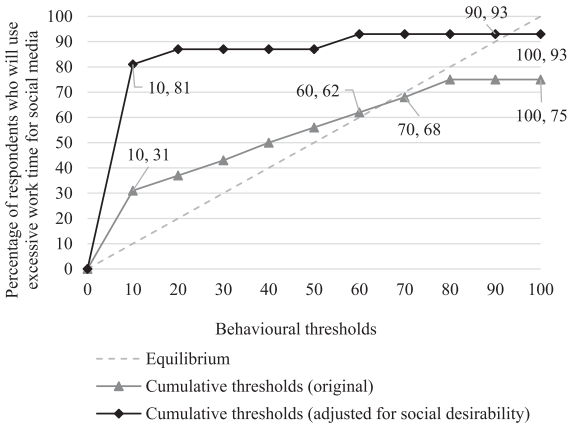


Figure 3. Behavioural threshold analysis for case study 2 (Focus area: Social media use).

media activities when others also do so (see cumulative thresholds – original – trend line in Figure 3). The graph of the cumulative thresholds indicates that excessive social media use is likely to grow until between 62% and 68% of the group members participate. The behavioural equilibrium is reached at this stage with the participation trend being stable against increase and stable against decrease (the gradient (m) of the line segments both sides of the equilibrium intersection is less than 1). Without any external influence, the number of participants should remain unchanged. When taking into account the influence of social desirability and adjusting the reported thresholds as recommended in Section IV (see Appendix A), the second trend line indicates that the initial 31% of individuals with low thresholds for participation should actually be closer to just over 80% (see cumulative thresholds – adjusted for social desirability – in Figure 3). The eventual equilibrium ($m = 0$) is established at over 90% of the group participating after the adjustment for social desirability. This indicates that the inclusion of the social desirability questions helps establish a better view of the actual behaviour exhibited by the group, rather than the reported behaviour. When factoring in social desirability the outcome is not necessarily concrete and caution should be taken when interpreting the results. The actual thresholds most probably lie between these two extremes.

The threshold results for the group show that the individuals have low thresholds for participation in the behaviour of social media use. A low threshold indicates that the individuals are easily influenced to join others in their behaviour. The outcome might be indicative that the level of security awareness of the individuals is not sufficient, or that they are coerced into demonstrating behaviour that is contrary to their better knowledge. In the following section, recommendations for the construction of a measurement instrument are presented after which case studies that validate the recommendations are shown.

6. Proposed methodology

As mentioned earlier, threshold analysis for information security behaviour poses unique challenges in its execution, as this approach does not conform to the traditional information security behaviour research expectations. The two aforementioned case studies are a practical confirmation thereof. Therefore, the aim in this section is to provide methodological recommendations for the construction of a specialised measurement instrument. The limitations of the proposed methodology are discussed. This section concludes with a reflection on the three research sub-questions from Section I.

6.1. Recommendations for measurement instrument

The overview of information security behaviours (Section III) and related questions (Section VI), in combination with the case studies that were presented in Section V form the basis for a set of recommended practices for the construction of measurement instruments for threshold analysis. Three main groups of recommendations are identified. They are based on themes that are commonly of importance when constructing traditional measurement instruments, namely sampling, question design, and validation. The recommendations are presented in Table 3.

The methodological recommendations as set out above were subsequently implemented in a further experimental case study to analyse the performance of the suggested measurement instrument. The validation case study is presented in Section VII. The following sub-section presents a discussion on the limitations of the methodology as well as the possible threats to its validity.

6.2. Limitations and threats to validity

The suggested methodology and measurement instrument was designed with the specific, unique requirements of behavioural threshold analysis in mind. In order to meet the requirements, the approaches that are common with traditional measurement instruments had to be either adapted or replaced by other approaches to follow these specifications. By tailoring the methodology according to these requirements, it is only natural that certain limitations are introduced. Furthermore, the rationale for the methodologies that are commonly used for surveys by means of questionnaires have been applied for quite some time. Consequently, they have matured and are used throughout a number of different applications (Redmiles et al. 2017; Sekaran and Bougie 2010). Along with this maturity comes an expected level of validity and reliability. This section is therefore a discussion of the possible limitations of the methodology and the threats to its validity that may exist. The limitations and validity threats are once more discussed in terms of the research sub-questions of *Sampling*, *Question design*, and *Validation*.

Sampling – The sample sizes for behavioural threshold analysis are specifically kept small as described in Table 3. However, when the sample becomes too small (i.e. less than 10 individuals) a meaningful analysis of behavioural thresholds becomes problematic. Due to the limitation of the sample sizes, no generalisation of the results to a greater population is possible. If a greater population

Table 3. Recommendations for an information security behavioural threshold analysis measurement instrument.

		Traditional measurement instruments (Pattinson et al. 2016; Redmiles et al. 2017; Sekaran and Bougie 2010)	Suggested information security behavioural threshold analysis measurement instrument	Rationale for methodological suggestions
Sampling	Sample sizes	Large	Small	Respondents need to be aware of the behaviour of others in their group (Growney 1983). Sample size should be limited to reflect this awareness, i.e. limited to organisational boundaries, such as departments. Where departments are large, i.e. extends across multiple office spaces or geographic locations, smaller groups where the members have a direct day-to-day influence on each other should be considered.
	Sampling methods	Probability sampling	Nonprobability sampling – Purposive	Purposive sampling refers to targeting specific groups of people with a very specific knowledge (Sekaran and Bougie 2010). Given the requirements of behaviour awareness of other group members, purposive sampling is recommended for behavioural threshold analysis.
	Generalisation	Generalise results to greater population.	No generalisation of results to greater population.	Information security behavioural threshold analysis in this context is not concerned with generalising findings. The analysis is limited to the group that is surveyed.
Question design	Question format	Self-reporting questionnaire or repertory grid interviews	Combination format (questionnaire and repertory grid)	In contrast to the traditional split between self-reporting questionnaires and repertory grid interviews (Pattinson et al. 2016), a combination method is suggested. Where applicable, optical polling provides a good middle ground between the approaches with good results for behavioural threshold analysis (Snyman and Kruger 2017b).
	Question topics	Generic	Specific	For behavioural threshold analysis, especially in terms of information security, the choice of topic is of cardinal importance. Questions should concentrate on specific, predetermined focus areas and should not attempt to cover all security focus areas through a general approach. The sensitive nature of questions may lead to social desirability.
	Number of questions	May have many questions to one aspect	One question to one aspect	Traditionally, multiple questions are employed in questionnaires to examine one aspect of interest. The threshold analysis model allows for only one question per aspect (Snyman, Kruger, and Kearney 2017).
	Response scales	Uneven Likert scales with five or more items recommended	Four-item (even) Likert scale	Common practice is to allow a respondent a neutral response by using uneven Likert scales (Redmiles et al. 2017; Sekaran and Bougie 2010). Given the binary nature of behavioural threshold analysis, an even Likert scale reflects this binary decision and ensures a measurable threshold. Using an even Likert scale is also a requirement for using novel media for collecting responses, such as optical polling (Snyman and Kruger 2017b), where only four possible responses are allowed.
Validation	Social desirability	Present, but may have limited effect	Needs to be specifically controlled for	Questions on information security behaviour are sensitive by nature (Redmiles et al. 2017). Sensitivity in questions often leads to 'acceptable', rather than 'accurate', responses (Dahlgren and Hansen 2015).
	Experimental controls	Reliability and validity based on statistical metrics	Face validity and iterative testing	Face validity (also known as expert reviewing) is the process whereby the measurement instrument is evaluated for validity by experts in the specific area of investigation rather than with statistical metrics (Bolarinwa 2015; Redmiles et al. 2017). This is commonly used during developmental phases of measurement instruments. The novelty of the suggested measurement instrument necessitates iterative implementation and critical review by the researcher. The specific nature of the proposed measurement instrument disallows the commonly used metrics for determining reliability and validity. This is because the instrument is inspired by a repertory grid approach and due to the unique responses that the instrument elicits.

needs to be surveyed, the threshold analysis instrument should repeatedly be administered to different groupings within the population that meet the requirements as set out in Table 3 until the desired coverage of the population is reached.

Purposive sampling is recommended as the sampling method for behavioural threshold analysis. This sampling method requires the target group to have a specific knowledge. For behavioural threshold analysis, this required knowledge is presumed to be about the security behaviour of others. Should the expected level of knowledge not be present in the group, this will impact negatively on the validity of the results that were obtained for the behavioural threshold analysis experiment.

Question design – On the theme of question format (from Table 3), optical polling is suggested as a middle ground between common self-reporting questionnaires and repertory grid interviews. Using optical polling to present a question and facilitate response collection requires all respondents to simultaneously be present in a room. This introduces logistical issues such as scheduling, geographical locations, etc. Such logistical difficulties complicate, and in some cases even prohibit, the use of optical polling. When optical polling is not a viable option, self-reporting (online) questionnaires are therefore used which introduces the known limitations thereof to the application of behavioural threshold analysis in information security.

Specific care should be given to selecting appropriate information security focus areas and question formulation. Even when a focus area is correctly identified, having the wrong question formulation can elicit responses that do not convey the expected information about the specific focus area. Such responses have a negative impact on the validity of the results that are obtained.

In Table 3, the use of a four-item Likert scale for response scales is suggested. Using this scale might not provide enough granularity should a more in-depth analysis of the responses be needed. Furthermore, respondents may become fatigued when confronted with many Likert scale questions (i.e. ten responses for each question as presented in Table 2). Fatigue in respondents typically leads to non-completion of questionnaires as well as lower response rates (Porter, Whitcomb, and Weitzer 2004). Respondents have also been noted to randomly select responses or complete patterns with the Likert scales. Respondent fatigue impacts negatively on the reliability of the data obtained with the measurement instrument.

Validation – Table 3 makes reference to the sensitive nature of survey topics relating to information security behaviour. This leads to social desirability, i.e. untruthful answers to survey questions. If the effects of social desirability are not controlled for, the validity of the data becomes uncertain. The mechanism to measure, and correct for, social desirability that is suggested for behavioural threshold analysis is presented in Appendix A. Special care should be exercised when adapting survey responses based on social desirability scores. Under-correcting, over-correcting, or not correcting responses will once more lead to questionable data for behavioural threshold analysis.

As stated in Table 3, the measurement instrument cannot be tested for reliability and validity using the statistical metrics that are commonly used with regular questionnaires. The instrument's validity is based on iterative testing and expert reviewing. Face validity testing depends solely on the expert reviewer. This limits the use of the measurement instrument to use by researchers who are well versed in the subtleties of behavioural threshold analysis and information security or requires the involvement of a reviewer who possesses the relevant expertise. If the researcher or reviewer is not impartial or is not seasoned enough to reliably complete a face validity review, the resulting measurement instrument can be biased or may not measure behavioural thresholds correctly.

6.3. Summary of methodology

To summarise this section, a brief overview of the methodological and practical value of the proposed methodology and its performance during experimentation is presented in terms of the main themes from Table 3. These themes are *Sampling*, *Question design*, and *Validation* and directly relate to the three research sub-questions from Section I. The themes, and where they fit into the overall behavioural threshold methodology are presented schematically in Figure 4. The left of Figure 4 outlines the behavioural threshold analysis methodology and related steps in broad terms. The right side of Figure 4 expands the 'Construct measurement instrument' step and shows the context of the three themes in this research. The shaded area shows the three main themes and their relevant sub-themes and highlights where this research makes its main contribution and answers the main research question through providing answers to the research sub-questions.

7. Validation

The validation of the aforementioned methodology and resulting measurement instrument by means of an experimental case study is presented in this section. This is followed by a cursory overview of a current real-world application of behavioural threshold analysis for the measurement of group behaviour in information security.

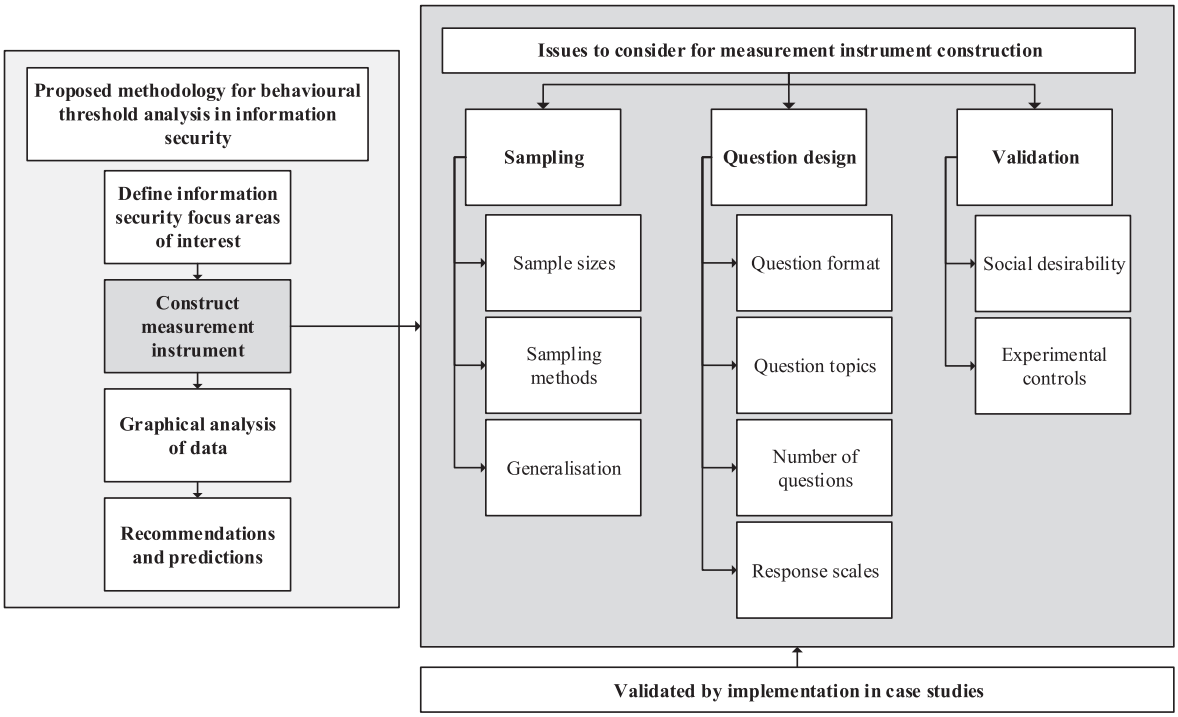


Figure 4. Schematic representation of the methodology of behavioural threshold analysis in information security.

7.1. Validation case study (Snyman and Kruger 2017b)

In order to further validate the information security questions and questionnaire structure that was determined above, a third case study was conducted with a group of 23 honours-level computer science and information systems students at a university. The following question was presented to the group in the format of Table 2:

> '*How inclined would you be to also access torrent websites from devices connected to your university network, given the percentage of students who regularly access torrent websites from devices connected to your university network?*' *(Focus area: Internet use).*

The question was presented on a projector screen and responses were collected using an optical polling platform (Snyman and Kruger (2017b) present more details on the data collection method). The resulting behavioural threshold graph is presented in Figure 5. The graph indicates the original cumulative thresholds for students' inclination to also make use of torrent sites (as an example of dubious website use) when a critical percentage of others also uses torrent sites. The eight questions to measure the level of social desirability of participants were included and displayed on the projector screen. The responses for these eight questions were also collected using the optical polling data collection method. Adjustments to the responses relating to the threshold levels of specific participants, where they showed high levels of social desirability, were made accordingly. See Snyman and Kruger (2017b) for a complete discussion of the results.

It can be seen from Figure 5 that, following the expected trend for threshold analysis, the cumulative thresholds remain above the equilibrium line and only intersect at an 86% participation level. The graph shows an initial incline in the cumulative thresholds,

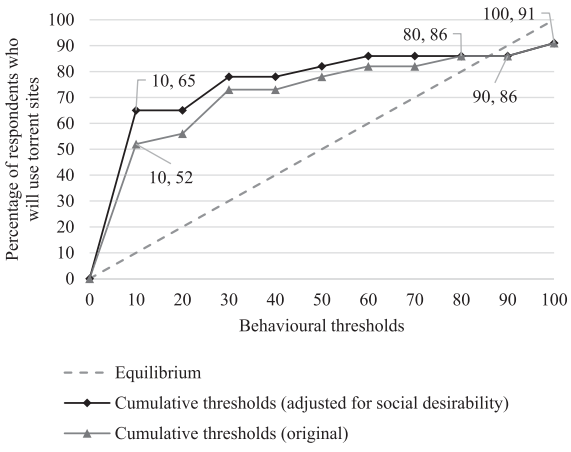


Figure 5. Behavioural threshold analysis for validation case study (Focus area: Internet use).

i.e. a willingness to follow group behaviour, with 52% of the group showing a threshold of 10% for participation in using torrent sites. This willingness might be higher than reported due to the level of social desirability that the respondents exhibit. When correcting for the socially desirable answers (see Appendix A), willingness for participation is shown to be higher at 65%. The original cumulative thresholds and the thresholds that were adjusted for social desirability converge before the intersection of the equilibrium line. The group reaches an equilibrium for participation ($m = 0$ for both line segments, left and right, of the intersection). This indicates that, in the absence of an extrinsic intervention, 86% of the group will eventually use torrent sites due to the group influence. Ultimately, this analysis indicates that the use of torrent sites is a problem and that the respondents are likely to transgress with this behaviour when they know that enough others in the group are also doing so. Training with regard to torrent sites should therefore typically be included in information security awareness programmes in order to address this behavioural phenomenon.

The results obtained for this validation study further indicate the suitability of the suggested information security questions and the presentation of the questions for behavioural threshold analysis. In comparison to the initial uncharacteristic results in case study 1, case studies 2 and 3 show encouraging results that conform to the expected patterns seen in literature. This was due to the positive effects of the presentation of the questions, i.e. in a grid pattern with threshold intervals. The participants then ranked their inclination towards participating in the behaviour by indicating their response in the grid. The presentation was based (in part) on the suggestions of Pattinson et al. (2016) on combining the methods of questionnaires and the repertory grid technique. The ranking of threshold intervals ensured that the threshold values could effectively be used for the mathematical analysis and prediction of the collective behaviour of the group.

The nature of the questions that were chosen is shown to be suitable for the task, based on the success of the implementation in the validation case study. The social desirability questions were shown to contribute positively to the interpretation of the results by allowing insights into the differences between the reported thresholds when compared to the actual inclinations that the individuals in the group exhibit.

7.2. Real-world implementation

The application of a duly prepared measurement instrument, based on the recommendations provided in this research, was performed to test the approach in a real-world environment (Snyman, Kruger, and Kearney 2017). Following the guidelines as set out in this paper, a practical experiment was conducted at a large utility corporation in Australia. With the support from management, a department with 63 respondents was identified for inclusion in this study. A complete questionnaire comprising all five focus areas as in Table 1 was used, supplemented with additional questions on positive security behaviour and social desirability. An analysis of the collected responses shows encouraging results and the results relevant to Table 1 are summarised here:

The results showed that the specific department exhibited high behavioural thresholds for *password management*, *internet use*, and *e-mail use*. High thresholds indicate that the respondents are highly aware of the associated risks with following negative examples in the group security behaviour and will therefore not participate in the detrimental actions that are performed by others. In terms of *social media use* and the *reporting of security incidents*, the group showed low behavioural thresholds. This indicates that the group is not sufficiently aware of the risks involved in participating in these behaviours. The respondents are likely to also partake in these behaviours when a critical mass of the group performs these actions. Inclusion of these topics in information security awareness programmes is therefore recommended to ensure that the department is sufficiently trained to avoid questionable information security behaviour.

The success of the practical implementation of threshold analysis in industry is attributed to the detail investigation and testing of the approach as presented here in this paper. Although the research in Snyman, Kruger, and Kearney (2017) only reports on one application, the measurement instrument and methodology are shown to work well in real-world situations. Further applications and expansions of the measurement instrument are planned for future work in other industries and new real-world studies.

8. Reflection

Through the case studies and validations, it was shown that a unique information security behavioural threshold analysis measurement instrument was successfully developed. This instrument addresses the special nature and requirements of threshold analysis and contributes to the enhancement of the methodology of behavioural threshold analysis in the context of information security. The result is also a positive answer to the main research question that was formulated in Section I. The substantiation for a positive answer is presented in terms of the

main themes (relating to the research sub-questions) as described above:

Sampling – The suggested sampling approach is to target a relatively *small* group of respondents in a purposive manner, i.e. they have *specific knowledge* of the behaviour of others in the group. The analysis does *not require any generalisation* of the results to a greater population as the prediction of information security behaviour is limited to the group that is surveyed. In the validation and real-world case studies, the sample sizes were kept small and were determined by a logical delimitation along the lines of organisational structures. The individuals in the group have the required knowledge of the behaviour of others in the group due to their daily exposure to one another. It was possible to obtain useful responses and the prediction of group behaviour, based on the aggregated behavioural thresholds, was successful.

Question design – In terms of question design, it is recommended to identify specific information security topics and present questions relating to the topics in a combination format (a cross between traditional questionnaires and repertory grids). The responses on the grid are limited to a four-point Likert scale to ensure that a respondent either commits to, or rejects the behaviour, given the percentage of others who participate. Due to the number of required responses per question, only one question per information security aspect is suggested. When the suggested question design was implemented, the respondents were guided to supply seemingly correct and useful responses due to the even nature of the Likert scale. By not allowing a neutral response, the scale mimics the binary nature of information security behaviour and it is ensured that each response can be used in the behavioural threshold analysis. The length of the measurement instrument was acceptable and even with the many responses required, due to the grid format, the time that was spent to respond was kept to a minimum. Even though the specific topics were identified to limit socially desirable responses, the group was shown to still have high levels of social desirability, but the effect could be assessed and controlled for.

Validation – Due to the unique nature of the measurement instrument and because it does not conform to the traditional questionnaire format, the usual statistical metrics for measuring reliability and validity cannot be applied in this context. It is therefore up to an expert to evaluate the suitability of the measurement instrument. The sensitivity of themes relating to information security gives rise to social desirability, which in this context, is unfavourable for the eventual behavioural threshold analysis. When the suggested measurement instrument was deployed during the exercises, the effect of the social desirability was measured and controlled adaptations to the responses could be made before the formal analysis. Both the original and adapted behavioural thresholds are then used as part of the analysis to provide a more accurate view on the group's information security behaviour. Finally, the methodological and practical considerations as presented in this paper can be employed during face validity examination as a guideline for a standard information security behavioural threshold measurement instrument.

In all the case studies, respondents were asked to provide feedback or comments regarding the measurement instrument in terms of how easily they understood the process, how easily they answered the questions and whether they had any suggestions or complaints. Their feedback was in the form of open-ended sentences at the end of each questionnaire. These were supplemented with follow-up discussions and informal interviews on their experiences with the measurement instrument. The feedback they provided was overwhelmingly positive, e.g. 'Love the scaling style of the question', 'The process was easy to follow', 'The questions were clear', etc. This type of feedback further serves to informally support the suitability of the suggested methodology for behavioural threshold analysis in information security in an analogical manner.

9. Conclusion

In this research, the aim was to provide a methodology for the construction of a measurement instrument for behavioural threshold analysis in information security and to provide a solution to the problem statement. Due to the unique requirements of an information security threshold application, traditional information security measurement instruments are insufficient and need considerable adaptation to determine behavioural thresholds.

In providing a methodology for the construction of a measurement instrument for behavioural threshold analysis, the problem of the unique requirements for an application in information security was addressed. This was achieved by determining information security topics and related questions for use in behavioural threshold analysis research in information security. Special attention was also given to the manner in which these questions are presented, both in physical layout and in wording, when used in questionnaires. This article presented the analysis of selected literature relating to information security themes and associated questions to base the specific behavioural threshold analysis questions on a sound theoretical framework. The questions that were identified were implemented in three case studies to test the suitability of the questions when used in experimental circumstances. The manner in which the questions were presented, i.e. in a grid fashion (similar to that of a repertory grid) was also tested in the experimental application of the behavioural

threshold analyses in the context of information security. The results of these experiments indicate the suitability of the identified questions and the manner in which they are presented. Future attention will also be given to the managerial value of information security behavioural threshold analysis and its utility as a management decision support tool to improve the information security of organisations.

Note

1. Based on migratory behaviour of rodents, the lemming effect refers to blindly following a group to one's own detriment.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Dirk Snyman http://orcid.org/0000-0001-7360-3214

References

Ajzen, I. 1991. "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* 50 (2): 179–211.

Al-Omari, A., O. El-Gayar, and A. Deokar. 2012. "Information Security Policy Compliance: The Role of Information Security Awareness." In *Proceedings of the 18th Americas Conference on Information Systems (Paper 16)*, 1–10. Seattle, WA: Association for Information Systems.

Ashenden, D. 2008. "Information Security Management: A Human Challenge?" *Information Security Technical Report* 13 (4): 195–201.

Bolarinwa, O. A. 2015. "Principles and Methods of Validity and Reliability Testing of Questionnaires Used in Social and Health Science Researches." *Nigerian Postgraduate Medical Journal* 22 (4): 195–201.

Butler, R., and M. Butler. 2018. "Some Password Users are More Equal than Others: Towards Customisation of Online Security Initiatives." *South African Journal of Information Management* 20 (1): 1–10.

Connolly, L., M. Lang, J. Gathegi, and J. D. Tygar. 2016. "The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study." In *Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 33–44. Frankfurt, Germany: Plymouth University.

Crowne, D. P., and D. Marlowe. 1964. *The Approval Motive*. New York: Wiley.

Cuganesan, S., C. Steele, and A. Hart. 2018. "How Senior Management and Workplace Norms Influence Information Security Attitudes and Self-Efficacy." *Behaviour & Information Technology* 37 (1): 50–65.

Dahlgren, G. H., and H. Hansen. 2015. "I'd Rather be Nice than Honest: An Experimental Examination of Social Desirability Bias in Tourism Surveys." *Journal of Vacation Marketing* 21 (4): 318–325.

Da Veiga, A., and N. Martins. 2017. "Defining and Identifying Dominant Information Security Cultures and Subcultures." *Computers & Security* 70: 72–94.

Dhillon, G., R. Syed, and C. Pedron. 2016. "Interpreting Information Security Culture: An Organizational Transformation Case Study." *Computers & Security* 56 (1): 63–69.

Dodou, D., and J. C. De Winter. 2014. "Social Desirability is the Same in Offline, Online, and Paper Surveys: A Meta-Analysis." *Computers in Human Behavior* 36: 487–495.

Fazio, R. H. 1990. "Multiple Processes by Which Attitudes Guide Behavior: The MODE Model as an Integrative Framework." *Advances in Experimental Social Psychology* 23 (1): 75–109.

Fisher, R. J. 1993. "Social Desirability Bias and the Validity of Indirect Questioning." *Journal of Consumer Research* 20 (2): 303–315.

Granovetter, M. 1978. "Threshold Models of Collective Behavior." *American Journal of Sociology* 83 (6): 1420–1443.

Growney, J. S. 1983. *I Will if You Will: Individual Thresholds and Group Behavior - Applications of Algebra to Group Behavior*. Bedford, MA: COMAP Inc.

Helfinstein, S. M., J. A. Mumford, and R. A. Poldrack. 2015. "If all Your Friends Jumped Off a Bridge: The Effect of Others' Actions on Engagement in and Recommendation of Risky Behaviors." *Journal of Experimental Psychology: General* 144 (1): 12–17.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory." *Computers & Security* 31 (1): 83–95.

Kaur, J., and N. Mustafa. 2013. "Examining the Effects of Knowledge, Attitude and Behaviour on Information Security Awareness: A Case on SME." In *Proceedings of the 2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 286–290. Kuala Lumpur, Malaysia: IEEE.

Kruger, H. A., and W. D. Kearney. 2006. "A Prototype for Assessing Information Security Awareness." *Computers & Security* 25 (4): 289–296.

Nguyen, Q. N., and D. J. Kim. 2017. "Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives." In *Proceedings of the 50th Hawaii International Conference on System Sciences*, 4947–4956. Hawaii: University of Hawaii at Manoa.

Parsons, K., D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans. 2017. "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies." *Computers & Security* 66 (2017): 40–51.

Parsons, K., A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram. 2014. "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)." *Computers & Security* 42 (2014): 165–176.

Pattinson, M. R., and G. Anderson. 2007. "How Well are Information Risks Being Communicated to Your Computer End-Users?" *Information Management & Computer Security* 15 (5): 362–371.

Pattinson, M. R., M. A. Butavicius, K. Parsons, A. McCormac, and C. Jerram. 2015. "Examining Attitudes Toward

Information Security Behaviour Using Mixed Methods." In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*, 57–70. Lesvos, Greece: Plymouth University.
Pattinson, M. R., K. Parsons, M. Butavicius, A. McCormac, and D. Calic. 2016. "Assessing Information Security Attitudes: A Comparison of Two Studies." *Information & Computer Security* 24 (2): 228–240.
Porter, S. R., M. E. Whitcomb, and W. H. Weitzer. 2004. "Multiple Surveys of Students and Survey Fatigue." *New Directions for Institutional Research* 2004 (121): 63–73.
PWC. 2017. *Strengthening digital society against cyber shocks - Key findings from The Global State of Information Security Survey 2018*. Online: Price Waterhouse Coopers https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf.
Ray, J. J. 1984. "The Reliability of Short Social Desirability Scales." *Journal of Social Psychology* 123 (1): 133–134.
Redmiles, E. M., Y. Acar, S. Fahl, and M. L. Mazurek. 2017. "A Summary of Survey Methodology Best Practices for Security and Privacy Researchers." *UM Computer Science Department Technical Reports*.
Reynolds, W. M. 1982. "Development of Reliable and Valid Short Forms of the Marlowe-Crowne Social Desirability Scale." *Journal of Clinical Psychology* 38 (1): 119–125.
Safa, N. S., R. Von Solms, and L. Futcher. 2016. "Human Aspects of Information Security in Organisations." *Computer Fraud & Security* 2016 (2): 15–18.
Scholl, M., K. Leiner, and F. Fuhrmann. 2017. "Blind Spot: Do you Know the Effectiveness of Your Information Security Awareness-Raising Program?" In *Proceedings of the 21st world Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017)*, 361–366. Orlando, Florida, USA: International Institute of Informatics and Systemics.
Sekaran, U., and R. Bougie. 2010. *Research Methods for Business: A Skill Building Approach*. 5th ed. Chichester, United Kingdom: John Wiley & Sons.
Shay, R., S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. 2010. "Encountering Stronger Password Requirements: User Attitudes and Behaviors." In *Proceedings of the Proceedings of the Sixth Symposium on Usable Privacy and Security*, 1–20. Redmond, Washington, USA: ACM.
Snyman, D. P., and H. A. Kruger. 2016. "Behavioural Thresholds in the Context of Information Security." In *Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 22–32. Frankfurt, Germany: Plymouth University.
Snyman, D. P., and H. A. Kruger. 2017a. "The Application of Behavioural Thresholds to Analyse Collective Behaviour in Information Security." *Information & Computer Security* 25 (2): 152–164.
Snyman, D. P., and H. A. Kruger. 2017b. "Optical Polling for Behavioural Threshold Analysis in Information Security." In *Proceedings of the International Conference on Information and Knowledge Engineering (IKE'17)*, 39–45. Las Vegas, USA: CSREA Press.
Snyman, D. P., H. A. Kruger, and W. D. Kearney. 2017. "The Lemming Effect in Information Security." In *Proceedings of the 11th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, 91–103. Adelaide, Australia: Plymouth University.
Sommestad, T., and J. Hallberg. 2013. "A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance." In *Proceedings of the IFIP International Information Security Conference*, 257–271. Auckland, New Zealand: Springer.
Sommestad, T., J. Hallberg, K. Lundholm, and J. Bengtsson. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies." *Information Management & Computer Security* 22 (1): 42–75.
Stanton, J. M., K. R. Stam, P. Mastrangelo, and J. Jolton. 2005. "Analysis of End User Security Behaviors." *Computers & Security* 24 (2): 124–133.
Tanis, M., and T. Postmes. 2005. "A Social Identity Approach to Trust: Interpersonal Perception, Group Membership and Trusting Behaviour." *European Journal of Social Psychology* 35 (3): 413–424.
Vance, A., and M. T. Siponen. 2012. "IS Security Policy Violations: A Rational Choice Perspective." *Journal of Organizational and End User Computing (JOEUC)* 24 (1): 21–41.
Van de Mortel, T. F. 2008. "Faking It: Social Desirability Response Bias in Self-Report Research." *The Australian Journal of Advanced Nursing* 25 (4): 40–48.

Appendix A

Social desirability scales

In case studies 2 and 3, the behavioural thresholds were adjusted to correct for and show the possible effect that social desirability has on the analysis of these thresholds. The table below lists the questions of the social desirability measurement instrument that is commonly used in literature. The questions to measure social desirability were based on a standardised 33 question measurement instrument, which was developed by (Crowne and Marlowe 1964) and later shortened to eight questions by (Ray 1984). These eight questions were used to measure social desirability in this research.

Social desirability questions (Ray 1984).

Appendix A1. Social desirability questions (Ray, 1984).

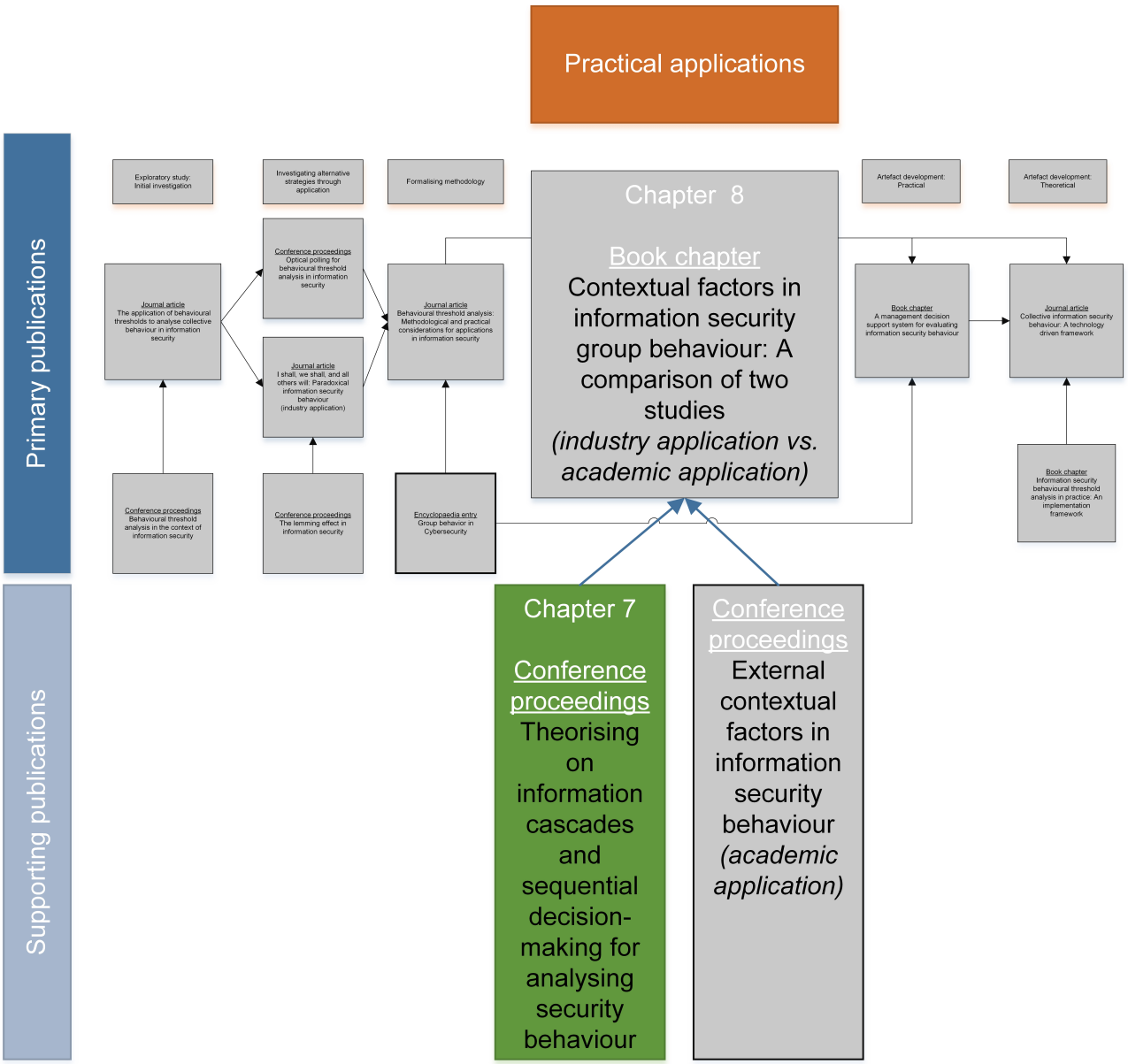
Social desirability questions	Scoring
1. Are you always courteous, even to people who are disagreeable?	Yes:**3** Unsure:**2** No:**1**
2. Are you always a good listener, no matter whom you are talking to?	Yes:**3** Unsure:**2** No:**1**
3. Are you quick to admit making a mistake?	Yes:**3** Unsure:**2** No:**1**
4. Have there been occasions when you took advantage of someone?	Yes:**1** Unsure:**2** No:**3**
5. Do you sometimes try to get even rather than forgive and forget?	Yes:**1** Unsure:**2** No:**3**
6. Do you sometimes feel resentful when you do not get your own way?	Yes:**1** Unsure:**2** No:**3**
7. Are you always willing to admit when you make a mistake?	Yes:**3** Unsure:**2** No:**1**
8. Have you sometimes taken unfair advantage of another person?	Yes:**1** Unsure:**2** No:**3**
	Min. score: **8** Max. score: **24**

In order to accurately measure the level of social desirability of a respondent, his/her responses to each question are scored on a scale of 1–3, based on their response of Yes, Unsure, or No.

The scores for all the responses are added and provide a possible score between 8 and 24. The higher a respondent's score on this scale, the higher the probability is that the respondent was not completely honest in answering the preceding questionnaire on information security behaviours.

In this research, only the highest possible score of 24 was taken as the cue to adapt responses to control for the possible effect of social desirability and was done in the following manner: If a respondent with a social desirability of 24 selected his/her inclination of participation for a negative information security behaviour, his/her response was adjusted upwards, e.g. a response indicated as *strongly inclined (3)*, was adjusted to *always (4)*. This translates to a *lower* behavioural threshold for participation than what the respondent originally reported. For positive behaviour the response is adapted downwards, e.g. from *strongly inclined (3)* to *somewhat inclined (2).* This is due to the high level of social desirability that causes the respondent to overstate his/her willingness to participate in the positive group behaviour. In these cases, the threshold for participation is taken at a *higher* percentage.

Chapter 7
-
Article V: Theorising on information cascades and sequential decision-making for analysing security behaviour



Chapter table of contents

7.1 Preamble to Article V 126

7.2 ICISSP conference proceedings style requirements 127

7.3 Article V 127

7.3.1 Introduction 128

7.3.2 Sequential decision-making 129

7.3.3 Illustrative case study 131

7.3.4 Reflection 133

7.3.5 Conclusion 134

7.3.6 References 135

7.1 Preamble to Article V

Up to this point, the progress in this research was firstly of an exploratory nature and subsequently of a more fundamental nature to establish the threshold model of collective behaviour as a recognised method in information security. Now that the approach has been formally defined, the focus of the research moves on to new *practical applications*. This phase comprises multiple publications, *i.e.,* two supporting publications and one primary publication. In this chapter, the first of the supporting publications is presented. This paper is still concerned with the theories that are involved in the formation of (information security) group behaviour and can therefore be viewed as part of the previous phase. However, a practical application is described and its results form part of the discussion of the related theory.

In this article, it is argued that individual behaviour formation in information security is often reliant on the example that is set by others. The observation of the behaviour of others and the influence on one's own behaviour can be described as sequential decision-making, *i.e.*, a decision that is made by one person informs the decision (and subsequent behaviour) of the next person. This process can be formally explained as an instance of information cascades. Information security behavioural threshold analysis (as conceptualised in Article IV) is proposed as a method for evaluating information cascades in the context of information security. The reasoned arguments put forth in this paper corroborate the appropriateness of behavioural threshold analysis as a valid and robust method for evaluating information security group behaviour.

Article V, *Theorising on information cascades and sequential decision-making for analysing security behaviour*[10]*,* was presented at the *5th International Conference on Information Systems Security and Privacy (ICISSP2019)* and published in the peer-reviewed proceedings of the conference. The conference was hosted in Prague, Czech Republic, from 23-25 February 2019.

The findings of this paper that the interactions between members of a group can be conceptually modelled and drive collective security behaviour, contribute to the remaining two publications in the following chapter.

[10] Snyman, D. P., & Kruger, H. A. 2019. *Theorising on information cascades and sequential decision-making for analysing security behaviour*. In Mori, P., Furnell, S. M., & Camp, O. Eds., Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP2019), Prague, Czech Republic, pp. 205-212.

7.2 ICISSP conference proceedings style requirements

The publications in the ICISSP conference proceedings are expected to conform to the SCITEPRESS proceedings style. Referencing is done in accordance with the American Psychological Association (APA) author, name system. The article is presented in its final edited and typeset form as it was published in the conference proceedings. Information regarding the author guidelines of the conference can be found in Appendix I.

7.3 Article V

Article follows on next page.

Theorising on Information Cascades and Sequential Decision-making for Analysing Security Behaviour

D. P. Snyman and H. A. Kruger
School of Computer Science and Information Systems, North-West University, 11 Hoffman Street, Potchefstroom, South Africa
dirk.snyman, hennie.kruger@nwu.ac.za

Keywords: Information Cascades, Sequential Decision-making, Information Security, Human Behaviour.

Abstract: Human behaviour is an ever-present aspect in information security and requires special attention when seeking to secure information systems. Information security behaviour is often based on an informed decision where information is obtained by previous experience and observation of the behaviour of others. In this research, the concept of sequential decision-making is contextualised in terms of information security behaviour. Information cascades, which are based on sequential decision-making, are theorised as a model to explain how decision-making (i.e. behaviour) takes place in terms of information security. A case study is presented to illustrate how behavioural threshold analysis can be employed as an instrument to evaluate the effect of information cascades and sequential decision-making on information security behaviour. The paper concludes by theorising on the applicability of the models and approaches that are presented in this research.

1 INTRODUCTION

A long-standing approach for protecting information systems was a focus on technical solutions. It was soon realised, however, that technical solutions alone were not sufficient to protect the systems and information from those who intend to access it without due authorisation (Arce, 2003; Lineberry, 2007; Soomro et al., 2016). Humans are inextricably linked to the creation and use of information systems. They are fallible by nature, and it is precisely this innate fallibility that can cause vulnerabilities in information systems, even when the systems are sufficiently protected by technological means (Glaspie and Karwowski, 2017). In a recent publication on information security threats, human conduct (mostly inadvertent behaviour) was responsible for more than two thirds of reported breaches in 2017 (IBM Security, 2018). These behaviours ranged from human error in server configurations, to human compliance with phishing attacks.

In order to attempt to address the human factor in information security, the phenomenon of human behaviour should first and fore mostly be understood. Researchers have long been seeking ways to formalise the study of human behaviour which gave rise to many theories and models that try to explain how behaviour is determined (Granovetter, 1978; Ajzen, 1991; Wilson, 1999; Kroenung and Eckhardt, 2015; Pham et al., 2017; Ooi et al., 2018). Such models are then used in an attempt to explain behaviour in terms of information security. Examples of the most prevalent of such models that have been used in this context include: The theory of reasoned action, the theory of planned behaviour, protection motivation theory, and general deterrence theory (Lebek et al., 2013; Pham et al., 2017).

These models aim to incorporate influencing factors that are intrinsic to an individual and describe how these factors contribute to the eventual behaviour. Ultimately, the behaviour that is performed is based on an informed decision by the individual. The application of the abovementioned models places a person in isolation, but this is seldomly, if ever, the case in a real-world situation.

The theories fail to consider the influence that the decisions of others might have on an individual. When decisions are no longer made in isolation, the direct application of these theories becomes problematic because the motivations for exhibiting a certain behaviour is no longer only an intrinsic one, but extrinsic factors now come into play. Information on the everyday decisions of others are

Snyman, D. and Kruger, H.
Theorising on Information Cascades and Sequential Decision-making for Analysing Security Behaviour.
In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, pages 205-212
ISBN: 978-989-758-359-9
Copyright © 2019 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

typically overt for an individual to observe, for instance, the choice in clothing brand, restaurant preferences, etc. These decisions in turn help determine the way in which someone would make his/her own decisions.

Information security behaviour is similarly based on an informed decision as mentioned above. Behaviour in this context is also not confined to an individual's intrinsic motivations but is similarly informed by the decisions that others make. The process of decision-making is often of a sequential nature, i.e. one decision informs the next, which in turn informs another. An individual bases future decisions on the knowledge of previous decisions.

Easley and Kleinberg (2010) describe the use of information cascades to formally model iterative, sequential decision-making of an individual in relation to decisions in a group. Information cascades, in short, refer to how an individual makes decisions (sequentially) based on the probability that the decision is correct, given the decisions previously made by others. This approach has never been used before to model information security behaviour but has been mentioned as a possible problematic phenomenon in relation to privacy and security (see Chesney and Citron (2018) on so-called "deep fakes" for a recent mention of information cascades in literature). Therefore, this paper aims to theorise on the applicability of information cascades as a technique to analyse information security behaviour.

The remainder of this paper is structured as follows: In **Section 2** an overview of the concept of sequential decision-making is presented, followed by an illustrative case study in **Section 3**. **Section 4** consists of a reflection on the implications of the study as well as the key contributions of this research is highlighted. The paper is concluded in **Section 5**.

2 SEQUENTIAL DECISION-MAKING

In this section, the concept of sequential decision-making is presented in a twofold manner. Firstly, sequential decision-making is discussed in terms of the information cascades model. Secondly, behavioural threshold analysis is presented as a possible instrument to measure sequential decision-making in information cascades, specifically in terms of information security.

2.1 Information Cascades

As mentioned in Section 1, information cascades refer to a formal expression of the process of sequential decision-making. The first mention and the development of information cascades (also called herd behaviour (Banerjee, 1992)) has its origins in the field of Economics to describe, among other things, investment decisions and consumer fads (Bikhchandani et al., 1992; Welch, 1992).

For the sake of the arguments of this paper, a simple, general, description of information cascades is subsequently presented. The aim of this description is to provide a high-level overview of the model and to create an analogy to relate information cascades to information security. The description is based on the explanation of Easley and Kleinberg (2010). They provide a more detailed explanation with mathematical substantiation of the model for further reading.

The decisions of a person are informed by signals, i.e. information, in relation to an expected gain. These signals come in two forms, namely private- and public signals. A private signal is information that is currently known to the person, be it a belief or a fact. When a person makes a decision in isolation, a private signal is what determines the outcome of the decision. When the signal aligns with an associated gain and is powerful enough to overcome the risk associated with potential loss, the decision is made solely on the information conveyed by the signal.

Easley and Kleinberg (2010) note that everyday decisions are rarely made in isolation from the rest of society. Information can be conveyed by signals that are formed extrinsically. Such public signals are based on information that does not come from the individual, but rather from the observation of the decisions that others have made. In a public setting, both private- and public signals will inform the decision. If the signals indicate the same course for the decision, the outcome is obvious but if the two signals provide contrasting information, the strongest signal will inform the decision. It is important to note that both signals are normally imperfect and do not convey infallible information. The signal is always weighed against the probability that the corresponding course for the decision will result in gain, rather than loss.

Due to the sequential nature of decision-making, the public signal becomes stronger with each decision that was made in its favour. The decision-maker is aware of all the public decisions, each one informed by the previous. As a result, the perceived

probability that the public signal suggests the "correct" course for the decision becomes higher.

The main premise of the model, therefore, is that the public signal will almost always prove stronger and influence the decision even when the private signal initially informed a contrasting course.

Information cascades rely on four prerequisites for the model to be applied to a situation (Easley and Kleinberg, 2010):

1) There is a (binary/contrasting) decision to be made;
2) Each person has a private signal that originally informs their initial proclivity;
3) The decisions that were made by others can be observed and the decisions happen sequentially; and
4) The private information of others is not known to the individual.

However, inferences can be made about another's private information based on their publicly noticeable decision from number 3 above.

Take, for instance, an example of adopting new technology. An individual, let us call him John, is looking for a new digital device and has an expectation of the utility (gain) that the new technology will have to him. He reads an online review of the device which indicates that the technology is in its infancy and it might be better to wait for revisions, rather than adopt the technology in its current form. John then forms a negative, personal signal because of the perceived lack of utility. The information that the signal relays prevents him from adopting the technology.

As stated before, John is not in isolation. He moves around in public spaces and notices that another person has one of the devices in their possession. He has, however, no sense of whether the other person is happy with the purchase (i.e. the decision to adopt was the correct decision to make), and he does not know what the private signal of the other person was that convinced him/her to adopt the technology. Instead, John receives a positive public signal that indicates that adoption of the technology has happened. As he encounters and sees more people that have adopted the technology, the higher the probability becomes that adoption, rather than rejection, is preferable and the signal becomes stronger.

As soon as the public signal becomes stronger than the private and overcomes the associated risk with adoption, John will make the decision to follow the group of adopters and adopt the technology. The prerequisites for an information cascade, mentioned above, have been met and an information cascade has taken place.

An example of how information cascades can be evaluated and, possibly, predicted is the application of behavioural threshold analysis. This is discussed in the following sub-section.

2.2 Behavioural Threshold Analysis

From the brief description in Section 2.1, it is clear that information cascades and sequential decision-making may play a significant role in information security behaviour. However, to do a meaningful evaluation thereof, in a way that provides new insights into information security behaviour and specifically paradoxical information security behaviour, an acceptable method for analysing information cascades should be found. One possible approach is to use behavioural threshold analysis which is also based on sequential decision-making. In this section, behavioural threshold analysis is introduced briefly as a possible instrument to evaluate information cascades. Parallels are also drawn between information cascades and behavioural threshold analysis to support the idea of behavioural threshold analysis as an evaluation instrument for information cascades and, specifically, sequential decision-making.

The notion of behavioural threshold analysis pre-dates the conceptualisation of information cascades by some time. Behavioural threshold analysis was first developed by Granovetter (1978) and was coined "threshold models of collective behaviour". The premise supporting the model of threshold analysis, is that the behaviour of an individual (Sarah) in a group setting will be influenced by the group's behaviour if a large enough number of other members of the group exhibit a specific behaviour. The number of others that must perform a behaviour before Sarah joins in, is determined by her inherent threshold for participation. If the number of others in the group that perform a certain action, exceeds Sarah's threshold for participation, she will follow the group and also perform the action. To demonstrate the similarities between information cascades and behavioural threshold analysis, an example of behavioural threshold analysis (in terms of information security behaviour) is presented.

Information cascades, in information security behaviour, can manifest itself when employees in a group setting, follow the security behaviour of others rather than relying on their own knowledge. This is similar for behavioural thresholds:

Information security awareness training is often conducted in organisations to educate employees on

basic security hygiene (Alshaikh et al., 2018). Topics such as password sharing, incident reporting, and responsible social media use are commonly addressed in these training programs. Sarah has undergone the training, and she internalises the content. She forms an informed opinion on the related practices and the associated risks (comparable to the risk/gain from information cascades that was mentioned earlier). When she is confronted with either performing, or abstaining from a certain information security behaviour, a contrasting decision (as with information cascades) is to be made. Sarah is not in isolation and she is aware of the actions that other people in her group perform (public signal). Her inherent threshold for participating in the behaviour (private signal) will be weighed against the number of others in the group that perform the action. Sarah *is not* aware what the motivations of the other group members (i.e. their own private signals) are for why they exhibit the behaviour, but she *is* aware of what their decision for behaviour was. If her threshold number (private signal) is exceeded by the number of group members (public signal), Sarah will follow the group example for the behaviour.

This parallel between the two models indicate that they are both applicable to sequential decision-making. The situations in which behavioural threshold analysis can be performed, satisfy the prerequisites for an information cascade to occur, i.e. both models depend on a person to make a contrasting decision, given both intrinsic and extrinsic evidence that inform the decision. Finally, the intrinsic basis for said evidence is not known, but the evidence is clear to see.

Behavioural threshold analysis therefore seems like a feasible approach to provide a mechanism by which information cascades may be evaluated. In the following section, a case study is presented to support this claim.

3 ILLUSTRATIVE CASE STUDY

To illustrate how behavioural threshold analysis can be used to evaluate information cascades, a case study was conducted and is presented below in terms of the experimental setup, followed by the results obtained.

3.1 Experimental Setup

Behavioural threshold analysis depends on the availability of information about the thresholds of the the members of a group (Granovetter, 1978). One way to obtain their threshold information is by surveying the group by means of a self-reporting questionnaire (Growney, 1983). An exploratory study (Snyman and Kruger, 2016) on the application of behavioural threshold analysis in the context of information security has, however, determined that the measurement instrument that was offered by Growney may not be suitable when applied in a context which is sufficiently different from its initial intended use. This has prompted on-going reflection on, and development of, a measurement instrument for use in this specific context. In its current form, the instrument suggested by Growney (1983) asks respondents to directly nominate their threshold for the number of group members that have to perform an action before they will follow suit. Snyman and Kruger (2016) found that respondents were confused by this style of questioning which lead to inaccurate responses. For this research, based on the ongoing development, it was opted to alter the measurement instrument in order to guide the respondents in answering what their thresholds are. This was achieved in the following way:

The respondents were asked to rate their willingness to follow the group example on a four-point Likert scale, i.e. *1. Never*, *2. Somewhat inclined*, *3. Strongly inclined*, and *4. Always*. Their willingness for participation in the group behaviour was recorded for different threshold level intervals, e.g. rate your willingness to not report security incidents if 31-40% of group members fail to report security incidents. Formally, the question was presented as follows:

How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?

An example of how the question, response scales, and threshold intervals are incorporated in an online questionnaire is presented in Figure 1.

In order to determine the minimum threshold level for participation, all responses of a *2. Somewhat inclined* and above for a specific threshold interval were taken to mean that the respondent will be influenced by the group if that percentage of group members participate in the specific action. For this illustrative case study The abovementioned approach was applied in a real-world setting by distributing an online questionnaire to contract employees within a company. The identity and other information of the company is not revealed to comply with a confidentiality agreement.

The employees whom were surveyed, typically

Incident reporting

How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them? *

	1. Never	2. Somewhat inclined	3. Strongly inclined	4. Always
0-10%				
11-20%				
21-30%				
31-40%				
41-50%				
51-60%				
61-70%				
71-80%				
81-90%				
91-100%				

Figure 1: Example of questionnaire layout.

work together in a group (in a departmental setting). They were asked to rate their willingness to participate in group information security behaviour that relates to the non-reporting of information security incidents. Willingness, in this context, relates to the likelihood that an individual will not report a security incident, given the number of other group members that also do not report security incidents.

Responses were obtained from a group of 33 employees. Contrary to the typical expectation for sample sizes relating to questionnaires, the nature of behavioural threshold analysis actually *requires* a smaller number of respondents but all the while imposes another unique requirement: The group members are required to have a knowledge of the behaviour of the other group members (recall the discussion on public signals from Section 2). This requirement determines that behavioural threshold analysis be performed with a group that have regular interaction with one another. In a company setting, this typically relates to business units or departments. Furthermore, the analysis of responses and any group behaviour prediction that is based thereon, is only applicable to the group that was surveyed and therefore the findings of behavioural threshold analysis are not generalised to a greater population. This means that regular guidelines of sample size versus greater population size do not apply in this context.

The behavioural thresholds were noted for each respondent after which a graph of the cumulative distribution of thresholds was constructed (see Figure 2). In the next section, the results that were obtained for the experiment are presented and discussed in short.

3.2 Results

Figure 2 shows the employees' cumulative behavioural thresholds for not reporting security incidents, given the number of others that do not report security incidents. On the y-axis, the percentage of participants in the behaviour is shown. The x-axis represents the different threshold-levels, also expressed as a percentage, e.g. the point X on the graph indicates that 36% percent of the group will not report security incidents if 30% of the group do not report such incidents. The different cumulative threshold levels that are shown, were joined with a line to aid in the interpretation of the graph. A uniform cumulative distribution of thresholds was also plotted on the graph as a dotted line. This in known as the equilibrium line. The equilibrium line refers to a collection of points with equal numerical coordinates (Granovetter, 1978; Growney, 1983), i.e. $x=y$ where the number of participants in a behaviour and the threshold levels intersect. When the number of participants becomes equal to an individual's threshold level, they will start to participate in the group behaviour.

When the threshold line (i.e. the cumulative distribution function $F(x)$) intersects with the equilib-

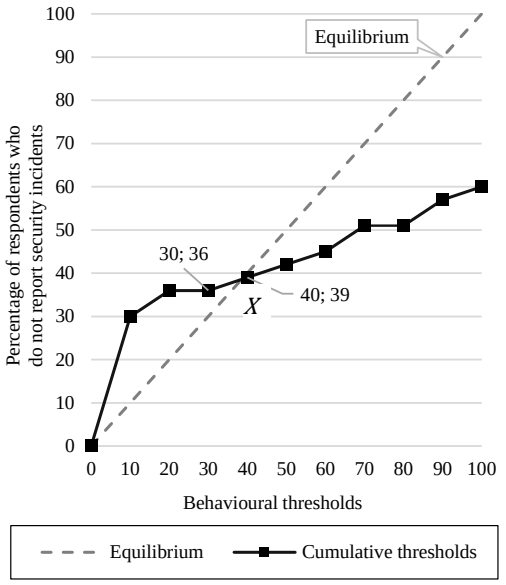


Figure 2: Cumulative threshold graph for information security behaviour (incident reporting).

rium line, where $F(x)=x$, certain inferences can be made about the group behaviour, based on the line-segments to the left and right of the intersection (Granovetter, 1978; Growney, 1983). The gradient of the line-sections determines whether a stable equilibrium is reached. When a stable equilibrium is reached, the number of participants (y-axis) at that intersection indicates to which extent the participation rate of the group is likely to grow. In other words, how many people will be influenced by the sequential decision-making cascade until the cascade eventually stops.

In Figure 2, the intersection of the two abovementioned lines occurs at the point *X* (40,39). The gradients of the line-segments indicate a stable equilibrium is reached. The equilibrium-state may be interpreted as an indication that sequential decision-making will influence up to 40% of the group to not report security incidents.

Many other explanations and deductions can be made from the graph but are limited to only those mentioned above due to space considerations. For a more comprehensive discussion on how behavioural threshold analysis graphs can be used and analysed, refer to the work of Growney (1983) and Granovetter (1978).

4 REFLECTION

4.1 Theoretical Implications

The arguments in this paper are of an introductory nature and attempt to explore new ideas that can help with the problem of human information security behaviour, which is often paradoxical. While no-one doubts the importance of the human factor in information security, it appears that the models used to explain it (theory of planned behaviour, protection motivation theory, etc.) have a disadvantage because they do not specifically take into account sequential decision-making and the influence of other people's decisions.

Information security behaviour is essentially a decision-making process where one must decide whether or not to perform an information security behaviour. When people work in a group setting and are aware of what other employees are doing (deciding) then the problem will be further compounded by sequential decision-making aspects of their co-workers. In order to ultimately be applied to information security behaviour, these principles for sequential decision-making will first have to be understood, and secondly be evaluated. This brings forth a new problem of *how* to understand it and *how* to evaluate it.

The principle of information cascades is presented in this article as one possible way of trying to understand information security behaviour and sequential decision-making specifically. The principles of how information cascades work as well as the four prerequisites (Section 2.1) for an information cascade fits the problem of information security behaviour (especially in a group or departmental setting where people can observe others' behaviours and decisions). Information cascades therefore provide a possible solution for understanding information security behaviour under certain circumstances.

In order to address the “how to evaluate” problem, the principles of information security behavioural threshold analysis are offered as a viable evaluation tool. Section 2.2 explained the concept of information security behavioural thresholds and indicated that there exists a parallel between information cascades and information security behavioural thresholds in terms of sequential decision-making. Section 3 then presented a practical case study on how to measure and evaluate sequential decision-making by applying information security behavioural threshold analysis.

The results indicated that sequential decision-making in a group influences the individual to follow the group example in matters of information security behaviour. The extent of an information cascade that takes place may be determined with the use of behavioural threshold analysis.

Behavioural threshold analysis may, therefore, contribute to understanding information cascades and may serve to help predict the extent to which such a cascade may influence a group's behaviour.

4.2 Application Challenges

Behavioural threshold analysis in itself is still under continual development and therefore it brings about its own challenges in terms of its application as a method to analyse sequential decision-making and information cascades. Some of the related risks and vulnerabilities relating to behavioural threshold analysis include, among others, the following:

-The respondents in a behavioural threshold analysis exercise need to have an intimate knowledge of the behaviour of the other group members. Due to their proximity in a group, the required level of knowledge is presumed. However, if this is not the case the results of the threshold analysis may be flawed;

-Even though the number of participants in threshold analysis is intentionally kept small, too small a number will not allow for accurate analysis;

-Due to generalisation to a greater population being disallowed, little information about the behaviour of one group becomes clear by surveying another group, e.g. performing behavioural threshold analysis for the finance department does not necessarily convey information on the IT department, for instance or about the company as a whole;

-No universal measurement instrument for behavioural threshold analysis currently exists. Even though there is continual development, these instruments may need to be customised for each application; and

-Respondents may not always be truthful in their responses to questionnaires due to a perceived correct or expected answer that the researcher would like to see. This phenomenon is called social desirability. Mechanisms to test for social desirability may be investigated to control for the occurrence thereof.

4.3 Contributions

The main contributions of this paper can be summarised as follows:

-As described in this paper, this research is the first to attempt to link sequential decision-making, and specifically information cascades, with information security behaviour and to show a possible explanatory relationship between the two;

-Sequential decision-making and information cascades provide a model to understand and evaluate (often paradoxical) information security behaviour;

-This study suggests a solution on how to evaluate sequential decision-making by means of an information security threshold model. This suggested solution is explained, motivated, and illustrated by presenting an investigative real-life case study; and

-By theorising on concepts like information cascades and information security thresholds, this research can potentially create new avenues for further research and enquiry which in turn might provide new insights on the problem of paradoxical information security behaviour.

5 CONCLUSION

This paper explored the possible influence of information cascades in security behaviour. Section 1 contextualised the research in the domain of human aspects of information security. In Section 2, the concept of sequential decision-making was presented. Two models were presented that aim to describe sequential decision-making in a group context, namely information cascades, and behavioural thresholds. These two models were shown to be mutually inclusive. An illustrative case study, to indicate how behavioural threshold analysis may be used as an instrument to evaluate information cascades and sequential decision-making was presented in Section 3. In Section 4, a reflection on the theoretical implications and practical challenges of this research is discussed, and the section concludes with a summary of the contributions of this paper.

Sequential decision-making and information cascades may contribute to how individuals determine their behaviour in terms of information security. Behavioural threshold analysis may contribute to understanding information cascades as the two approaches share many similarities and are applicable under the same circumstances. The findings of this research are still in its infancy and should therefore be understood as such. The theories and concepts that are discussed in this paper, warrant

further investigation in order to better understand the implications thereof.

REFERENCES

Ajzen, I. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50**,** 179-211.

Alshaikh, M., Maynard, S. B., Ahmad, A. and Chang, S. 2018. An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations.

Arce, I. 2003. The weakest link revisited [information security]. *IEEE Security and Privacy*, 99**,** 72-76.

Banerjee, A. V. 1992. A simple model of herd behavior. *The quarterly journal of economics*, 107**,** 797-817.

Bikhchandani, S., Hirshleifer, D. and Welch, I. 1992. A theory of fads, fashion, custom, and cultural change as informational cascades. *Journal of political Economy*, 100**,** 992-1026.

Chesney, R. and Citron, D. K. 2018. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *107 California Law Review (2019, Forthcoming); U of Texas Law, Public Law Research Paper No. 692; U of Maryland Legal Studies Research Paper No. 2018-21*.

Easley, D. and Kleinberg, J. 2010. *Networks, crowds, and markets: Reasoning about a highly connected world*, Cambridge University Press.

Glaspie, H. W. and Karwowski, W. Human Factors in Information Security Culture: A Literature Review. In *Advances in Human Factors in Cybersecurity: International Conference on Applied Human Factors and Ergonomics (AHFE 2017)*, 2017 Los Angeles, CA, USA. Springer, 269-280.

Granovetter, M. 1978. Threshold models of collective behavior. *American Journal of Sociology*, 83**,** 1420-1443.

Growney, J. S. 1983. *I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior*, Bedford, MA, COMAP Inc.

IBM Security 2018. *IBM X-Force Threat Intelligence Index 2018: Notable security events of 2017, and a look ahead*. USA: IBM Corporation.

Kroenung, J. and Eckhardt, A. 2015. The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship. *Information and Management*, 52**,** 611-627.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M. and Hohler, B. Employees' information security awareness and behavior: A literature review. In *46th Hawaii International Conference on System Sciences (HICSS)*, 2013. IEEE, 2978-2987.

Lineberry, S. 2007. The human element: The weakest link in information security. *Journal of Accountancy*, 204**,** 44.

Ooi, K.-B., Hew, J.-J. and Lin, B. 2018. Unfolding the privacy paradox among mobile social commerce users: a multi-mediation approach. *Behaviour and Information Technology*, 37**,** 575-595.

Pham, H., Brennan, L. and Richardson, J. Review of Behavioural Theories in Security Compliance and Research Challenge. In *Informing Science and Information Technology Education Conference, Vietnam*, 2017 Santa Rosa, CA, USA. Informing Science Institute, 65-76.

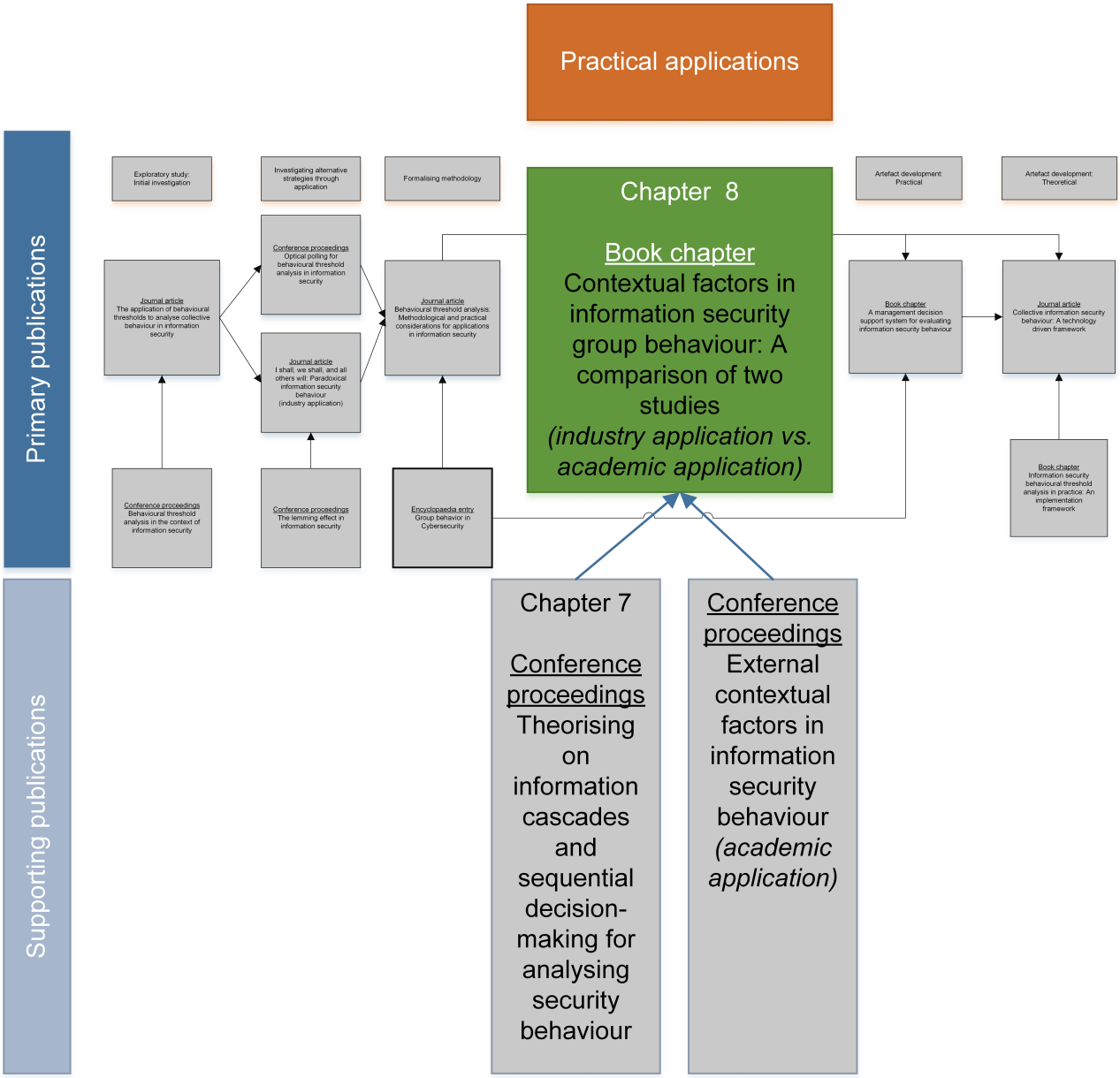
Snyman, D. P. and Kruger, H. A. Behavioural thresholds in the context of information security. In *10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 2016 Frankfurt, Germany. Plymouth University, 22-32.

Soomro, Z. A., Shah, M. H. and Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36**,** 215-225.

Welch, I. 1992. Sequential sales, learning, and cascades. *The Journal of finance*, 47**,** 695-732.

Wilson, T. D. 1999. Models in information behaviour research. *Journal of documentation*, 55**,** 249-270.

Chapter 8
-
Article VI: Contextual factors in information security group behaviour: A comparison of two studies



Chapter table of contents

8.1 Preamble to Article VI 138

8.2 Springer book chapter style requirements 139

8.3 Article VI 139

8.3.1 Introduction 140

8.3.2 Information security behaviour: a product of circumstance? 142

8.3.3 Experimentation 145

8.3.4 A comparison of two studies through behavioural threshold analysis 150

8.3.5 Discussion 154

8.3.6 Conclusion 157

8.3.7 References 159

8.3.8 Appendix 161

8.1 Preamble to Article VI

Continuing the *practical applications* phase of this research, this chapter is dedicated to the second full-scale application of information security behavioural threshold analysis in practice (recall that Chapter 5 described the first). In the previous chapter (Article V), it was described how the behaviour of people in a group could determine the behaviour formation for an individual who is exposed to the group behaviour to a considerable extent. It would follow logically that the presence of the group can be regarded as an external influence. An individual is inextricably interconnected with his/her environment and a mutual influence is constantly being exerted. The role and influence of the environment (context) where an individual finds him-/herself on his/her behaviour (specifically with reference to information security behaviour) are investigated in this paper. The premise of the threshold model is that the individual will follow the group example and that behavioural threshold analysis can predict the eventual collective behaviour of the group.

A practical experiment was conducted in an academic residence setting where students live together while pursuing their studies. These students are representative of tomorrow's workforce and this environment was chosen due to the contrasting characteristics of such living arrangements when compared to the environment of co-workers in a corporate setup. The resulting behavioural threshold evaluation was compared against the industry experiment from Article III, Chapter 5, to assess how the differences in environment, *i.e.*, contextual factors, result in different information security group behaviour between the two groups. The methodology for applying behavioural threshold analysis in information security, as established in Article IV, Chapter 6, was used as the theoretical underpinning for the experiments.

Article VI was originally presented at the *6th International Conference on Information Systems Security and Privacy (ICISSP 2020)* from 25-27 February 2020, and published in the peer-reviewed conference proceedings as *External contextual factors in information security behaviour*[11]. The conference chairs identified the very best, high quality papers from the conference to invite for further publication in a Springer book series named *Communications in Computer and Information Science*. The criteria for selection included recommendations from the session chairs, classifications and comments from the programme committee members, and finally the conference chairs' global view of all the papers in the technical programme. The revised and extended version of the paper, *Contextual factors in information security group behaviour: A comparison of two studies*[12], is presented here as Article VI. This book chapter was still under

[11] Snyman, D. P., & Kruger, H. A. 2020. *External contextual factors in information security behaviour*. In Furnell, S. M., Mori, P., Weippl, E., & Camp, O. Eds., Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), Valletta, Malta, pp. 185-194.

[12] Snyman, D. P., & Kruger, H. A. 2020. Contextual factors in information security group behaviour: A comparison of two studies. Submitted to *Communications in Computer and Information Science*. Springer International Publishing.

review at the time of compiling the thesis. The original conference contribution in the proceedings is presented in Appendix D.

8.2 Springer book chapter style requirements

The Springer book chapter style requirements determined the use of the Lecture Notes in Computer Science reference style. The article is presented in its pre-published form as it was submitted to the Springer book series. Information regarding the author guidelines of the publication can be found in Appendix J.

8.3 Article VI

Article follows on next page.

Contextual factors in information security group behaviour: A comparison of two studies

Dirk Snyman[0000-0001-7360-3214] and Hennie Kruger [0000-0001-8514-4422]

North-West University, School of Computer Science and Information Systems,
11 Hoffman Street, Potchefstroom, 2531, South Africa
dirk.snyman;hennie.kruger@nwu.ac.za

Abstract. Group behaviour is a relatively under researched field in research pertaining to information security. Most behavioural studies in information security focus on the individual and how he/she reasons and eventually behaves. Recent investigations into security group behaviour have revealed that the context within which the members of a group function plays an important role. Behavioural threshold analysis has been identified as a possible tool to evaluate security group behaviour and provide insights into the possible influence of the group's contextual milieu. Based on earlier research on contextual factors in information security, this paper embodies an elaboration on the theoretical and practical implications of the previous work by comparing two distinct information security group behaviour experiments. The contextual environments for the two experiments include a group of employees in an industry setting, as well as a group of students that reside together in a university residence. These experiments are discussed, firstly by looking at the information security behavioural threshold analysis results for the two groups, and secondly, by expounding on the external contextual factors that play a part in the formation and eventual practice of information security behaviour in a group setting. The paper concludes by reflecting on the research aims and possible future work. This research has shown that external contextual factors play an important role in information security group behaviour and its effect should be taken into account in the strategies of managing information security.

Keywords: Information Security Behaviour, Contextual Factors, Human Factor in Information Security.

1 Introduction

Human behaviour remains one of the more challenging information security aspects to understand and, by extension, to manage [1]. Issues that complicate the understanding thereof, include phenomena such as the privacy paradox, i.e. willingly providing your own sensitive information in the full knowledge that it is unwise to do so [2]. Differences between the behaviour of individuals in seclusion, in contrast to group behaviour, is another contributing factor that hampers the effective management of the human factor, which is further exacerbated by the influence of external contextual factors. The

circumstances and setting in which attitude and intention towards human behaviour is formed has a marked effect on the behaviour that is eventually acted upon. The way in which one behaves in a social setting among friends surely differs from the sort of behaviour one exhibits in a corporate environment. This difference in behaviour is due to the contextual factors that are different between the two settings.

In terms of the information security behaviour of individuals, many attempts to understand its nuances exist. Often, psychological models are used to examine how intention, and eventually behaviour, is formed as part of an individual's cognition. This theoretical foundation sees many recurring models that guide information security behaviour research, notably knowledge, attitude, behaviour (KAB), the theory of reasoned action (TRA), protection motivation theory (PMT), and the theory of planned behaviour (TPB) [1, 3]. Once a model is selected, it is used to try to explain both cases of straightforward security behaviour where the motivations for behaviour are uncomplicated, but it is also used to understand paradoxical behaviour where the reasoning behind the behaviour and the behaviour itself, seem contradictory. For the evaluation of group behaviour, models like that of [4] and recently [5], that contemplate the use of threshold analysis to explain the intricacies of group behaviour in information security exists. Similarly, there is also research such as that of Willison and Warkentin [6], supported by more recent research [7-9] that indicate the need to understand the context and contextual factors to be able to better evaluate and comprehend information security (group) behaviour.

In an attempt to contribute to the abovementioned body of knowledge, this paper constitutes an extension of previously published work by Snyman and Kruger [10]. This extension draws on the theoretical foundations as described in [10] but augments the understanding of the practical implications by providing more in-depth results and discussions on the contextual factors that influence information security behaviour. Furthermore, the results from the previous work are expanded here to include more examples of information security group behaviour focus areas and are compared to that of another practical application by providing a two-fold comparison by 1) comparing the results of the two studies in terms of the predicted information security behaviour of the two groups, and 2) discussing the similarities and differences in the contextual factors of the two studies as described in the previous research.

The aim of this study is therefore to firstly, theorise on the external contextual factors that will influence information security behaviour, and secondly, to present the application of a model that considers external contextual factors in the prediction of group behaviour in information security. Thirdly, and finally, to compare the group behaviour of two distinct groups, based on the aforementioned model and discuss the influence that the identified contextual factors might have on the security behaviour of said groups.

The remainder of the paper is structured as follows: Section 2 gives an introductory overview of contextual factors that typically influence human behaviour and indicates its relevance in information security behaviour., In Section 3 a short overview of the experimental background for evaluating group behaviour, the contextual environments, and behavioural threshold analysis is given, while Section 4 provides a comparison of the experimental results from Section 3. Section 5 reflects on the underlying contextual

factors that influence information security group behaviour and a final reflection on the contributions made in this research conclude the study in Section 6.

2 Information security behaviour: a product of circumstance?

Exploiting the preceding, related work [10], the concept of contextual factors in information security behaviour is revisited in this section. The contextual factors that were identified in [10], were based on the initial influential work of Belk [11], which were also used in a more recent study by Kirova and Thanh [12] to investigate the influence of contextual factors on smartphone use.

The five contextual factors which they identified were:

- *Physical milieu;*
- *Social milieu;*
- *Perspective of elapsed (or remaining) time;*
- *Individual predisposition; and*
- *Individual intention.*

Following a critical reflection on these identified contextual factors, with due consideration of the predominant psychological theories and approaches to evaluating information security behaviour, an emergent taxonomy became apparent. This allows for the classification of the five contextual factors as being either intrinsic or extrinsic to an individual and were grouped as follows in Table 1:

Table 1. Categorisation of contextual factors in behaviour [10].

Contextual factors in behaviour	
Extrinsic factors	***Intrinsic factors***
Physical milieu	Perspective of elapsed (or remaining) time
Social milieu	Individual predisposition
	Individual intention

Many of the aforementioned psychological models and theories already address the intrinsic factors when used to evaluate information security behaviour, e.g. individual predisposition (which relates to intention). Intention is one of the core indicators which guides behaviour in the TPB. In contrast thereto, the extrinsic factors are not explicitly provided for in these frameworks.

Due to the fact that intrinsic factors are commonly considered in these theories, the focus of this research revolves around the extrinsic factors and how they influence behaviour with specific reference to information security behaviour. A short description is provided below for each of the extrinsic factors from Table 1:

The material environment in which an individual functions, comprises their *physical milieu.* The corporeal experiences of the individual, based on their sensory perception, are relevant here. These experiences include, what a person, feels (both in terms of touch and emotion), hears, tastes, and smells.

Social milieu refers to the effect of other people in the environment of an individual. Others may be present in the physical milieu, thereby directly influencing the behaviour of an individual by his/her exposure to their example. The social milieu can also extend beyond the physical proximity of an individual to include, for example, interactions across digital communication channels. The other people that influence the individual's behaviour may either be formal acquaintances including their close social network or may be strangers with whom the individual has (coincidental) contact.

In terms of information security behaviour, it is imperative to understand how these external factors manifest in the environments where security behaviour is performed. For instance, the physical milieu also includes aspects that may be considered intangible in terms of a person's senses, e.g. ease of access to systems and information can be thought of as part of the physical milieu as it relates to processes in the physical world. Similarly, interactions that relate to the social milieu of information security behaviour do not only refer to the overtly observable actions of others, but also incorporate aspects of an interpretive nature, e.g. social cues such as body language, and (implied) peer pressure.

Table 2 shows some examples of what these factors might look like in terms of information security behaviour as conceptualised by the authors. The conceptualisation is based on the extrinsic contextual factors as identified from the work of Kirova and Thanh [12]. The extrinsic factors that are shown here do not comprise an exhaustive list. Depending on the specifics of different scenarios, many other examples may exist.

Table 2. Extrinsic contextual factors in information security behaviour (adapted from [10]).

Extrinsic contextual factors in information security behaviour	
Physical milieu	***Social milieu***
– Ease of access to systems, processes and people. – Level of convenience associated with certain tasks. – Availability of technical expertise. – Presence of security controls.	– Peer pressure – Presence of co-workers/family/friends. – Organisational structure. – Required to work together with others. – Collective purpose. – Exposed to the actions/behaviours of others.

In a related study, Snyman and Kruger [13] investigate information security behaviour in terms of the TPB model. In contrast to other studies that use TPB as the underlying theoretical framework, their study theorises that TPB on its own is not sufficient for evaluating behaviour. They argue that (external) contextual influences should be taken into account in conjunction with the intrinsic motivations that form the basis of the model. The effect that contextual factors might exert on the eventual behaviour is only

discussed on a theoretical level and was not specifically applied in practice. Expanding upon their theoretical work and incorporating the two external contextual factors that are identified in this research, it will inform the practical part of this study.

To contextualise the TPB (as applied in [13]) with the current research presented in this paper, a graphical depiction is provided in Figure 1.

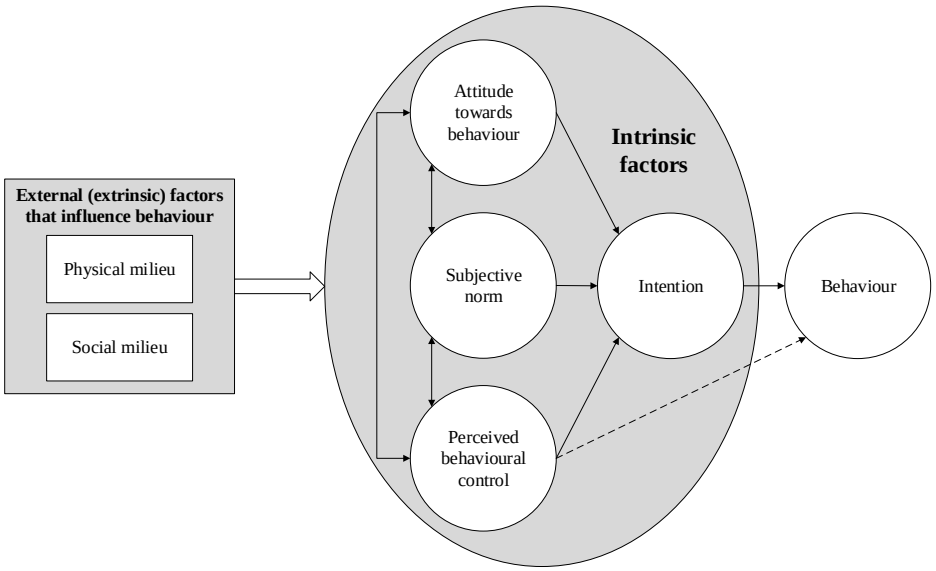


Fig. 1. Conceptual model of the influence of contextual factors in relation to the TPB [10].

Figure 1 shows a conceptual diagram in which the external contextual factors in this research, relates to the TPB and the intrinsic contextual factors that are implicitly included therein. The intrinsic factors form the basis for the establishment of intention (informed by attitude, norms, and perceived behavioural control) and ultimately the resulting behaviour. All the while, the intrinsic factors being affected by the external factors. An approach for evaluating group behaviour, identified in [13] as being able to implicitly encapsulate the influence of external factors, was first proposed by Granovetter [4]. The model is known as Threshold models of collective behaviour.

Granovetter [4] contends that behaviour and the underlying motivation for behaviour is rarely self-informed. Behaviour is said to be the product of circumstance, where circumstance (an extrinsic factor) refers to the observed, or perceived, behaviour of others. Given a situation with only two possible avenues of behaviour (i.e. acting or choosing not to act), an individual is thought to always try to enhance their efficacy in the given situation by electing how to behave, based on the perceived risk versus reward in choosing one alternative over the other.

Arguably, one would always choose the behaviour with the highest associated benefit, relative to the associated cost. However, as the number of individuals that perform one of the behaviours increases, the perceived benefit of also participating in the behaviour increases along with it. Even if the cost was initially, and in reality, probably

still is higher than the benefit. The decision-making process is often taking place subconsciously and is said to be based on the concept of behavioural thresholds.

Granovetter [4] hypothesises that each individual has an intrinsic threshold for participation in behaviour. In a group setting, the aforementioned mechanism of determining behaviour changes due to the influence of external contextual factors as the behaviour of other people become part of the equation. Choosing which behaviour to act on becomes a function of one's intrinsic threshold, expressed as the number of other people that should first be engaging in a behaviour before the associated benefit will outweigh the cost in one's mind. Once the number of actors in a behaviour outweighs one's threshold, participation in the behaviour becomes almost inevitable. When left to their own devices, without any external influence, an individual will mostly follow their own perception of cost versus benefit and choose in favour of the behaviour with the highest perceived benefit. Such individuals may be referred to as instigators. In a group setting, instigators are required to be the initial catalyst that influences others to follow their example. This specifically holds true for situations where the cost of participation is particularly high and very few individuals will participate of their own accord.

In order to apply this theoretical model in a real-world situation, behavioural threshold analysis is employed. This analysis entails that the threshold values for participation in a behaviour is known for each of the group members and is dependent on, and specific to, the composition of individuals that constitute the group. The process by which these individual thresholds may be elicited from the group members by means of self-reporting questionnaires is presented in [5]. Given the individual thresholds, mathematical aggregation is used to provide an outlook for the eventual group behaviour.

To relate the threshold model and analysis of Granovetter [4] back to information security, two practical exercises were conducted which are described in the following section.

3 Experimentation

This section describes two information security group behaviour experiments with reference to the experimental setup, contextual factors, and behavioural threshold analysis.

3.1 Experimental setup

To practically evaluate the idea of external contextual factors and to see the influence of these factors on the information security behaviour of people in groups, behavioural threshold analysis exercises were conducted in two discrete organisational settings i.e. an academic setting, specifically where students live together in a university residence, and an industry setting where people work together.

The first experiment [10] was conducted to examine the information security behaviour of students at a predominantly residential university in South Africa. The threshold questionnaires were digitally distributed to residents at a single-sex (male) university residence. A group of students were asked to distribute the questionnaire in the resi-

dence and ask willing participants to forward the questionnaire to other possible candidates in the residence. Participation was voluntary and all responses were anonymous. Due to the relatively sensitive nature of questions that relate to personal information security behaviour, along with participation not being compulsory, suitable responses were obtained from 52 respondents This resulted in a notional response rate of around 30%, based on the total number of residents as it is unknown how many students were eventually targeted by the word of mouth type distribution of the questionnaires. Of these 52 respondents, 17 were self-identified as first-years (typically 19 years old), 15 as second years (20 years old), 13 as third years (21 years old), and 7 as being fourth-year and above (22 years old and over). The respondents represented students studying in seven different academic faculties.

The relatively low response rate and the possible influence of phenomena such as selection bias notwithstanding, the distribution between four year-groups and seven faculties were considered to be representative enough to allow for the useful application of information security behavioural threshold analysis [5].

The second experiment was conducted in an industry setting (first reported in [14]). The experiment was specifically chosen for comparison due to the difference in the sets of contextual influences in mind when compared to that of [10].

The experiment was performed with working adults within a utility company. A behavioural threshold analysis questionnaire was distributed within a risk assurance department. Supervisors were asked to distribute the questionnaire which was completed by 63 employees. Once again, the nature of the online, self-reporting approach does not provide an indication of the number of respondents who were targeted but based on the number of employees in the department, a notional response rate of 50% is plausible. Three categories of the type of employment were identified as management (14%), contractors (53%), and permanent staff (33%).Given the compulsory nature of the information security assessment in the second experiment, a 100% response rate was achieved. This is in contrast to the 28% response rate reported on in [10] which can be ascribed to the voluntary nature of completing the questionnaire for the first experiment. The response rate was dependent on students dedicating time and effort into completing the survey. They were not compensated for their participation and therefore seemed reluctant to do so if there was no direct gain to be had.

The questionnaires which were distributed to both groups of respondents in experiments one and two, consisted of six questions relating to information security behaviours. To cover a range of common information security themes, selected focus areas of the Human Aspects of Information Security Questionnaire (HAISQ) were employed as the topics for the questions [3]. The six questions related to *information security training*, *password management*, *incident reporting*, *social media use*, *internet use*, and *email use*.

A four-point Likert scale was used for the question responses. The respondents rate their predisposition for participating in the security behaviour, relative to the percentage of other group members that perform the behaviour [5]. This predisposition for participation is used as the behavioural threshold for the respondent. Responses from all the respondents were mathematically aggregated and analysed.

In the next section, a high-level overview of the contextual environments is presented.

3.2 Contextual environment

Given the distinctly different natures of the two environments in which the abovementioned experiments were performed, this section provides a summary of the two contexts in terms of the physical milieu and the social milieu as identified in Table 1. The summary is provided in the form of Table 3, based on the general contextual factors from Table 2.

Table 3. External factors that influence information security behaviour.

External factors in information security behaviour		
Extrinsic factor	***Factors in student information security behaviour***	***Factors in industry information security behaviour***
Physical milieu	**– Ease of access to systems, processes and people** Common areas (lounges, television rooms, kitchens, laundry rooms, public computer rooms, reception), as well as private sleeping quarters which houses one or two students per room. The close proximity of this kind of living arrangement provides the members of the residence with unprecedented access to the behaviour of others. Both in practical terms that allow the observation of the behaviour of others, and physical terms in which access is afforded to personal and university computers and networks.	**– Ease of access to systems, processes and people** In contrast to people that live together, co-workers rarely have unrestricted access to each other's private spaces like workstations, cubicles, or offices. A level of professional distance is expected that limits the observation of the behaviour of others. Access to systems and processes are strictly controlled and enforced to prevent unauthorised access and behaviour.
	– Level of convenience associated with tasks A certain level of convenience is conveyed by living in close quarters. For instance, if network access is required after business hours and a person's credentials have expired, it is easy to simply ask any other inhabitant of the residence to supply their details. It is convenient for the borrower as their ability to access the network is instantly restored without the need to contact the helpdesk which will not respond in real-time.	**– Level of convenience associated with tasks** Within larger organisations, convenience of performing everyday tasks is diminished by the associated red tape and governing policies. In terms of the levels of information security within the organisation, this can be seen as both a hindrance and a help. Tighter control and oversight might help prevent human error but might also lead to security fatigue [15] which can lead to employees trying to find workarounds for frustrating security controls.

	– Availability of technical expertise Given the combination of different academic levels, fields of study, and technical proficiencies that cohabit, it is probable that someone with a high level of know-how or expertise can readily be found to help circumvent security controls that stand in the way of quickly or conveniently completing a task. An example of such a circumvention is accessing dubious websites that are restricted on the university network by means of masking their network traffic by employing virtual private networks to third party providers.	**– Availability of technical expertise** Industries tend to group different functions that logically belong together within departments or sections. With reference to the availability of technical expertise, this might lead to a scenario where expertise is concentrated (e.g. within the IT department) and not readily accessible to many of the members of other groupings. Dedicated persons are appointed to fulfil technical roles and are typically well versed in good security hygiene. Such employees would ideally not assist others in performing unwanted security behaviour and will preferably report any security circumventions.
	– Presence of security controls In the specific university and residence environment, no formal information security training is provided. The only mechanism that is used to raise awareness is notifications when accessing the university network and posters stating relevant rules for the use of university computer labs.	**– Presence of security controls** In the industry setting, formal information security training is provided to the employees which should ensure an enhanced level of awareness and compliance.
Social milieu	**– Organisational structure and peer pressure** A strict hierarchy prevails where a pecking order distinction is made based on the number of years someone has been residing in the specific residence. There is also a specific distinction between junior (usually first-year students or first-time entrants) and senior students. In this hierarchy, juniors have very little autonomy and, especially during an initial orientation, are forced to obey senior residents [17]. The peer pressure and hierarchy that is present in residences are usually seen as factors in hazing [17] and alcohol consumption in literature [15, 16] but is also applicable to security behaviour. A resident may easily be coerced, through this hierarchical structure and peer pressure, into divulging credentials, downloading illicit content, etc.	**– Organisational structure and peer pressure** Organisations, specifically larger organisations, typically have fixed organisational structures with clearly defined levels and roles. In such a hierarchy there is a noticeable unidirectional balance of authority, e.g. a manager has influence over an employee, but the reverse is rarely true. When viewed in terms of information security, this control of the upper echelons over the lower can have either a positive or a negative effect. An authority figure can serve as the embodiment of policy and procedure and can be a strong deterrent for unsafe security behaviour. Contrariwise, such a figure can, for example, strong-arm a subordinate into not reporting security incidents or performing other negative security behaviours.

	– Presence of co-workers, family, or friends and being exposed to the actions/behaviours of others In a residence, there is a constant presence of other people. Even in a private space like sleeping quarters, there might be another resident present. This implies that some actions of an individual, that would normally go unnoticed, are being observed. If they visit a dubious website, someone may be there to observe it. When password sharing occurs between two parties it may be witnessed by any or all of the others present. Therefore, this constant presence may convey an unprecedented sense of awareness of the information security habits of the resident corps. The awareness may set the precedent for future behaviour.	**– Presence of co-workers, family, or friends and being exposed to the actions/behaviours of others** Arguably the most important, distinction between the physical environment in industry and that of the university residence is the amount of time that the members of the two groups spend together. Assuming a typical eight-hour workday, this is the only exposure that the members of the industry group will have to the behaviour (including information security behaviour) of others on a regular day. This is in contrast to the residence where the exposure is constant except for the interruptions of attending classes. This reduced contact time leads to a different dynamic in the *social milieu*.
	– Collective purpose and working with others Even though the abovementioned hierarchy may be seen in a negative light as illustrated above, it may also contribute to a sense of belonging and camaraderie [17]. There is an implied level of trust associated with shared experiences. This is compounded by the compulsory attendance of events [15, 17] that are meant to reaffirm the bond between the residents. This trust allows for a false sense of safety where security is concerned. For instance, one might not appropriately scrutinise an email that was (presumably) sent by a confidant and assume it to be safe. The assumption will leave one open to malware and phishing attacks.	**– Collective purpose and working with others** It stands to reason that the ultimate purpose of an organisation is to be successful and sustainable. The specific measure of what successfulness entails notwithstanding, it should be the clear collective vision of the members of the organisation to contribute to reaching this goal. This vision serves as a moral compass that guides their behaviour and by extension should influence information security behaviour. Especially when confronted with security behaviour is known to be imprudent, the collective purpose of the group should guide the individual to behave in a positive way.

Information security behavioural threshold analysis from [5] was subsequently implemented in the specific contexts as described above in Table 3. In the following section, a cursory reflection is provided on the process of behavioural threshold analysis.

3.3 Behavioural threshold analysis

For a detailed description on behavioural threshold analysis in general terms, the reader is referred to [4] as only a brief overview is presented here, followed by the specific descriptions of the behavioural threshold analysis results in the following section.

To interpret the behavioural thresholds that were reported by the respondents, the thresholds are aggregated by calculating the cumulative frequencies for each threshold interval. In order to simplify the analysis, behavioural thresholds are grouped into intervals of 10%. These frequencies are then graphed as a line of participation level (y) versus cumulative behavioural thresholds (x). Furthermore, Granovetter [4] stipulates that the cumulative frequencies of the respondents' behavioural thresholds should be graphed in relation to a uniform distribution of thresholds. This uniform distribution is referred to as the equilibrium line and is represented by the $y = x$ line. The intersection (if present) of the two lines may indicate that the group behaviour has reached an equilibrium point, i.e. the number of participants in the behaviour has stabilised. Behaviour that has reached equilibrium will not gain any new participants, but neither will any participants desist from their current behaviour

Granovetter [4] states that the requirement for equilibrium is that the two line segments to the left and right of the intersection have gradients $(m = \Delta y/\Delta x)$ of less than one. This implies that an equilibrium state requires the threshold line to intersect the equilibrium line from above. An intersection from below does not constitute an equilibrium state, i.e. the gradient is greater than one. When $m < 1$ to the left of the intersection, the number of participants will not decrease in and of itself. An external influence or stimulus (e.g. information security training or awareness campaigns) is required to reduce the participation rate. In the same manner, to the right of the intersection, the number of participants will not increase.

In the following section, a comparison of the results for experiments one and two (explained in Section 3.1) in the application of behavioural threshold analysis are presented.

4 A comparison of two studies through behavioural threshold analysis

As per its definition, contextual factors in information security behaviour is dependent upon the environment in which such behaviours are to be performed. The influence of such factors may be assessed by means of behavioural threshold analysis. Therefore, in this section, a pairwise comparison of two behavioural threshold analysis experiments are presented.

As mentioned before in Section 2, two main classes for external contextual factors were identified, i.e. physical milieu, and social milieu. For the purposes of the comparison between the two experiments (experiments one and two from Section 3.1), only three information security focus areas are presented here namely, information security training, social media use, and internet use. The cumulative threshold graphs for the remaining three focus areas (password management, incident reporting, and email use) are included in the Appendix for reference. This is due to page restriction considerations and it was reasoned that the similarity in the behavioural threshold analysis results of the graphs in the Appendix, compared to those that already form part of the discussion, are such that including them do not contribute significantly to the arguments presented here.

A concern that often comes with employing measuring instruments (questionnaires) for evaluating behaviour, is social desirability [16], i.e. respondents report on what they suppose the "correct" response is rather than responding candidly This problem can also occur in behavioural threshold analysis experiments and in previous studies it has been provided for in the form of adapted responses [5]. For the purpose of this study, it was decided to use the original data that was not adjusted for social desirability, specifically to show the effect of the original data. Because these are two such divergent examples, using the unaltered data should provide a more accurate picture of the effect of the contextual factors on the behaviour of the two groups.

In Section 3.3, the process of behavioural threshold analysis was described. The principles that were discussed are now applied to evaluate the behaviours that relate to the focus areas from Section 3.1.

Information security training – The behaviour of voluntarily completing information security training is considered a positive behaviour. One would therefore expect that others should ideally copy this behaviour from the example that is set by the group. The cumulative threshold graph for information security training behaviour is presented in Figure 2.

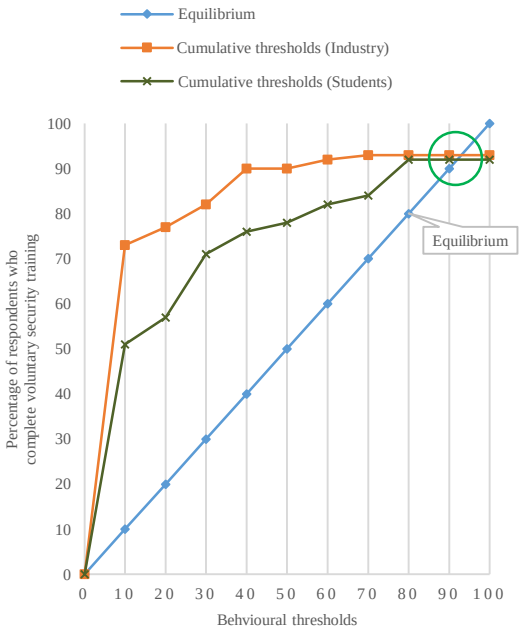


Fig. 2. Behavioural threshold analysis graph – Information security training (Industry vs. Students)

From Figure 2 it can be observed that respondents that work together in an industry setting are more willing to initially follow the behaviour of their peers in attending voluntary information security training than students that live together in a university residence. However, as participation in this behaviour gains traction, the difference in

the eventual predicted participation is very low, i.e. 92% for students, and 93% for industry workers. These percentages are derived from where the two cumulative frequency lines for the industry and student respondents intersect the equilibrium line (highlighted in Figure 2). Both groups exhibit low thresholds for participation which means that they will easily follow the group example. Seeing as security training contributes positively to the levels of information security in the organisations, this behaviour should be encouraged and reinforced.

Social media use – In the context of this research, social media use refers to the use of company or university resources and time to access social media websites. The intersections of the cumulative thresholds for the two groups for this behaviour are once again highlighted in Figure 3.

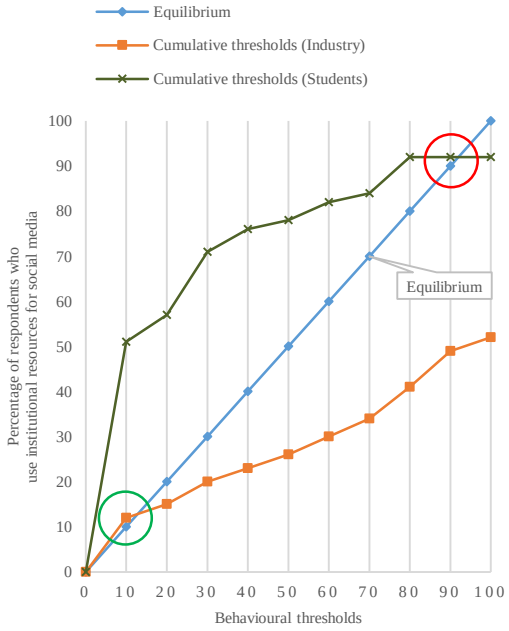


Fig. 3. Behavioural threshold analysis graph – Social media use (Industry vs. Students)

Contrary to the information security training example, the predicted behaviour for the two groups for social media use, shows a stark contrast. An early equilibrium is reached for the industry group. The green highlighted area at the bottom left of the graph (Figure 3) shows that only between 12% and 13% of industry workers will eventually follow the social media behaviour of others. This low level of behavioural compliance indicates that the industry group members retain high threshold values against participation. The behaviour cannot propagate to other group members beyond this point.

Students, on the other hand, will follow the social media behaviour of their cohorts until it reaches a 92% participation rate (red highlighted area, Figure 3) They show low

behavioural thresholds for this behaviour. Furthermore, as many as 51% of the student respondents will start to participate if they think that as little as 10% of their group are already taking part. This pattern foretells a rapid preliminary uptake in the behaviour and thereafter a steady increase until the equilibrium is reached. A participation level of 92% in any improper information security behaviour should be considered problematic. The group behaviour will remain unchanged unless specific action is taken to rectify it. With reference to the human aspect of information security, awareness campaigns are thought to be one of the more effective interventions whereby to ensure good information security practices within an organisation and effect change in behaviour [7]. Such awareness campaigns can be tailored to fit the focus areas that need to be addressed to raise awareness, i.e. social media use in this particular case.

Internet use – This focus area refers to risky behaviour when using the Internet, e.g. visiting dubious websites which exposes one to possible malware attacks and the interception of sensitive information. The cumulative behavioural threshold graph for Internet use behaviour presents an interesting case that differs from the preceding three focus areas. The participation rate of 69% for the student group (see the red highlighted area in Figure 4), indicates that the respondents, are quite willing to follow the example of their fellow residents. However, the aggregated reported thresholds for the industry respondents do not intersect the equilibrium line when plotted.

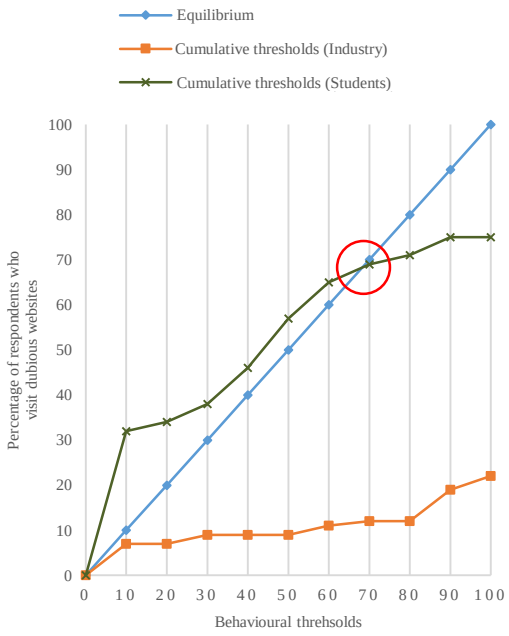


Fig. 4. Behavioural threshold analysis graph – Internet use (Industry vs. Students)

This occurrence is an example of what Growney [17] refers to as a dying problem. In a dying problem scenario, there is not enough initial stimulus to get the underlying individual behaviour to grow into an accepted group behaviour. In the example of internet use behaviour, an instigator (or several instigators) might initially perform the behaviour of visiting dubious websites. They do not require anyone else to exhibit the behaviour and they will perform it out of their own intrinsic motivations. This number of initial actors does not, however, satisfy the chief requirement of the threshold models of collective behaviour, stating that the number of people that perform a certain behaviour must exceed an individual's internal threshold before the individual will join in the behaviour. At all the threshold levels, the plotted cumulative thresholds for the industry respondents remain below the equilibrium line. This contrasts with the threshold graph for the students, which remains above the equilibrium line for the most part. With the current composition of the industry group, there is no individual that will be convinced to join in the behaviour because their own threshold for participation has not been exceeded. Given the nature of the behavioural thresholds model, the dying problem might even cause the process to work in reverse. If an instigator notices that very few others, if any, take part in the behaviour that they themselves perform, they might reconsider their own behaviour and desist from any future action.

The commonalities and differences in their contextual environments and the influence that context has on behaviour is now discussed in Section 5.

5 Discussion

In the previous section, a comparison of the predicted information security behaviour for the two groups, based on behavioural threshold analysis, was presented. It is notable that for each of the information security focus areas, the industry respondents fare better than their opposite number in the academic setting. The results are summarised in Table 4 which shows the mean values for the reported thresholds for the two groups. Note that the training behaviour is a positive behaviour (indicated with *). This is opposed to the other behaviours that negatively impact information security. Therefore, in these instances, the threshold model should be interpreted in reverse, i.e. it can be considered a good thing if positive information security behaviour spreads through a group.

Table 4. Mean reported behavioural thresholds per group

	Security behaviour	**Students** (μ_1)	**Industry** (μ_2)
Mean behavioural threshold (μ)	Information security training*	23.65	21.27
	Social media use	31.15	74.44
	Incident reporting	51.15	70.79
	Email use	51.92	86.51
	Internet use	50.96	90.00
	Password management	68.27	90.95

The mean behavioural thresholds (μ) for all of the listed behaviours are higher (save for * where lower thresholds are considered better) for the industry respondents (μ_2) than for the student respondents (μ_1), i.e. the chances that unwanted security behaviour will propagate within the industry group, based on the principles of threshold models of collective behaviour, are lower than for the student group by a margin as big as 43.29 percentage points for the social media use behaviour.

The two experiments that were described in Section 3.1, were conducted in exactly the same manner, i.e. the same methodology [5] was used in both cases. This means that the data collection methods, information security focus areas, the way the questions were worded, and the question layouts were kept constant in both settings. The main differences between the experiments, were differences in the contexts in which they were performed (issues such as age and gender notwithstanding). Hence, one possible conclusion is that the differences in predicted behaviour for the groups, can be attributed to the considerable influence that the different external contextual factors have on the two groups.

The remainder of this section is dedicated to a discussion of how the two external contextual factors that were identified, i.e. physical milieu and social milieu, may have influenced the way in which the two groups go about information security behaviour for the different focus areas.

Information security training – Formal information security training is not provided in the specific university context for this research, apart from inconsequential notices in the university computer labs and login screens. In industry however, there is a marked tendency to provide training to employees in an attempt to protect the digital and financial assets of the organisation. It stands to reason then, that the motivations of the groups to perform the behaviour differ. Their heightened knowledge of the importance of security training, in comparison to that of the students, influence employees to choose voluntary training. Receiving security training can be seen as part of their physical milieu that provide the availability of and access to expertise. Students, on the other hand, having not received any previous formal security training, may opt to choose voluntary training due to their social milieu. Taking part in activities as a group is a common occurrence in the residence setting and gives a sense of collective purpose.

Social media use – In the two contexts under review, the security implications of the use of social media are quite different in terms of their physical aspects. In an industry context, social media use might expose the organisation to phishing attacks, or accidental dissemination of proprietary information, and the like. The risk for the student is, however of a personal nature, e.g. identity theft, even if the student does use the university infrastructure for their social media interactions. Undergraduate students rarely (if ever) have access to information of a sensitive nature relating to the university itself. Based on the differences in security implications, the motivations for exercising caution with social media behaviour is also different. Students also experience the influence of the social milieu as many of their events and activities use social media platforms for interaction and organisation. This further contributes to their willingness of using social media, even when information security circumstances dictate that it should best not be done.

Internet use – Student behavioural thresholds are low, i.e. it takes little motivation or the perception that only a few others already perform the behaviour for them to also perform the behaviour. On the physical level, this may be attributed to the access that the student respondents have to technologically knowledgeable peers. An example scenario can include that academic institutions often employ firewalls and other network infrastructure to prohibit access to websites and other network protocols they deem to be dubious in terms of security or questionable in terms of the content they provide [18]. Residences provide the ideal environment where these restrictions may be circumvented by a knowledgeable person and the method of access disseminated to others. The social factor determines how dissemination might take place: The required awareness that such circumventions are possible is created through constant presence and observation within the residence. The student that originally exploited the circumvention is then either coerced to help others bypass the existing security (through peer pressure or levels of hierarchy) or might provide other students with the solution willingly because of a sense of solidarity and collective purpose.

Stricter policies and deterrence measures, as an example of the physical milieu, might be the reason why their industry counterparts are less willing to follow bad examples of internet use. Similar to the physical aspect, the social aspect in the workplace can be interpreted as the reason for the high thresholds for the industry respondents. Being aware of the security and disciplinary risks associated with disregarding policies and accessing dubious websites and possibly having to circumvent technical security measures to achieve this, should cause a certain reluctance to follow the example of others. Also, if an individual is performing such actions, it will be done in secret and kept hidden from the observation of his/her co-workers.

The following three focus areas did not form part of the comparison between the predicted information security behaviour of the two groups in Section 4. The resulting behavioural threshold graphs are available in the Appendix. However, a cursory overview of the possible underlying contextual factors is presented here.

Incident reporting – Although incident reporting is often touted as being important in the management of information security, it is rarely being practised. One of the main impeding problems is that without a clearly defined process of reporting, responsibility and accountability guided by policy [19], reporting will not take place as it should without the proper commitment of the members of the organisation. Conceivably, it is often easier to just ignore incidents, due to security fatigue [15], than to navigate the process of reporting them, if such a process exists. The actual and perceived ease associated with reporting an incident, is one of the barriers that translate to how an employee or student will behave when an incident occurs. Convenience and access are considered factors that inform behaviour and therefore these reporting mechanisms can be considered part of the physical milieu of an organisation. Existing hierarchies and mutual experiences (social milieu) can be considered as another stumbling block for reporting security incidents. An individual might be reluctant to be an informant on the security transgressions of others for fear of retribution or for simply being ostracised from the group.

Password management – The sharing and mismanagement of passwords is said to be one of the main security threats that relates to the human aspect of information security [20], and as such it is one of the most common topics in information security awareness programs. Both formally (through such programs) and informally (through media and many websites) people are warned to take the security of their passwords seriously. Often, the social milieu is an external contextual stimulus for password sharing. This is both relevant for the industry and residence settings as one of the main reasons for sharing passwords is to simply "get the job done". As mentioned before, expired or forgotten credentials stand in the way of completing tasks and are therefore circumvented by using another's credentials to avoid the inconvenience of retrieving them.

Email use – The use of email for communication is common in both the academic and industry settings. Phishing attacks, social engineering, and the distribution of malware are prevalent in the email ecosystem [21]. Email servers and their technical configuration, including spam filtering functionality, and antimalware and antivirus capabilities all comprise the physical milieu in relation to email use behaviour. Reliance on the protection afforded by these functionalities may lead to complacency and an unwarranted sense of security. However, if these technical measures fail, the success of these attacks draws on the interactions between people on a social level. The social milieu will therefore influence the related behaviours. In the context of the university students, the reasons for unwanted behaviour in terms of email security can once again be linked to the common practice of digital piracy that is rife in university settings [22, 23]. Many different file formats are used to encode, compress, or hide illicit content. Email attachments may therefore not be scrutinised thoroughly if a file with a strange or unknown file extension is accompanied by a convincing message. The implied sense of trust and camaraderie that forms part of the social milieu further exacerbates the problem by strengthening the associated credibility of an email and its attachments if the source appears to be from within one's social milieu. Similarly, in industry the social milieu may influence even well-trained employees with the necessary awareness to lower their guard with respect to email security.

In the final section, the study is summarised. The aims of the study are revisited, and a reflection is provided on the contributions and limitations of this research. A look ahead to possible future work concludes the article.

6 Conclusion

This paper presented an extension of previously published work [10] in which external contextual factors and their possible influence on information security behaviour were studied.

The aims of this research were to firstly provide a theoretical discourse about the applicability of external contextual factors to information security behaviour and then to apply a model to evaluate information security group behaviour. Secondly, this model should be able to observe the influence of contextual factors on the way in which a group behaves. Finally, the evaluations of the security behaviour of two different

groups through the identified model, including the underlying contextual factors, were to be compared. The contributions to the field of information security behaviour, by virtue of addressing these three aims, are shortly discussed here.

Aim 1 – A literature review on how context influences human behaviour in general revealed five distinct factors that play a role in how humans behave. Two distinct classifications of contextual factors were identified and conceptualised in terms of the theory of planned behaviour (TPB). TPB was consequently used as the theoretical foundation for connecting the extrinsic contextual factors to information security behaviour. Even though TPB is often used in information security behaviour studies, TPB on its own only considers individual cognition and does not provide insights into behaviour in groups. This limitation was addressed in the second aim.

Aim 2 – Behavioural threshold analysis was recognised as a suitable approach to evaluate information security group behaviour and is conceptually compatible with TPB. Furthermore, this approach implicitly takes the influences of external contextual factors on information security group behaviour into account.

Aim 3 – Two group behaviour experiments were conducted in which behavioural threshold analysis was applied and the different behaviours of the two experiment groups were compared. The information security group behaviour was found to be consistently better for the industry stetting in comparison to that of the university residence setting. The behavioural threshold analysis comparison for the two groups was further augmented by a discussion that highlighted the differences in the external contextual factors that ultimately affected the information security behaviours of these two groups. This discussion demonstrates the importance of taking into account the contextual environment when seeking to address information security behaviour in an organisation.

Lastly, this paper only reflects on the influence of the extrinsic contextual factors on information security behaviour. This is due to the intrinsic factors already being implicitly addressed in other security studies that are based solely on TPB. However, future studies may seek to investigate the applicability of these factors to group behaviour, especially how these contextual factors influence the individual's thresholds and related susceptibility to follow the behaviour of others.

Acknowledgements

The authors would like to thank Johann Allers and Wayne Kearney for their assistance with the experiments.

References

1. Shropshire, J., Warkentin, M., Sharma, S.: Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security 49, 177-191 (2015)
2. Barth, S., De Jong, M.D., Junger, M., Hartel, P.H., Roppelt, J.C.: Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telematics and Informatics 41, 55-69 (2019)
3. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security 66, 40-51 (2017)
4. Granovetter, M.: Threshold models of collective behavior. American Journal of Sociology 83, 1420-1443 (1978)
5. Snyman, D.P., Kruger, H.A.: Behavioural threshold analysis: Methodological and practical considerations for applications in information security. Behaviour & Information Technology 38, 1-19 (2019)
6. Willison, R., Warkentin, M.: Beyond deterrence: An expanded view of employee computer abuse. MIS quarterly 37, 1-20 (2013)
7. Johnston, A.C., Di Gangi, P.M., Howard, J., Worrell, J.: It takes a village: Understanding the collective security efficacy of employee groups. Journal of the Association for Information Systems 20, 186-212 (2019)
8. Wu, P.F., Vitak, J., Zimmer, M.T.: A contextual approach to information privacy research. Journal of the Association for Information Science and Technology 7, 485-490 (2019)
9. Kroenung, J., Eckhardt, A.: The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship. Information & Management 52, 611-627 (2015)
10. Snyman, D.P., Kruger, H.A.: External contextual factors in information security behaviour. In: 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), pp. 185-194. SCITEPRESS – Science and Technology Publications, Lda. (2020)
11. Belk, R.W.: Situational variables and consumer behavior. Journal of Consumer research 2, 157-164 (1975)
12. Kirova, V., Thanh, T.V.: Smartphone use during the leisure theme park visit experience: The role of contextual factors. Information & Management 56, 742-753 (2019)
13. Snyman, D.P., Kruger, H.A.: The application of behavioural thresholds to analyse collective behaviour in information security. Information & Computer Security 25, 152-164 (2017)
14. Snyman, D.P., Kruger, H.A., Kearney, W.D.: I shall, we shall, and all others will: Paradoxical information security behaviour. Information & Computer Security 26, 290-305 (2018)
15. Furnell, S., Thomson, K.-L.: Recognising and addressing 'security fatigue'. Computer Fraud & Security 2009, 7-11 (2009)
16. Fisher, R.J.: Social desirability bias and the validity of indirect questioning. Journal of Consumer Research 20, 303-315 (1993)
17. Growney, J.S.: I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior. COMAP Inc., Bedford, MA (1983)
18. Miller, C., Stuart Wells, F.: Balancing security and privacy in the digital workplace. Journal of Change Management 7, 315-328 (2007)
19. Wiant, T.L.: Information security policy's impact on reporting security incidents. Computers & Security 24, 448-459 (2005)
20. Furnell, S., Esmael, R.: Evaluating the effect of guidance and feedback upon password compliance. Computer Fraud & Security 2017, 5-10 (2017)

21. IBM Security: IBM X-Force Threat Intelligence Index 2018: Notable security events of 2017, and a look ahead. IBM Corporation, USA (2018)
22. Lee, B., Fenoff, R., Paek, S.Y.: Correlates of participation in e-book piracy on campus. The Journal of Academic Librarianship 45, 299-304 (2019)
23. Gan, L.L., Koh, H.C.: An empirical study of software piracy among tertiary institutions in Singapore. Information & Management 43, 640-649 (2006)

Appendix

As mentioned in Section 4, this Appendix shows the cumulative behavioural threshold graphs for the information security focus areas for *Email use*, *Password management* and *Incident reporting* in Figures 5, 6, and 7 respectively. The external contextual factors that contribute to the predicted eventual group behaviours for these three focus areas were discussed in Section 5.

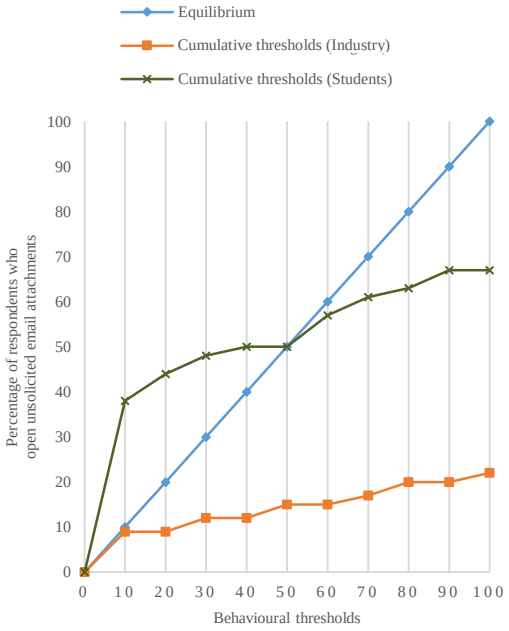


Fig. 5. Behavioural threshold analysis graph – Email use (Industry vs. Students)

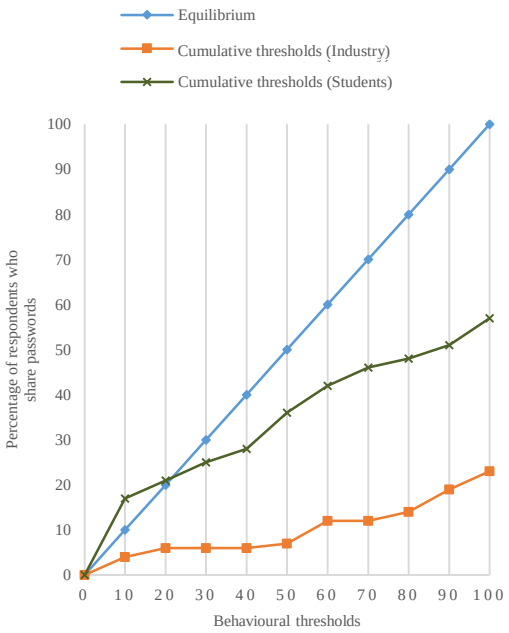


Fig. 6. Behavioural threshold analysis graph – Password management (Industry vs. Students)

24

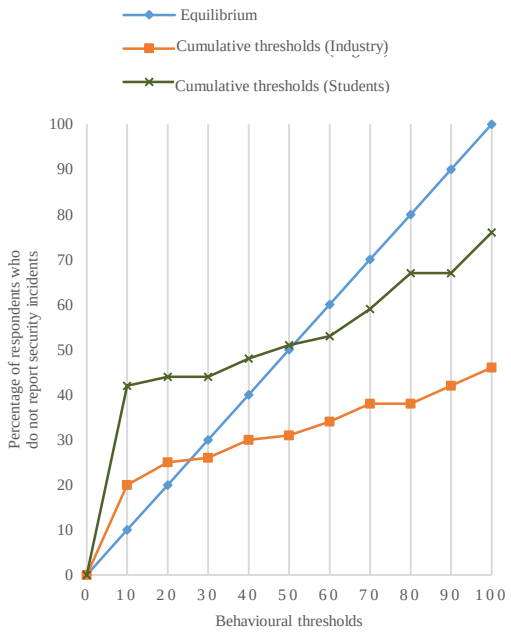
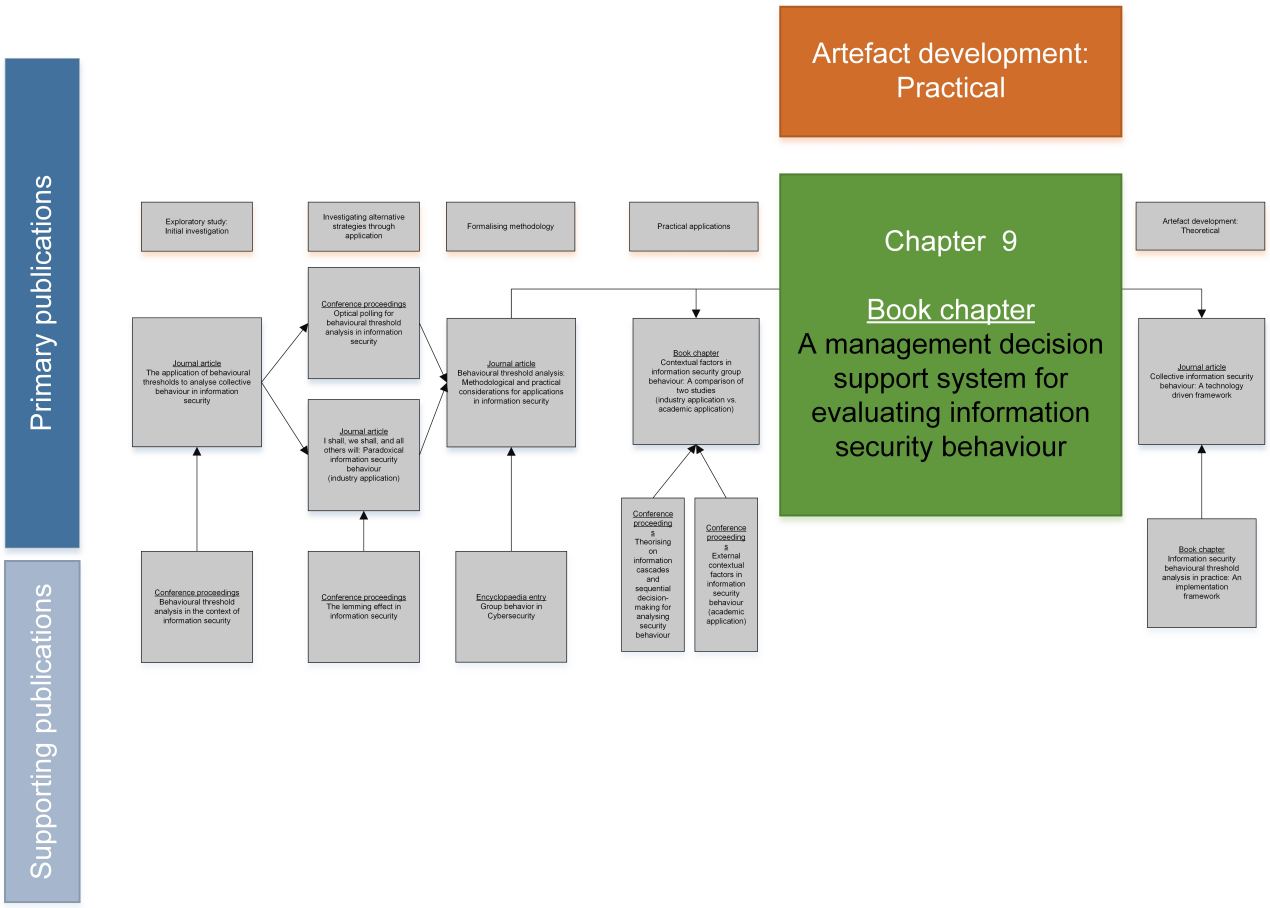


Fig. 7. Behavioural threshold analysis graph – Incident reporting (Industry vs. Students)

Chapter 9
-
Article VII: A management decision support system for evaluating information security behaviour



Chapter table of contents

9.1 Preamble to Article VII 166

9.2 Springer book chapter style requirements 167

9.3 Article VII 167

9.3.1 Introduction 168

9.3.2 Background 170

9.3.3 Description of the system 172

9.3.4 Critical reflection 177

9.3.5 Conclusion and future work 179

9.3.6 References 179

9.1 Preamble to Article VII

In this chapter, the development of a practical software artefact is described as part of the research phase *Artefact development: Practical*.

Often, the burden of information security management in an organisation falls to a manager or managers that have not received any domain-specific training. This lack of education leaves managers unprepared for the information security challenges they might face and they do not have the confidence to make informed decisions on how to best protect the organisation. Existing research makes mention of decision support systems to assist management in selecting technical controls to protect their organisation from technological cyber-attacks. However, literature that describes a decision support system that can help managers make informed decisions about the human aspects of their information security strategies could not be found. This research therefore contributes a practical artefact by creating the first decision support system of its kind that can provide assistance in assessing information security group behaviour. The methodology and strategy for information security behavioural threshold analysis that were created in Chapter 6, Article IV, are embodied as a software decision support system and is presented here in Article VII. This system automates much of the process of performing behavioural threshold analysis exercises in an organisational setting. After initial expert involvement, the DSS empowers otherwise lay managers to perform assessments of the levels of information security group behaviour of their workforce and to identify problem areas.

The article that describes the decision support system was presented at the *18th International Information Security South Africa Conference* on 15 August 2019, and was published as a peer-reviewed book chapter in the Springer book series *Communications in Computer and Information Science* in 2020. The chapter is entitled *A management decision support system for evaluating information security behaviour*[13]. As part of the review process, a scoring system was implemented to rank all the contributions. As a top scoring contribution, this paper was placed in the “best paper” category as a finalist. After further evaluation of the presentation at the conference by the conference chair and members of the programme committee, the article that is presented in this chapter was identified as the best written and oral contribution to the conference and was bestowed the “best paper award” for its exceptional academic quality.

[13] Snyman, D. P., & Kruger, H. A. 2020. A management decision support system for evaluating information security behaviour. In Venter, H, Loock, M., Coetzee, M., Eloff, M., & Eloff, J. Eds., *Information and Cyber Security - 18th International Conference, ISSA 2019, Johannesburg, South Africa, August 15, 2019*, Proceedings (1st ed.): Springer International Publishing, pp. 15-27.

9.2 Springer book chapter style requirements

The Springer book chapter style requirements determined the use of the *Lecture Notes in Computer Science* reference style. The article is presented in its final edited and typeset form as it was published in the Springer book series. Information regarding the author guidelines of the publication can be found in Appendix J.

9.3 Article VII

Article follows on next page.

A Management Decision Support System for Evaluating Information Security Behaviour

Dirk Snyman(✉) and Hennie Kruger

School of Computer Science and Information Systems, North-West University, 11 Hoffman Street, Potchefstroom 2531, South Africa
{dirk.snyman,hennie.kruger}@nwu.ac.za

Abstract. Information security management is a difficult task in organisations. Owing to skills shortages and the like, there are relatively few managerial staff that possess the required expertise to confidently make security decisions. The purpose of this paper is to present a decision support system that can analyse, and provide insight into, information security behaviour in an organisation, all the while supporting management decision-making for organisational factors. Behavioural threshold analysis is employed by the system to predict eventual information security behaviour for different groupings in an organisation. The decision support system that is presented here, which is the first of its kind, can be helpful in understanding the current state of organisational information security behaviour, and what can be done to improve upon the current state. After intervention measures the system may be used to test whether these measures had the intended positive effect. The system is discussed in terms of the different information areas that are used to allow insight into the security behaviours. A critical reflection provides an analysis of the contributions and limitations of the system.

Keywords: Information security · Decision support system · Behavioural threshold analysis

1 Introduction

The management of information security challenges within organisations have become of paramount importance in the contemporary landscape of reliance on information systems [1]. Traditional organisational structures often fail to address the potential impact that information security breaches might have. Organisations fail to employ preventative measures before an incident occurs, and after an incident has occurred they fail to correctly manage the aftermath.

Information security has three aspects that need to be considered in order to successfully provide for these abovementioned eventualities [2]. These are *technical aspects*, *organisational aspects*, and *behavioural aspects*. The management of these aspects needs to be well balanced and receive equal attention if an organisation is to attempt to ensure the information security of their stakeholders.

Technical aspects include the myriad of technological protection measures that are put in place to protect an organisation, such as anti-virus software, firewalls,

© Springer Nature Switzerland AG 2020
H. Venter et al. (Eds.): ISSA 2019, CCIS 1166, pp. 15–27, 2020.
https://doi.org/10.1007/978-3-030-43276-8_2

encryption, authentication systems, etc. This aspect is difficult to manage due to its inherent complexity in the implementation thereof, as well as the scalability of such implementations as an organisation grows and its needs changes [3]. However, even with the level of complexity, technical aspects remain the more straightforward to manage of the three, due to the availability of best practises (as set out in standards, e.g. ISO/IEC/SANS27002), and the successes of strategies that are used by other organisations. Shao, Siponen and Pahnila [4] presents information on how security decision-makers base their decisions on the example set by others.

The remaining two aspects, i.e. *organisational*, and *behavioural*, prove more challenging to manage. This is due to their relative unstructured nature in comparison to the technical aspects. *Organisational aspects* of information security typically refer to the influence that the organisational structure (usually including organisation size, physical location(s), management structures) of an organisation has on information security management. More specifically the organisational aspects in this context also refer to management decision-making under uncertainty with regards to information security policy and practise. Information security has been recognised as difficult to quantify when compared to traditional business and organisational analyses of risk versus reward trade-offs [3, 4]. This means that quantitative analysis, that is used by management to inform decisions, does not perform well as it does not incorporate the intangible aspects of information security. To further complicate matters, when management have (eventually) made decisions on how information security is to be promoted within the organisation, *behavioural aspects* come in to play. This relates to the attitudes and behaviours of the members of the organisation when working with information systems and how they go about security topics like password management and incident reporting. Policies and best practices are often not clearly communicated and therefore not followed by the members of the organisation. They are sometimes ignored or circumvented in favour of individual preference or to reduce so called red tape [5]. In the context of information security, behavioural aspects are often referred to as human aspects.

While the above-mentioned standards do provide some direction for the management of organisational and behavioural factors, the guidance that they provide are still mostly of a technical nature and do not prescribe specifics due to the unique requirements of each organisation. This leaves management, and by extension the organisation itself, at the mercy of an almost trial and error approach to information security management of the human aspect.

In an attempt to address the abovementioned shortcomings for managing both organisational and behavioural factors in information security, this paper reports on the development of a management decision support system (i.e. software program). The aim of the system is to provide managers with insight into the behavioural aspects of information security in their organisations, as well as provide concrete solutions on how these aspects may be addressed.

The decision support is based on a behavioural threshold analysis approach to measure the attitude of members of an organisation and, based on the analysis of these attitudes, can predict eventual behaviour of the group in terms of information security challenges. This will then allow a manager to make informed decisions on remedial

actions that guide the information security behaviour of members of an organisation, e.g. through security awareness programs.

The remainder of this paper is structured as follows: Sect. 2 highlights related literature pertaining to the information security challenges that are faced by management, as well as literature on the information security behaviour model that is applied in the system. In Sect. 3, the software is described in terms of its features and insights it provides, and in Sect. 4, a critical reflection on the novelty and utility of such a computerised implementation is presented. Finally, conclusions and possibilities for future work is discussed in Sect. 5.

2 Background

As stated in Sect. 1, the management of information security in organisations faces many challenges. In order to formalise some of the challenges that are relevant to this research, i.e. organisational decisions (relating to) and behavioural factors, a twofold discussion is presented in this section, namely management issues and behavioural issues.

2.1 Management Issues in Information Security

A cursory look at information security literature confirms that the problems that are faced by such decision-makers are not a new occurrence and the same kinds of problems are universal across different types organisations. The (re)occurrence of some common themes in literature indicate that managing information security remains a troubled area. Some of these common themes include the following:

Top management buy-in [2, 6] – The support from the higher echelons of management often has a make-or-break influence on the information security of an organisation. Top management sets the tone for the company's outlook on security. They approve funding, support initiatives, and contribute to the overall security culture (see Sect. 2.2) in the organisation.

Managing human factors [1, 4, 7] – The human factor (and the effective management thereof) remains one of the key components in any organisation's information security strategy and include topics such as information security behaviour.

Budget constraints – Limited funding constrains decision-makers in the security controls that they can put in place [8]. Limited controls mean that some of the avenues of attack remain unprotected. Decision-making under this level of uncertainty is an assuredly difficult task.

Management confidence and skill - When confronted with decisions in terms of information security management, many organisational decision-makers are not confident in their ability to manage the possible threats and countermeasures appropriately [5]. This may be due to the sheer number of possible avenues that attackers can use to exploit systems and leave organisations and their data vulnerable. Well-trained and experienced information security analysts and managers are currently difficult to recruit. This skills shortage is a global phenomenon [9] which is still the case today.

These are only some of the management issues seen in literature, but the pervasiveness thereof highlights its importance and the relative ineptitude of organisations to effectively provide for it.

2.2 Behavioural Issues in Information Security

This sub-section highlights security behaviour in general as well as a model to quantify behaviour in this context.

2.2.1 Information Security Behaviour

Behaviour, in the context of information security, usually denotes the actions that the members of an organisation take when confronted with computerised systems and the interaction with security safeguards [10]. These actions (which are mostly negative actions) can be either deliberate, or unintentional in nature, but both types of actions have the potential to put an organisation at risk. As herding behaviour suggests [4], individuals do not commonly form attitudes (and the resulting behaviours) on their own in isolation. Being exposed to the behaviour of others, influences the way in which one behaves. This interaction of individuals within an organisation informs an information security culture which is the collective outlook (guided by norms, attitudes and behaviours) of the members of the organisation. The nature of how behaviour propagates between individuals allows negative behaviour to permeate the culture. In order to prevent this occurrence, the security culture of an organisation may be directed by implementing security awareness programs.

Security awareness programs have the main goal of influencing the attitudes of organisation members in such a manner that their behaviour is ultimately positively influenced [11]. Such programs usually focus on practical advice and guidelines to emphasise positive behaviour in specific security scenarios, often called security focus areas, e.g. incident reporting, working with e-mail attachments, etc. Selecting appropriate focus areas for inclusion in an awareness program helps to keep the associated costs low and prevents security fatigue due to overexposure to known focus areas [12, 13].

2.2.2 Model for Measuring Information Security Behaviour

In order to understand group dynamics in behaviour, Granovetter [14] suggests a threshold model to quantify and predict the eventual behaviour of people in groups. This model was first applied to information security behaviour by Snyman and Kruger [15]. In this sub-section, the model is only briefly described in concept.

For a detailed report on the underlying sociological and mathematical mechanisms, refer to the work of Granovetter [14] and Growney [16]. The behavioural threshold model is applicable to situations where actors (individuals) have a choice of participating in two diverging alternatives of behaviour, i.e. the decision to conform to the behaviour of the group, or not. The principle states that, given a group situation, the decision of whether to conform to the group is no longer only determined by the individual, but also by the example that is set by the other members in group. Each person has an innate threshold for when group example will override their own decision-making faculties. This threshold is expressed as the proportion of other people in a group that will have to exhibit a certain behaviour before the current actor will

participate in the behaviour. The concept can be simplified by saying, *if the number of group members that do something is big enough, an individual will be inclined to also join in the behaviour*.

Thus, when a group is actively engaging in a certain behaviour, the number of participating people in the behaviour should theoretically increase, given the group members' thresholds for participation. The instigators (i.e. the first group members to perform an action) have a very low to non-existent threshold and will therefore exhibit behaviour without the example of others. Their participation will encourage the following wave of participants with slightly higher thresholds. This pattern continues until there are no more individuals whose thresholds for participation are being satisfied by the current number of actors and the increase in participation stops. The increase may also continue until all group members participate in the behaviour.

The model states that each individual has a measurable threshold that can be explicitly stated. The eventual level of participation, i.e. how many participants will eventually join in the behaviour, becomes a function of the cumulative aggregation of all the members in the group's thresholds. When graphed, an equilibrium (or point where the number of participating actors stabilises) is reached when the cumulative frequencies for the members' thresholds, equals a uniform distribution of frequencies.

When applied to information security, this model can be implemented to determine the number of people in an organisation that will exhibit insecure behaviour, given specific information security focus areas. An example in this context can be expressed as, *how many group members will have to open unsolicited email attachments, before an actor will also open unsolicited email attachments*? By analysing the underlying thresholds for all the organisation members, a glimpse into the current state of information security of the organisation may be obtained. Based on the observation, the organisation can make informed changes to their information security landscape.

The following section describes how this behavioural threshold model was implemented in a decision support system and how the analysis can inform management decision-making.

3 Description of the System

The system in question is a web-based implementation of a behavioural threshold model as presented by Granovetter [14] and threshold analysis as presented by Growney [16]. The platforms and environments that the system is based on include: Laravel PHP framework, JavaScript in Node.js (with NPM) and Vue.js, including HTML and CSS. Support for multiple devices and operating systems is provided through their native browsers.

The following steps (A) are completed before the system is put to use by management:

A1. Based on an evaluation of the unique requirements of an organisation by management, relevant information security focus areas are identified. Applicable questions about information security behaviour, relating to the focus areas, are then compiled; and

A2. An information security behavioural threshold analysis measurement instrument (online questionnaire) is constructed. The instrument is ensured to adhere to the methodological and practical considerations as prescribed by Snyman and Kruger [10].

After the initial evaluation, the management of the organisation (hereafter referred to as the user) then proceed with the following step (B):

B1. The questionnaire is distributed to members of the organisation through an online platform like Google Forms and anonymous responses are uploaded to the online system;

The system completes the next set of steps (C):

C1. The responses are automatically pre-processed into the correct format and care is taken to ensure the integrity of the data;
C2. The system extracts the information security focus areas which were determined for the organisation, as well as organisational groupings (i.e. departments or job level) that were reported by the individual respondents;
C3. From the responses and the extracted information, the system performs behavioural threshold calculations and completes the threshold analysis. A dashboard is then displayed from which the user can gain insight into the current state of information security behaviour for the organisation and departments under review.

The advantage of this step is that users do not have to understand the aforementioned analysis themselves and perform the required calculations. It is therein that the novelty and value of the system lies. The application of the behavioural model, that will help in supporting management decisions, is automated and the results are simplified and displayed on an interactive dashboard (C4), even a layperson is able to gain insight into the information security challenges and how members of an organisation behave.

C4. The system dashboard, that displays the results from C.3., is divided into three main areas, i.e. a *security heatmap*, an *analysis and reporting area*, and a *what–if analysis area*. These three areas are discussed individually below in terms of their functionality:

Heatmap – The heatmap (pictured in Fig. 1) is the main point of departure for the system. It entails a matrix that shows the information security focus areas, relative to each organisational grouping. The number at each matrix intersection describes the percentage of participants that will eventually participate in unwanted behaviour for the specific information security focus area.

The different levels of participation are color-coded to provide another dimension to the representation that assists the user in detecting problem-areas. A total row shows a summary of the organisation as a whole, and the average levels of participation in unwanted behaviour for the different organisational groupings are indicated by an average column to the right of the matrix.

For an illustrative example, the heatmap in Fig. 1 displays information security behaviour in five information security focus areas for 52 university students of different academic levels (analogous to the organisational departments), that live together in a

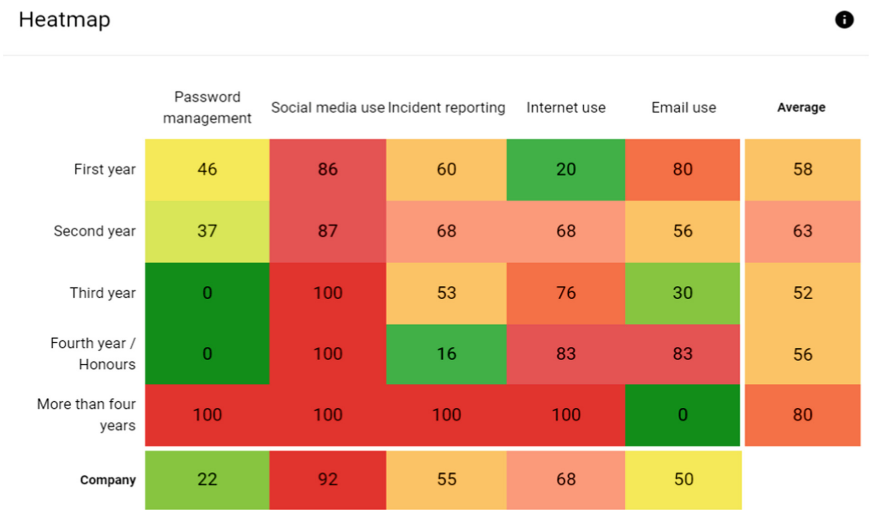


Fig. 1. Dashboard area: heatmap (Color figure online)

single university residence (as the organisational environment). This is based on preliminary real-world data from another, ongoing research project on the security behaviour of individuals living together in close quarters and is used here in order to illustrate the working of the system.

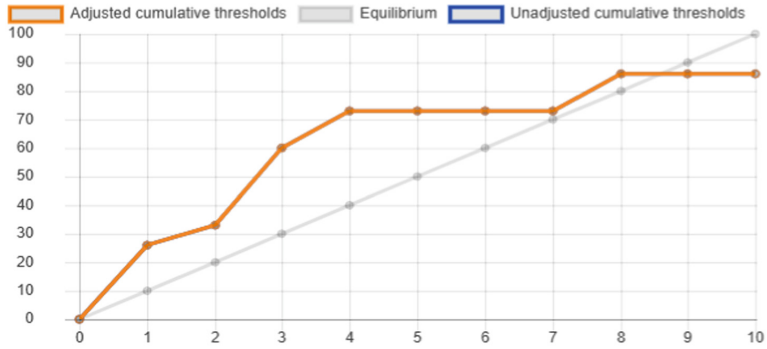
In reference to the row/column intersection of "First years" and "Social media use" that is highlighted in Fig. 1, the high level of participation (denoted by the number 86, i.e. the percentage of members of the organisational group that will exhibit the behaviour), accompanied by the reddish shading of the cell indicate a problematic focus area/department combination. This indicates an immediate risk-area which management of the organisation should pay specific attention to by implementing an intervention of sorts. In contrast, the low participation score and green colour for "Fourth years/Honours" and "Incident reporting" indicate that the outlook for the combination is currently favourable and may be regarded as low-risk at this point in time with no immediate intervention required.

Each row/column intersection on the matrix, as well as the total row, is clickable to allow the user to drill down into the specific behaviour for the specific grouping to see more detailed information in the *Analysis and Reporting area*.

Analysis and Reporting – Firstly, after selecting a focus area and grouping from the heatmap, the reporting area shows a cumulative frequency graph for the behavioural thresholds which were reported by the respondents. This view provides insight into the manner in which the behavioural threshold analysis model was used to determine the level of participation for the specific information security behaviour and is depicted in Fig. 2. The graph, and more specifically the intersection of the graph with the equilibrium

Analysis and Reporting

Social media use for First year



Heatmap report

Overview

The current outlook for the participation in unsafe information security behaviour for **first year** members, with regards to **social media use** is **high**. The percentage of first year members that will act in a contraindicated manner, is currently **86%**. This requires **immediate attention** as unwanted social media use behaviour may put your organisation at risk.

The following common threats, among others, exist for social media use:
-- Exposure to online malware;
-- Exposure to social engineering attacks like phishing, identity theft;
-- Spamming due to publicly available email addresses; and
-- Improper disclosure of information which may lead to financial or reputational losses.

Suggestions

Employ **security awareness programs** that address the abovementioned threats. During training, it should be emphasised that:
-- Do not click on unknown links. They may lead to malware infections;
-- Keep sensitive information private. Do not disclose passwords or other details to any other person, in person or online;
-- Always restrict access to online profiles to only allow known persons;
-- Review organisational policies and guidelines relating to social media;
-- Do not post updates about operational or other sensitive organisational information; and
-- Review privacy policies of social media providers.

Fig. 2. Dashboard area: analysis and reporting

line, is used to determine the level of participation, based on the interpretation in Growney [16] and Granovetter [14]. For example, the intersection of the two lines on the graph in Fig. 2, indicate that the percentage of group members (Third years) that will participate in unwanted security behaviour, relating to the focus area (Incident reporting), will (based on the underlying model) rise until 53% of the group are participating in the unwanted behaviour. The model reaches an equilibrium and group participation should not grow and exceed this percentage but will also not decline on its own without an intervention.

Secondly, a textual report (seen in the bottom part of Fig. 2) is provided that highlights and explains the specifics of the behavioural threshold graph. The report helps the user interpret the meaning that the graph conveys by classifying and explicitly stating the magnitude of the possible security threats (classified as high-, medium-, or low-level threats) that the current level of participation in the information security behaviour might entail. The report also provides suggestions on interventions that may be made to improve upon the current state of information security behaviour.

The report shown in Fig. 2 is based on social media threats described in Hekkala, Väyrynen and Wiander [17], and Gardner and Thomas [18]. The functionality to download the report is also available which allows the user to distribute the Analysis and Reporting screen (Fig. 2) to other stakeholders without them requiring access to the system.

Generic reports and recommendations are provided beforehand when deciding on the information security focus areas that are relevant for the organisation (see A.1. above). Reports and recommendations that relate to high, medium, and low risk level evaluations of the security behaviour, are provided for each of the focus areas and are dynamically compiled, based on the results for the specific grouping. The resulting report that the system provides, is also dynamically updated with the relevant measurements, threat levels, and other information as the specific evaluation dictates.

What-if analysis – The final area on the dashboard is the what-if analysis area and is shown in Fig. 3. This area can be used by the user to see estimates on how changes in the information security behaviour of the members of the organisation will influence the overall outlook for the organisation. The effect of changing the participation levels will be highlighted by colour changes in all the affected areas. This allows the user to instantly see how a positive (e.g. a security awareness campaign) or negative (e.g. deteriorating information security behaviour) change will influence the organisation's levels of security and will help identify areas that require the most attention, e.g. by inclusion in security awareness programs.

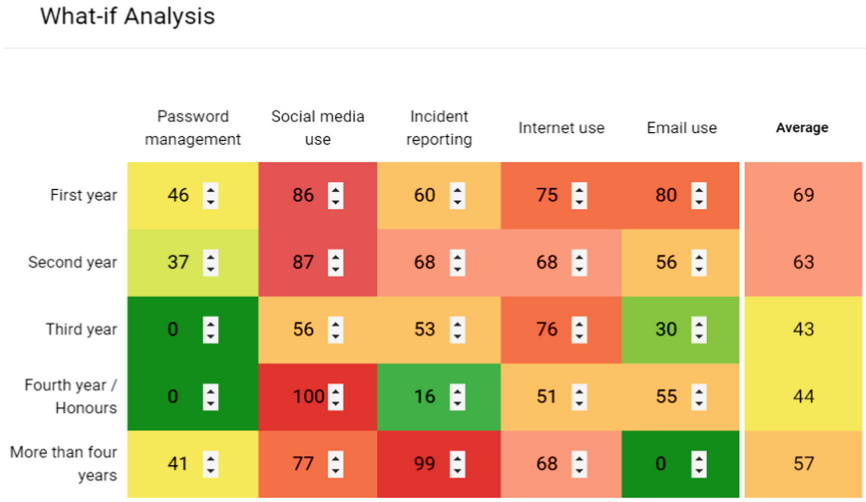


Fig. 3. Dashboard area: What-if analysis

4 Critical Reflection

In this section, a critical reflection of the system is presented in a twofold manner: (1) a reflection is provided on the contributions of the system and, by extension, the contributions of this paper; and (2) the limitations of the system are reflected upon.

4.1 Contributions of the System

Apart from a few earlier endeavours to quantify and analyse information security investment and technical controls using mathematical models [5, 8] as well as software artefacts to analyse the technical security of a specific system [7], the development of this system that takes into account human behaviour in information security by means of threshold analysis is, to the best of the authors' knowledge, the first of its kind. This kind of analysis of information security behaviour, by means of behavioural threshold analysis is a novel approach to decision support for management in an organisation.

Management (especially those with less comprehension of information security issues) may use the system to *gain insights into the security* proclivities of the members in their organisation. Once management is aware of the specific issues that may leave their organisation vulnerable, they are *empowered to address the shortcomings* and thus provide better levels of information security than the current status quo. The built-in reporting functions may help to provide concrete courses of action for management to investigate in order to address these issues.

Using the analysis that the system facilitates may provide insights into information security behaviour trends in the organisation. When a certain behaviour is identified that compromises the organisation's security, these behaviour trends may be addressed

through the inclusion of *relevant topics in security awareness programs*. Similarly, when the analysis indicates that certain security behaviours are within acceptable limits, these behaviours might be left out from awareness programs as to *prevent security fatigue*. Security fatigue refers to the phenomenon where individuals forego good security practices because they are considered burdensome or the individual becomes desensitised to the possible dangers of their behaviour due to over-exposure to it through constant reminders thereof [12, 13].

By conducting behavioural threshold analysis exercises with the members of the organisation and including different information security focus areas in the exercise, the software may help *identify new risks* that were previously unknown or not overtly identifiable through traditional means of investigation.

Finally, the system may help in evaluating the success of intervention measures, e.g. in a situation where bad security behaviour was identified. After attempts to intervene and correct the behaviour have been implemented (i.e. through awareness programs or campaigns), a follow-up analysis of the organisation's security behaviour should indicate whether the interventions were successful or not. This would further help management to strategize and enhance their approaches to security behaviour improvement.

4.2 Limitations of the System

In its current form, the implementation does exhibit some limitations. While the system empowers management to make informed decisions about security behaviour, a certain level of expertise and evaluation of an organisation is still initially required to identify information security focus areas and construct the relevant measurement instrument. However, after this has been completed, the exercises may be repeated as many times as required without any further reliance on expertise.

The aforementioned system-based analysis of security behaviour is only as accurate as the data that the analysis is based on. Seeing as the behavioural threshold analysis is performed on data that are reported by humans, there is room for error. Occurrences of the social acceptability bias, also called social desirability, might influence the members of the organisation to misrepresent their security behaviour [19]. Basing the aggregation of behavioural thresholds on flawed data, may provide insights that are incorrect. The system, in combination with the measurement instrument (see Sect. 3), attempts to correct for such occurrences by adapting a member's behavioural thresholds if they are deemed untruthful in the reporting of their behaviour. The adapted aggregation, when present, is indicate by a blue line on the reporting graph in the *Analysis and Reporting* area (Fig. 3).

Finally, the system provides management with insight only into the behavioural aspects of information security. It makes no provision for the analysis of technical aspects of information security protection. This shortcoming may be addressed by combining the recommendations of this system with analyses similar to those suggested by other studies [5, 8, 20] to gain a more well-rounded insight into all the organisation's security aspects.

5 Conclusion and Future Work

This paper described the instantiation of information security behavioural threshold analysis in a web-based decision support system. The system allows for the evaluation of information security behaviour in an organisation. An in-depth knowledge of threshold analysis is not required by anyone who uses the system as the analysis is automatically performed by the system and insight is provided through representing the results on an online dashboard. Supplementary to the dashboard, textual reports provide suggestions on intervention measures that may help to address deviant security behaviour. This empowers decision-makers to make relevant organisational choices that may address the information security behaviour of organisation members.

The main contribution of this paper is that the system is the first of its kind to incorporate decision support for information security behaviour. Future work includes a possible evaluation of the system by a manager in an organisation. The evaluation may include different scenarios that the manager has to analyse (using the decision support system) and make organisational decisions based on members' security behaviour. Thereafter, a critical review on different success factors may be completed.

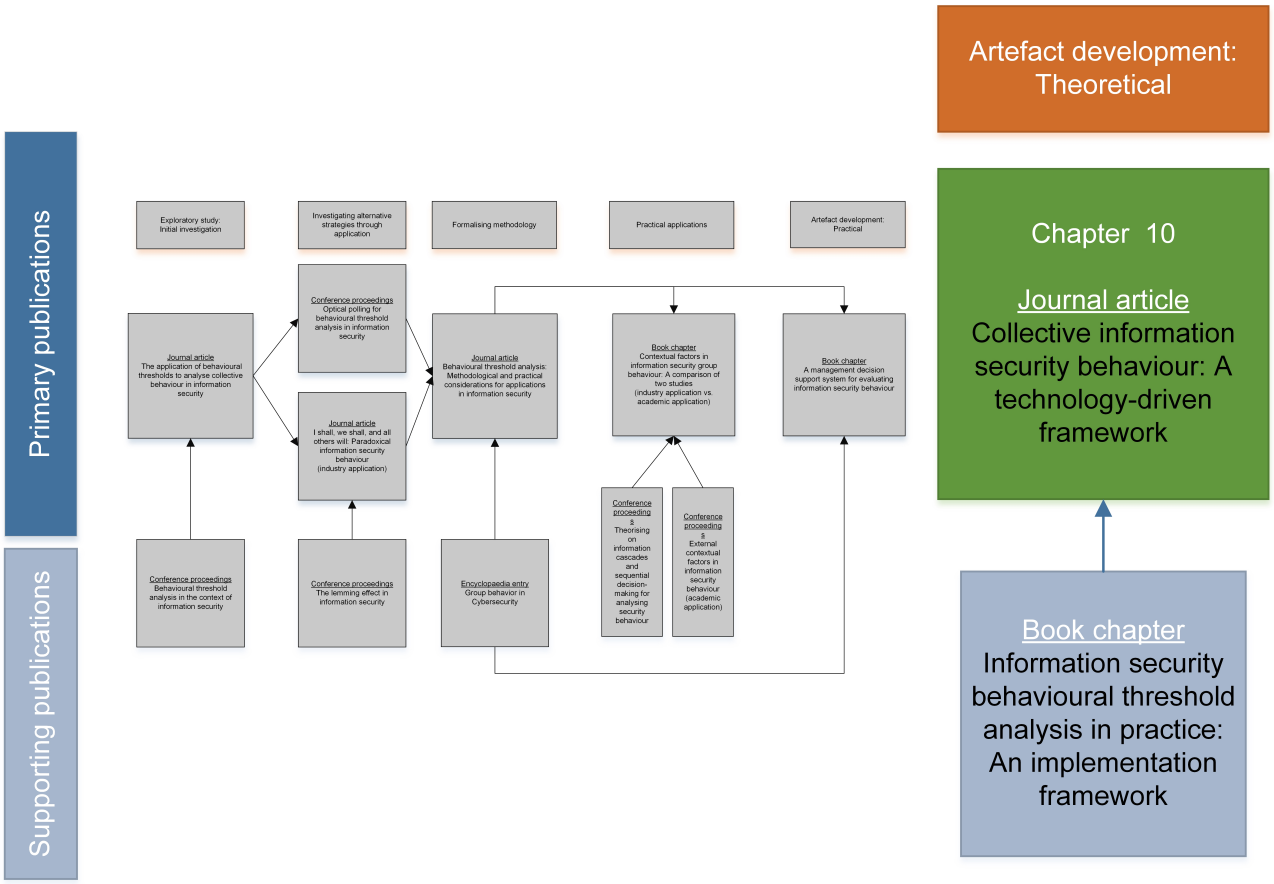
Acknowledgements. The authors would like to thank and acknowledge the contributions of Erik Jonker and Arno Strydom for their undertaking in programming the system based on the requirements as set out by the authors.

References

1. Alshaikh, M., Maynard, S.B., Ahmad, A., Chang, S.: An exploratory study of current information security training and awareness practices in organizations. In: 51st Hawaii International Conference on System Sciences, pp. 5085–5094 (2018)
2. Singh, A.N., Gupta, M.: Information security management practices: case studies from India. Glob. Bus. Rev. **20**, 253–271 (2019)
3. Werlinger, R., Hawkey, K., Beznosov, K.: An integrated view of human, organizational, and technological challenges of IT security management. Inf. Manag. Comput. Secur. **17**, 4–19 (2009)
4. Shao, X., Siponen, M., Pahnila, S.: To calculate or to follow others: how do information security managers make investment decisions? In: 52nd Hawaii International Conference on System Sciences, pp. 4885–4894 (2019)
5. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., Smeraldi, F.: Decision support approaches for cyber security investment. Decis. Support Syst. **86**, 13–23 (2016)
6. Kankanhalli, A., Teo, H.-H., Tan, B.C., Wei, K.-K.: An integrative study of information systems security effectiveness. Int. J. Inf. Manag. **23**, 139–154 (2003)
7. Shropshire, J., Warkentin, M., Sharma, S.: Personality, attitudes, and intentions: predicting initial adoption of information security behavior. Comput. Secur. **49**, 177–191 (2015)
8. Almeida, L., Respício, A.: Decision support for selecting information security controls. J. Decis. Syst. **27**, 173–180 (2018)
9. Furnell, S., Fischer, P., Finch, A.: Plugging the cyber-security skills gap. Comput. Fraud Secur. **2013**, 5–10 (2013)
10. Snyman, D.P., Kruger, H.A.: Behavioural threshold analysis: methodological and practical considerations for applications in information security. Behav. Inf. Technol. **38**, 1–19 (2019)

11. Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: why do they fail to change behaviour? In: 1st International Conference on Cyber Security for Sustainable Society, pp. 118–131 (2019)
12. Furnell, S., Thomson, K.-L.: Recognising and addressing 'security fatigue'. Comput. Fraud Secur. **2009**, 7–11 (2009)
13. Stanton, B., Theofanos, M.F., Prettyman, S.S., Furman, S.: Security fatigue. IT Prof. **18**, 26–32 (2016)
14. Granovetter, M.: Threshold models of collective behavior. Am. J. Sociol. **83**, 1420–1443 (1978)
15. Snyman, D.P., Kruger, H.A.: Behavioural thresholds in the context of information security. In: 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016), pp. 22–32. Plymouth University (2016)
16. Growney, J.S.: I Will if You Will: Individual Thresholds and Group Behavior - Applications of Algebra to Group Behavior. COMAP Inc., Bedford (1983)
17. Hekkala, R., Väyrynen, K., Wiander, T.: Information security challenges of social media for companies. In: 20th European Conference on Information Systems, p. 56 (2012)
18. Gardner, B., Thomas, V.: Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats. Elsevier, Amsterdam (2014)
19. Ashenden, D.: In their own words: employee attitudes towards information security. Inf. Comput. Secur. **26**, 327–337 (2018)
20. Pérez-González, C.J., Colebrook, M., Roda-García, J.L., Rosa-Remedios, C.B.: Developing a data analytics platform to support decision making in emergency and security management. Expert Syst. Appl. **120**, 167–184 (2019)

Chapter 10
-
Article VIII: Collective information security behaviour: A technology-driven framework



Chapter table of contents

10.1 Preamble to Article VIII....183

10.2 Emerald journal style requirements....184

10.3 Article VIII....184

10.3.1 Introduction....185

10.3.2 Literature review....186

10.3.3 Framework model and development....189

10.3.4 Framework evaluation....192

10.3.5 Technology dimension....195

10.3.6 Contributions....198

10.3.7 Conclusion....198

10.3.8 References....199

10.1 Preamble to Article VIII

Artefact development: Theoretical is the final of the research phases that is presented in Figure 1.3, Chapter 1. Consequently, this chapter represents the last of the articles that comprise this thesis. Throughout the different research phases there is a focus on investigations that lead to more fundamental theoretical contributions and practical development that could have important implications for applications in practice. Literature, however, shows a general disconnect between the contribution that research makes, and the eventual applications of the research findings in practice. A possible reason why research findings, while extensive in their own right, seldom effect real-world change can be ascribed to a lack of guidance by researchers on how to facilitate the transition from research into practice. If this premise holds true, researchers have a responsibility to reflect on both the implications of their research and on how the findings thereof can be translated into a practical setting through specifically providing guidelines on how it is to be done. In an attempt to address this shortcoming, the article in this chapter (Article VIII) has the specific aim of proposing an implementation framework for applying information security behavioural threshold analysis in practice. This framework is critically evaluated through exploiting a combination of two qualitative framework evaluation methods from literature. The findings from the previous articles (Articles I-VII) are used to substantiate the successful evaluation of the implementation framework while still observing the evaluation criteria of the amalgamated evaluation methods.

Article VIII was initially written as a conference paper, *Information security behavioural threshold analysis in practice: An implementation framework*[14], and was presented at the *14th IFIP International Symposium on Human Aspects of Information Security & Assurance* which was to be held in Mytilene, Lesvos (Greece) from 8-10 July 2020. However, due to the COVID-19 pandemic and the resulting health and travel restrictions in 2020, the event was held virtually and the paper was presented in this format and subsequently published in the peer-reviewed proceedings.

[14] Snyman, D. P., & Kruger, H. A. 2020. Information security behavioural threshold analysis in practice: An implementation framework. In Clarke, N. L. & Furnell, S. M. Eds., *Advances in Information and Communication Technology: Proceedings of the 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece*, 2020 (Vol. 593): Springer International Publishing, pp. 133-143.

The conference paper is presented in Appendix E. Following the same trend as Articles I, III, and VI, this contribution was once again invited to be extended for further publication after being identified as being of high quality by the conference chairs. This extension which is presented here as Article VIII, named *Collective information security behaviour: A technology-driven framework*[15], was accepted for publication in the *Information & Computer Security* journal.

10.2 Emerald journal style requirements

The requirements of the journal specified that the *Emerald Harvard* referencing style be used. The article is presented in its pre-publication form as it was submitted to the journal as it has not yet been typeset for publication. Information regarding the author guidelines of the journal can be found in Appendix F.

10.3 Article VIII

Article follows on next page.

[15] Snyman, D. P., & Kruger, H. A. (2020). Collective information security behaviour: A technology-driven framework. To appear in *Information & Computer Security.*

Collective information security behaviour: A technology-driven framework

D.P. Snyman, H.A. Kruger
School of Computer Science and Information Systems
North-West University, Potchefstroom, South Africa
dirk.snyman;hennie.kruger@nwu.ac.za

Abstract

Purpose – This paper presents the development of a framework for evaluating group behaviour in information security in practice.

Design/methodology/approach – Information security behavioural threshold analysis is employed as the theoretical foundation for the proposed framework. The suitability of the proposed framework is evaluated based on two sets of qualitative measures (general frameworks and information security frameworks) which were identified from literature. The successful evaluation of the proposed framework, guided by the identified evaluation measures, is presented in terms of positive practical applications, as well as positive peer review and publication of the underlying theory.

Findings – A methodology to formalise a framework to analyse group behaviour in information security can successfully be applied in a practical environment. This application takes the framework from only a theoretical conceptualisation to an implementable solution to evaluate and positively influence information security group behaviour.

Practical implications – Behavioural threshold analysis is identified as a practical mechanism to evaluate information security group behaviour. The suggested framework, as implemented in a management decision support system, allows practitioners to assess the security behaviour and awareness in their organisation. The resulting information can be employed to exert an influence for positive change in the information security of the organisation.

Originality/value – A novel conceptual mapping of two sets of qualitative evaluation measures is presented and used to evaluate the proposed framework. The resulting framework is made practical through its encapsulation in a decision support system.

Keywords Information security, group behaviour, framework development, framework evaluation, decision support system.

Paper type Research paper

1 Introduction

In many disciplines, and for some time, frameworks are developed for a number of different reasons, e.g. to deal with risk or to study and manage behaviour (Tsohou *et al.*, 2008). One of the problems with these frameworks is that most of the time it tends to be just a theoretical framework and when it comes to practical application it is often difficult, and sometimes impossible, to implement it.

This is also the case with behavioural information security research where many models and frameworks are used throughout literature to determine or explain attitude that individuals exhibit towards information security which is indicative of their eventual behaviour (Pham *et al.*, 2017). Behavioural models such as knowledge, attitude, and behaviour (Moletsane and Tsibolane, 2020), theory of planned behaviour (Sommestad *et al.*, 2017), and general deterrence theory (Yuryna Connolly *et al.*, 2017) are used to guide research but are seldom incorporated in implementable frameworks which find their way to practical application

Furthermore, such models are mainly focussed on the individual's behaviour, and researchers infer that this should apply to group behaviour as well. However, this is not always the case, as there are many other influences on group behaviour, such as the lemming effect, contextual factors, influential people, etc. (Johnston *et al.*, 2019). It is, therefore, not enough simply to expect individual behaviour to be indicative of group behaviour.

In this research, an extension of previous work that was presented at a conference and published in the conference proceedings (Snyman and Kruger, 2020b) is presented here. To the best of the researchers' knowledge, save for that of Snyman and Kruger (2020b) which is reiterated here, no other framework for analysing and predicting information security group behaviour is currently available in literature. Therefore, a formal framework is proposed for group behaviour in information security. This proposed framework is based in part on aspects found in existing frameworks (Pham *et al.*, 2017), i.e. norms, beliefs, attitudes, etc. The other integral part of the framework will then consist of those aspects that are specific to group behaviour, i.e. the use of a technique, such as behavioural threshold analysis that considers factors, such as the lemming effect and external contextual factors. An overarching study, in which the use of a behavioural threshold analysis approach was conceptualised in terms of group behaviour in information security, culminates with the research that is presented here.

With the abovementioned background in mind, the aims of this study are to:

1. *Formalise a framework for evaluating information security group behaviour in practice, supported by behavioural threshold analysis as the underlying theory and critically evaluate the proposed framework based on qualitative measures from literature; and*
2. *Discuss a practical implementation of the framework as a management decision support system, thereby allowing information security practitioners to utilise the approach in a real-world setting.*

The remainder of this paper is structured as follows: In **Section 2,** a brief contextualisation for applying research in practice and a theoretical view on the requirements of a successful framework are presented. In **Sections 3** and **4** the development of the resulting framework and the evaluation thereof, based on the requirements from Section 2 are described. The use of technology to facilitate the practical application of the theoretical framework is discussed in **Section 5**. A discussion on the general and specific contributions of the resulting framework is presented in **Section 6** and the paper is concluded in **Section 7**.

2 Literature review

In this literature review section, attention is given to the contextual background of this research and the requirements for frameworks in general as well as for information security.

2.1 Contextualisation

Translating research findings and recommendations of any nature into practice remains an elusive process (Kent, 2019; Grimshaw *et al.*, 2012; Kitson *et al.*, 1998). Some of the reasons why this general disconnect exists between most types of research and the related acceptance thereof in practice include: Ambiguity in existing research (Kent, 2019; Tsohou *et al.*, 2008); limited published reflection on implementation (Tsohou *et al.*, 2008); ongoing research is often still inconclusive (Kitson *et al.*, 1998); decision makers lack the required information (Haines and Donald, 1998); and attitudes and beliefs of individuals (Kent, 2019; Bakry, 2003) which translates to social and cultural resistance to the change associated with implementation.

This disconnect between research and practice has also been identified in the domain of information security (AlHogail, 2015; Tsohou *et al.*, 2008), where it especially holds true for non-technical aspects of information security such as information security awareness and behaviour. Research into human behaviour (and how it relates to information security behaviour and culture) is often based on, and guided by, theoretical models from the fields of sociology and social psychology. While such models can assist in uncovering the intricacies of behaviour by highlighting complexity and structuring the underlying themes, they do not necessarily provide for simple integration into actionable methods in practice.

Further compounding the issue are challenges that relate to the management of information security in organisations, which are apparent in literature. These issues include, but are not limited to the following:

Top management buy-in – The support from executive management often has a profound influence on the eventual information security in an organisation through funding, supporting initiatives, and contributing to the overall security culture in the organisation (Singh and Gupta, 2019; Kankanhalli et al., 2003).

Managing human factors – The elusive task of effectively addressing the human factor remains one of the key components in any organisation's information security strategy (Shao *et al.*, 2019; Alshaikh *et al.*, 2018; Shropshire *et al.*, 2015).

Budget constraints – Limited funding (often due to lack of top management buy-in) constrains the security controls that can be put in place by those charged with maintaining information security (Almeida and Respício, 2018). Limited or lacking controls leave unprotected avenues that can be exploited.

Management confidence and skill – A shortage of trained and arguably more importantly experienced security practitioners is a decades old global phenomenon that persists to this day (Furnell *et al.*, 2013). As a result, organisational decision-makers are often not trained to manage information security and are therefore not confident in their ability to assess threats and determine how countermeasures are to be implemented (Fielder *et al.*, 2016).

The abovementioned divide between research and practice, and the subsequent management issues in information security highlight the importance for developing approaches that do not remain only theoretical but are implementable in practice. The level of success of the implementation of such an approach, in general terms, is subject to three criteria, namely *Evidence*, *Context*, and *Facilitation* (ECF) (Kitson *et al.*, 1998). In terms of research pertaining to information security (specifically security culture), AlHogail (2015) suggests following the STOPE approach (Bakry, 2003) to facilitate change when implementing new approaches to effect change in the culture and the eventual underlying behaviour. The dimensions to be adhered to for STOPE are *Strategy*, *Technology*, *Organisation*, *People*, and *Environment*.

These criteria and dimensions are therefore subsequently used to guide and evaluate the development of a framework for applying the behavioural threshold analysis approach, in the context of information security, in practice. In the resulting practical implementation of the framework as a decision support system, specific reference is made to the *Technology* dimension (STOPE) as explained in the following sub-section.

2.2 Framework requirements

The qualitative criteria for evaluating frameworks in general (*Evidence*, *Context*, and *Facilitation*) and for frameworks for information security (STOPE) will be presented here and contextualised in terms of research in general versus information security research. Finally, a mapping of how these two approaches align, and how they relate to this research is presented.

2.2.1 Evidence, Context, and Facilitation

In terms of an implementation framework, the interaction between Evidence (E), Context (C), and Facilitation (F) is said to determine the eventual Successful Implementation (SI) of the framework in practice, i.e. SI is a function of three criteria (Kitson *et al.*, 1998) so that

$$SI = f(E, C, F) \quad (1)$$

The success of the implementation is therefore dependent on the level of maturity by which each of the criteria is met. Each of the criteria, and what each represents in terms of a framework, is briefly described here. Where applicable, these criteria are already presented in terms of information security:

Evidence – Evidence refers to the level of scrutiny that the model or approach that underpins a framework has undergone. Is there substantiated proof that the model is fit for purpose? (Kitson *et al.*, 1998)

Context – Context is concerned with the setting in which a framework is to be applied in practice. In general, this refers to the physical attributes of the environment such as buildings, people, and processes (Snyman and Kruger, 2020a). However, for the successful implementation of a framework, this view might be too narrow, since in essence context also implicitly refers to intangible qualities, such as individual and group behaviour, and the underlying (security) culture (Snyman and Kruger, 2020a; Kent, 2019).

Facilitation – Implementing research in practice is essentially a process whereby change of some kind is sought to be effected. Change is a process that ought to be facilitated if it is to be successful and long-lived (Kent, 2019). Such facilitation refers to the understanding of (and ultimately altering) attitudes and behaviours, specifically by leveraging the way in which "an individual is able to influence other individuals' attitudes or overt behaviour" (Kent, 2019; Rogers, 2010). In terms of information security, Snyman and Kruger (2017a) hypothesise that while some people may inherently be more influential (Kent, 2019), the behaviour of all individuals exerts influence on the eventual behaviour of a group.

2.2.2 STOPE

Information security frameworks may be evaluated by means of a critical evaluation of how well the framework addresses *Strategy*, *Technology*, *Organisation*, *People*, and the *Environment*. Each of these dimensions is briefly explained below, based on the work of AlHogail (2015) which contextualises them in terms of information security.

Strategy – Strategy refers to the suggested measures that are applied to effect change within an organisation to improve its overall levels of information security. These approaches may include the implementation of formal plans of action, such as information security policies and guidelines as well as the structured approach of a framework.

Technology – In this context, technological means of addressing information security is referred to as technology. Frameworks should ideally provide for changes or improvements on the technical measures that are used to safeguard systems. In line with the second research aim,

a decision support system is presented in Section 5 as an implementation of the framework as a whole, but also specifically addressing the technology dimension.

Organisation – The success of strategy is reliant on the underlying security culture of an organisation. This culture and eventual behaviour are often influenced by the way in which an organisation is structured. A framework should provide guidelines for how structures within an organisation will influence the application thereof and, ideally, how structures may be leveraged to achieve the goal of the framework.

People – Information security ultimately revolves around people. It is often people that undo security through unwanted actions. Frameworks should seek to address the human aspect of information security in terms of behaviour, culture and awareness.

Environment – Environment view refers to the greater context in which an organisation has to address information security, and which should be included in the application of a framework. On a macro level, this may include concepts, such as regulatory frameworks and legislation (AlHogail, 2015), but on a smaller level can refer to the context in which an individual or group behave in terms of information security (Snyman and Kruger, 2020a).

2.2.3 Mapping STOPE to ECF

An assessment of the framework evaluation criteria as mentioned in Sections 2.1 and 2.2 above allows for a combination of the two approaches by means of a conceptual mapping. Table I shows the conceptual mapping of STOPE to ECF:

Table I. Conceptual mapping of STOPE to ECF

Evidence	*Context*	*Facilitation*
Peer review combined with resulting STOPE evaluation	O: Organisation P: People E: Environment	S: Strategy T: Technology

From Table I, it can be seen that the individual views from STOPE could not as easily be mapped to Evidence (ECF), as all these views can contribute in some way to this criterion. It is concerned with the rigour of the underlying model on which a framework is based. It stands to reason then, that in combination with other types of measures that can confirm said rigour (e.g. peer review, or experimentation), evidence can thus be conceptualised as the resulting evaluation that is conveyed by STOPE. However, in the context of this research, Evidence will be used as a freestanding criterion, evaluated on the available peer review, case studies, and successful implementations. For the remaining criteria, the Organisation, People and Environment from STOPE (AlHogail, 2015) can be directly mapped to Context (Kent, 2019) from ECF. Overlapping themes include people, behaviour, culture, and physical attributes of the environment. In the final instance, Facilitation (ECF) encompasses the strategy and technology views from STOPE. The common concepts from these constructs that can be identified are the approaches for achieving positive change through organisational, technological, and human means.

3 Framework model and development

In order to describe the development of the suggested framework, the underlying theoretical model should first be presented. In this section, the aim is firstly to summarise the behavioural

threshold analysis model as implemented in the greater research project, followed by a description of the resulting framework and its elements.

3.1 Behavioural threshold analysis model

Group behaviour is a complex phenomenon. To analyse this complexity, Granovetter (Granovetter, 1978) describes a theory called "Threshold models of collective behaviour". The model described by Granovetter is used as the underlying theoretical grounding for the framework. In short, the model takes into account the mechanisms whereby individuals influence the behaviour of each other, i.e. based on an intrinsic inclination of an individual to follow the example of existing group behaviour. This inclination to follow behaviour is conceptualised as the individual's behavioural threshold. The said threshold is expressed as a percentage of group members who perform a behaviour that will sway an individual to participate in the specific behaviour. When the (perceived) participation rate of group members exceeds the behavioural threshold of the individual, the individual will follow the group's example and will also perform the behaviour. When participation in the group behaviour exceeds an individual's threshold for participation, the individual might even perform group behaviour that is contrary to his/her convictions and predisposition.

Growney (1983) describes how the model can be implemented in circumstances where groups of individuals congregate and how the mathematical aggregate of behavioural thresholds may be interpreted to allow for a prediction of eventual group behaviour. The model was successfully applied in information security in earlier, related studies and the reader is referred to these sources for in-depth reading on the application of behavioural threshold analysis in information security (Snyman and Kruger, 2019a; Snyman *et al.*, 2018; Snyman and Kruger, 2017a).

3.2 Development of information security group behaviour framework

In Section 1, reference was made to the first aim of this research, namely, to formalise a framework for the practical application of behavioural threshold analysis in information security. To address this aim, Figure 1 shows the proposed framework for evaluating group behaviour in information security and illustrates the overarching development and categorises different epochs of the framework's development. Each of the epochs is subsequently briefly described below.

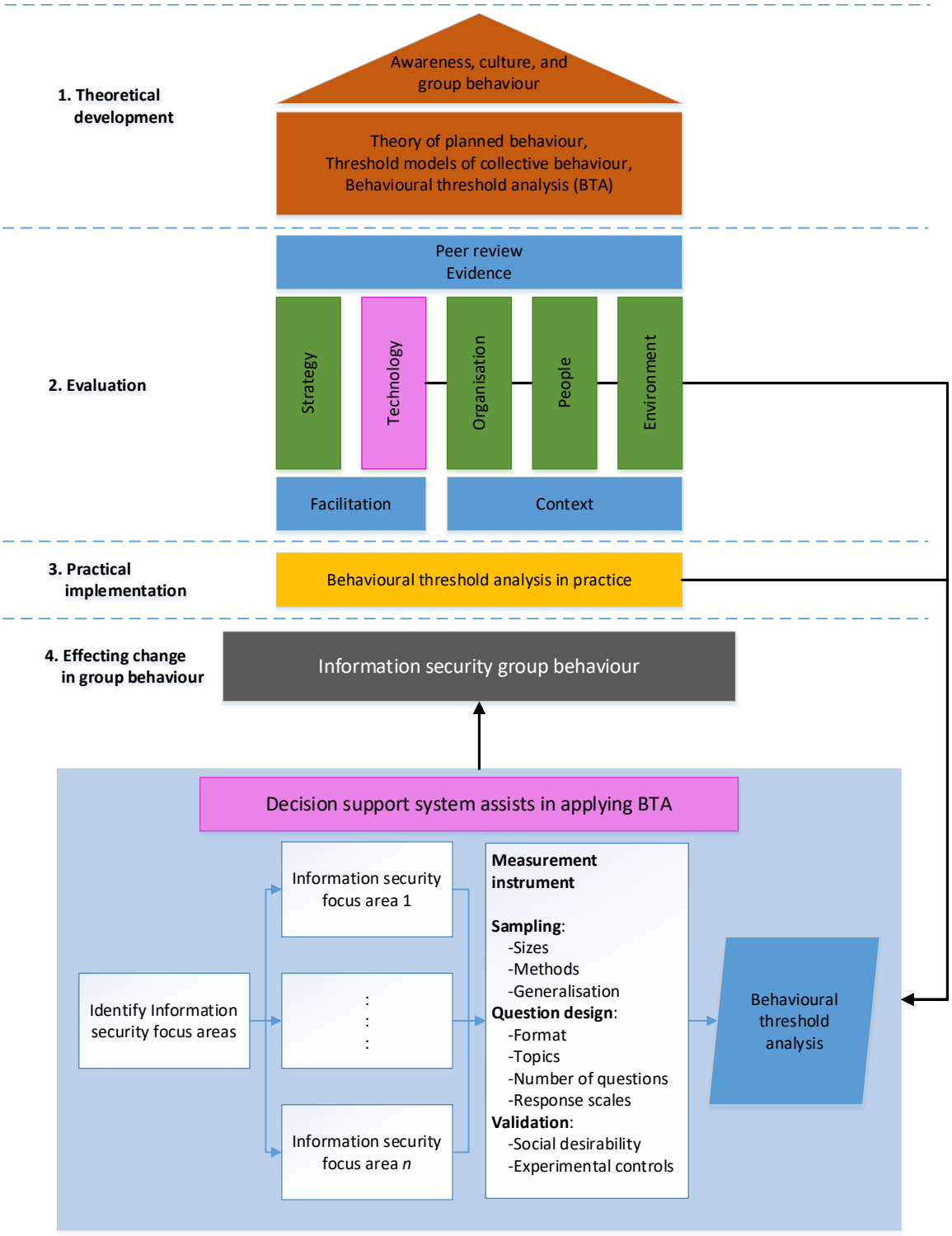


Figure 1. Framework for the evaluation of information security group behaviour in practice

1) Theoretical development – This epoch refers to the investigation into group behaviour in information security. It includes a review of the related literature on the following themes: human behaviour in general and in the context of information security; modelling human behaviour, e.g. the theory of planned behaviour, and its employment in security awareness and security culture; and group behaviour (threshold models of collective behaviour) and the analysis thereof (behavioural threshold analysis). The development of the underlying theory

also comprises the development of methodological and practical guidelines for experimental and practical applications.

2) Evaluation – Based on the aforementioned ECF criteria and STOPE views, the evaluation epoch refers to a formal evaluation of the underlying theoretical assumptions and the framework itself. In the following section (see Section 4), a formal evaluation of the proposed framework is shown.

3) Practical implementation – After a successful evaluation, evidencing a well-founded theoretical basis and framework, the approach is ready for implementation. The blown-up view shows the minutia of the application of behavioural threshold analysis in information security that is facilitated through the decision support system in Section 5.

4) Effecting change in group behaviour – The results of the behavioural threshold analysis application may be interpreted to detect areas of information security that need intervention to improve behaviour.

In the following segment (Section 4), how the combination of ECF and STOPE was employed to evaluate the proposed framework is shown.

4 Framework evaluation

During the related research and the development of behavioural threshold analysis as an approach for information security, the requirements for ECF and STOPE were met. In this section, the extent to which peer review and practical applications contribute to the maturity of the framework is described.

4.1 Peer review and publication

Table II shows the STOPE criteria and ECF views. A critical evaluation and motivation for the resulting evaluation are provided. It should be noted that the evaluation, especially the *Evidence* column, is chiefly based on the findings from the preceding works of the authors on the central theme of behavioural threshold analysis in information security. This does not disregard the contributions of other authors on related topics. Each prior research contribution drew from the available body of literature at the time of its publishing and is used here as summative reference. The reader is referred to these publications for the full literature backgrounds that allow them to be used here as motivation and evidence.

Table II. Critical evaluation of the proposed framework

	STOPE criteria	**Critical evaluation and motivation**	*Evidence* (peer-reviewed publications)
Context	Organisation	One of the main c*ontexts* with which behavioural threshold analysis is concerned, is that of the *Organisation*. The ultimate outcome of the successful implementation of the approach is improved levels of information security within any organisation where it is applied. A collection of papers in information security journals, conference proceedings, and book chapters, that contribute to the rigour of the underlying theoretical model and approaches were published. *Organisation* forms part of all of the previous papers. The reader is referred to the References section for full bibliographic information. However, one of the papers that specifically relate to the evaluation of information security behaviour in an organisational setting is pertinent here.	*I shall, we shall, and all others will: Paradoxical information security behaviour* (Snyman *et al.*, 2018)
	People	Behavioural threshold analysis is based on the behaviour and interaction of people. All the previous work therefore encompasses the *People* view; however, one paper is highlighted here: Developing the interrelated concepts of sequential decision-making and information cascades in information security, a novel view of the *context* of how information security behaviour is formed was peer-reviewed, published and presented at an international conference.	*Theorising on information cascades and sequential decision making for analysing security behaviour* (Snyman and Kruger, 2019b)

	Environment	Given the influence of the *environment*, and its many facets on behaviour, a paper on the *contextual* factors that influence information security behaviour was presented at an international conference after peer review and published in the proceedings.	*External contextual factors in information security behaviour* (Snyman and Kruger, 2020a)
Facilitation	Strategy	A paper that describes and validates the underlying methodology, including some practical considerations for behavioural threshold analysis in information security, was published in a peer-reviewed journal. This contributes to formalising the *strategy* to *facilitate* positive change in information security.	*Behavioural threshold analysis: Methodological and practical considerations for applications in information security* (Snyman and Kruger, 2019a)
	Technology	With the aim of facilitating and partially automating behavioural threshold analysis, a novel data collection method (optical polling) and decision support system (DSS) were developed. This *technology* can help *facilitate* the practical aspects of the model implementation. The novel data collection and the DSS was presented at an international conference and published as a peer-reviewed book chapter. The Technology dimension is discussed further in Section 5.	*Optical polling for behavioural threshold analysis in information security* (Snyman and Kruger, 2017b); *A management decision support system for evaluating information security behaviour* (Snyman and Kruger, 2020c)

The applications of the approach in practice are presented in the following sub-section.

4.2 Applications in practice

Throughout the development of the approach to apply behavioural threshold analysis in information security, practical experiments were conducted to test the working of the model within this context. An initial pilot study was conducted to test the feasibility of the model (Snyman and Kruger, 2017a). After further development of the approach and the underlying theoretical foundations, such as the required methodological approach (*Strategy*, Table II), two successful practical applications were conducted:

The first practical application of behavioural threshold analysis was conducted at a utility company (*Organisation*, Table II). The resulting insights and recommendations regarding employees' information security behaviour were communicated in a report to the company. Feedback indicated that the insights were found to be invaluable in guiding the directions of future awareness campaigns.

The second application was in an academic context (*Environment*, Table II) at a South African University. The results from the exercise correlated with the expected and observed information security behaviour of students in a university residence. The success of these practical applications, the commonalities and differences between the different contexts where the approach was applied, and the reporting publications passing peer review, verifies that this procedure for application (as presented in this framework) is effective.

In the following section, a contribution to promote future practical applications of the approach is presented which also formalises the approach along the lines of the *Technology* dimension of the STOPE evaluation criteria.

5 Technology dimension

Snyman and Kruger (2020c) describe the development of a decision support system for supporting and automating the application of behavioural threshold analysis in practice. The working of this system is reiterated here and related to the *Technology* dimension of STOPE as a practical instantiation of the framework. Technology should be harnessed by management to facilitate and promote positive change. This system is proposed as a tool for management (as the user) to evaluate and understand information security behaviour in their organisation and ultimately provide insight on how to proceed to effect the desired outcomes. In the context of information security behavioural threshold analysis, three phases need to be completed to evaluate group behaviour. These phases are typically all performed by an expert in the absence of a mechanism that empowers a nonprofessional to perform the evaluation by him/herself with limited expert involvement. The phases are briefly discussed below and the contribution of the system highlighted:

Phase 1 – Expert

- An expert performs an initial assessment of the organisation and suggests information security focus areas that are relevant to the specific environment; and
- Constructs a behavioural threshold analysis measurement instrument to evaluate said focus areas. The instrument is based on predetermined, appropriate guidelines. Care is given to the format of the questions and responses to allow importing into the system.
- Expert involvement terminates at this junction.

Phase 2 – User

- Management distributes the measurement instrument to the members of the organisation through an online platform.
- The responses are then uploaded to the decision support system.

Phase 3 – Decision support system

- The responses undergo automatic pre-processing to recognise the security focus areas, and different organisational levels and roles of the respondents in order to categorise behaviour per focus area and organisational grouping. A clean-up of the response data is performed as required for behavioural threshold analysis. The integrity of the underlying data is assured through validation.
- Threshold calculations are performed by the system and the resulting analysis is presented on an interactive dashboard that conveys the results and suggestions in an intuitive manner.

The advantage of the automation that is presented in the third phase, is that the user does not require expert knowledge. A nonprofessional manager can gain insight into how group members of the organisation will behave when confronted with different information security issues.

To illustrate the information conveyed by the dashboard the analysis and reporting area of the dashboard is presented in Figure 2. The behavioural threshold analysis result that is depicted here is based on the responses that were collected for the aforementioned practical application at a utility company. *Incident reporting* is shown as an example security focus area. Permanent staff is selected as the organisational grouping.

The primary graph (blue line) shows the cumulative original responses as they were provided by the respondents, while the secondary (orange) reflects the responses that were modified due to possible presence of the social desirability bias that may be present in self-reporting of this kind (Van de Mortel, 2008). Adjustments to the responses were made in accordance with seminal social desirability literature (Ray, 1984; Reynolds, 1982; Crowne and Marlowe, 1964). The two graphs indicate the boundaries of the best- and worst-case scenarios between which the actual behaviour should fall.

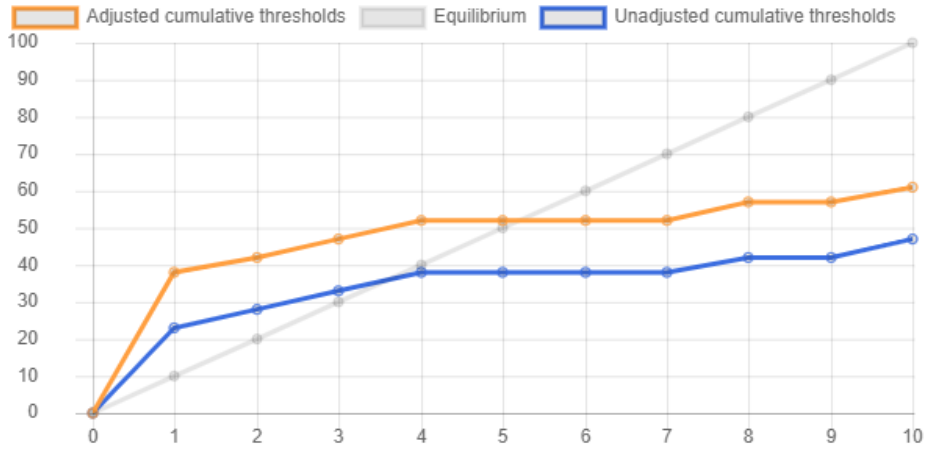
The two graphs, and more specifically the intersections of the graphs with the equilibrium line, are used to determine the level of participation in the information security behaviour (Growney, 1983; Granovetter, 1978). For example, the intersection of the orange line on the graph in Figure 2 indicates that the percentage of *staff* that will not *report incidents* might be as high as **53%**. The model reaches an equilibrium at this point, i.e. equilibrium is found when a graph intersects the equilibrium line from above. This means that the group participation should not grow and exceed this percentage but will also not decline on its own without an intervention.

A text-based report (bottom part of Figure 2) helps the user interpret the meaning that the graph conveys by explaining the magnitude of the security threats, classified as high-, medium-, or low-level threats. The report provides possible actions to improve the current state of information security behaviour in the organisation.

The aforementioned measurement instrument is commonly used to assess a number of security focus areas for a number of organisational groupings simultaneously. The system can harness this information and provides an aggregated view of the overall outlook for the organisation. This information is presented as a heatmap that allows the user to identify problem areas. The heatmap also provides functionality to perform a what-if analysis to visualise how behavioural improvements in one focus area or one organisational grouping will influence the levels of information security for the organisation as a whole. Interested readers are referred to Snyman and Kruger (2020c) for a detailed discussion of the complete decision support system.

Analysis and Reporting

Incident reporting for Staff



Heatmap report

The current outlook for the participation in unsafe information security behaviour for **staff** members, with regards to **incident reporting** is **medium**. The percentage of staff members that will act in a contraindicated manner, is currently **52%**. This requires **moderate attention**. Unsafe **incident reporting** behaviour may put your organisation at risk. Address security behaviours with a **higher** evaluation first.

Overview

The following **consequences**, among others, exist if **incident reporting** is not applied:
-- Direct and indirect financial losses;
-- Non-compliance with legislation and/or standards; and
-- Damage to organisational image.

Suggestions

Employ **security awareness programs** that address the abovementioned threats. During training, the following should be emphasised:
-- Review organisational policies and guidelines relating to incident reporting procedures;
-- Basic security hygiene should be reaffirmed;
-- Policies relating to information security in general should be revisited;
-- Review incident types; and
-- Address incidents that require reporting.

Other

Typical incidents to **report** include:
-- Phishing attempts;
-- Lost or stolen computers or storage devices;
-- (Willful) exposure of sensitive information;
-- Malware attacks;
-- Data breaches of any kind; and
-- Password sharing.

Figure 2. Decision support system: Analysis and reporting

6 Contributions

The contributions of this research are discussed here in terms of the initial research aims. The aims are reiterated and a discussion is provided on how these aims were met:

> *Formalise a framework for evaluating information security group behaviour in practice, supported by behavioural threshold analysis as the underlying theory* and *critically evaluate the proposed framework based on qualitative measures from literature*

The first research question was addressed in the following way: Behavioural threshold analysis was identified as a *mechanism* to evaluate information security group behaviour and expressed as a well-founded underlying theory for the proposed framework; the framework was *critically evaluated* in terms of the qualitative measures conceptualised from literature, and furthermore, the approach outlined in this framework was successfully applied in practice, which further illustrated the suitability of the framework; the framework can be construed as an instrument for *appraising information security awareness* in organisations, which allows information security practitioners to effect positive change in information security behaviour; a *methodology* for identifying information security focus areas was identified; and an instrument was contributed that is *novel* in comparison to existing tools for analysing information security group behaviour with respect to its sensitivity towards the influence of external stimuli, such as contextual factors and the lemming effect.

Subsequently, the second research question is discussed.

> *Discuss a practical implementation of the framework as a management decision support system, thereby allowing information security practitioners to utilise the approach in a real-world setting.*

The instantiation of the framework as a decision support system contributes to the framework transitioning from a theoretical artefact to a practically workable solution: Organisational management are afforded a *tool* whereby insight into the information security behaviour of the group members can be generated; management are *empowered in decision-making* relating to the human aspect of information security; *risks* to the information security of the organisation can be identified by using the decision support system and then addressed through specific inclusion of related topics in security awareness programs; and the *technology* dimension (STOPE) for *evaluating* framework was specifically harnessed to facilitate the instantiation.

7 Conclusion

In this paper, a formal framework for the evaluation of group behaviour in information security was presented. The framework is based on behavioural threshold analysis as the central theoretical model. Two qualitative evaluation methods for frameworks were identified from literature and contextualised in terms of information security group behaviour. A combination of the two evaluation methods was used to evaluate the fittingness of the proposed framework for analysing information security group behaviour. Based on the resulting evaluation, grounded in scientific peer review, as well as successful applications in practice, the proposed framework was deemed to be fit for purpose. The ensuing framework was made practical through the implementation thereof as a decision support system, which allows organisations to employ the theoretical approach framework in practice to effect the desired change in their organisational information security behaviour.

References

Alhogail, A. (2015), "Design and validation of information security culture framework", *Computers in Human Behavior,* Vol. 49, pp. 567-575.

Almeida, L. and Respício, A. (2018), "Decision support for selecting information security controls", *Journal of Decision Systems,* Vol. 27, No. Sup. 1, pp. 173-180.

Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2018), "An exploratory study of current information security training and awareness practices in organizations", *51st Hawaii International Conference on System Sciences,* pp. 5085-5094.

Bakry, S.H. (2003), "Development of security policies for private networks", *International Journal of Network Management,* Vol. 13, No. 3, pp. 203-210.

Crowne, D.P. and Marlowe, D. (1964), "The approval motive", *Wiley, New York.*

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. and Smeraldi, F. (2016), "Decision support approaches for cyber security investment", *Decision Support Systems,* Vol. 86, pp. 13-23.

Furnell, S., Fischer, P. and Finch, A. (2013), "Plugging the cyber-security skills gap", *Computer Fraud & Security,* Vol. 2013, No. 7, pp. 5-10.

Granovetter, M. (1978), "Threshold models of collective behavior", *American Journal of Sociology,* Vol. 83, No. 6, pp. 1420-1443.

Grimshaw, J.M., Eccles, M.P., Lavis, J.N., Hill, S.J. and Squires, J.E. (2012), "Knowledge translation of research findings", *Implementation Science,* Vol. 7, No. 1, pp. 50.

Growney, J.S. (1983), "I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior", *COMAP Inc., Bedford, MA.*

Haines, A. and Donald, A. (1998), "Making better use of research findings", *British Medical Journal,* Vol. 317, No. 7150, pp. 72-75.

Johnston, A.C., Di Gangi, P.M., Howard, J. and Worrell, J. (2019), "It takes a village: Understanding the collective security efficacy of employee groups", *Journal of the Association for Information Systems,* Vol. 20, No. 3, pp. 186-212.

Kankanhalli, A., Teo, H.-H., Tan, B.C. and Wei, K.-K. (2003), "An integrative study of information systems security effectiveness", *International Journal of Information Management,* Vol. 23, No. 2, pp. 139-154.

Kent, B. (2019), "Implementing research findings into practice: frameworks and guidance", *International Journal of Evidence-Based Healthcare,* Vol. 17, pp. S18-S21.

Kitson, A., Harvey, G. and Mccormack, B. (1998), "Enabling the implementation of evidence based practice: a conceptual framework", *BMJ Quality & Safety,* Vol. 7, No. 3, pp. 149-158.

Moletsane, T. and Tsibolane, P. (2020), "Mobile information security awareness among students in higher education: An exploratory study", *2020 Conference on Information Communications Technology and Society (ICTAS),* IEEE, pp. 1-6.

Pham, H., Brennan, L. and Richardson, J. (2017), "Review of behavioural theories in security compliance and research challenge", *Informing Science and Information Technology Education Conference, Vietnam*, COHEN, E., (ed.), Santa Rosa, CA, USA, Informing Science Institute, pp. 65-76.

Ray, J.J. (1984), "The reliability of short social desirability scales", *Journal of Social Psychology,* Vol. 123, No. 1, pp. 133-134.

Reynolds, W.M. (1982), "Development of reliable and valid short forms of the Marlowe-Crowne Social Desirability Scale", *Journal of Clinical Psychology,* Vol. 38, No. 1, pp. 119-125.

Rogers, E.M. (2010), "Diffusion of innovations"*, Simon and Schuster, New York, NY*.

Shao, X., Siponen, M. and Pahnila, S. (2019), "To calculate or to follow others: How do information security managers make investment decisions?", *52nd Hawaii International Conference on System Sciences,* pp. 4885-4894.

Shropshire, J., Warkentin, M. and Sharma, S. (2015), "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior", *Computers & Security,* Vol. 49, pp. 177-191.

Singh, A.N. and Gupta, M. (2019), "Information security management practices: Case studies from India", *Global Business Review,* Vol. 20, No. 1, pp. 253-271.

Snyman, D.P. and Kruger, H.A. (2017a), "The application of behavioural thresholds to analyse collective behaviour in information security", *Information & Computer Security,* Vol. 25, No. 2, pp. 152-164.

Snyman, D.P. and Kruger, H.A. (2017b), "Optical polling for behavioural threshold analysis in information security", *International Conference on Information and Knowledge Engineering (IKE'17),* Las Vegas, USA, CSREA Press, pp. 39-45.

Snyman, D.P. and Kruger, H.A. (2019a), "Behavioural threshold analysis: Methodological and practical considerations for applications in information security", *Behaviour & Information Technology,* Vol. 38, No. 11, pp. 1-19.

Snyman, D.P. and Kruger, H.A. (2019b), "Theorising on information cascades and sequential decision-making for analysing security behaviour", *5th International Conference on Information Systems Security and Privacy (ICISSP2019),* SCITEPRESS – Science and Technology Publications, Lda., Prague, Czech Republic, pp. 205-212.

Snyman, D.P. and Kruger, H.A. (2020a), "External contextual factors in information security behaviour", *6th International Conference on Information Systems Security and Privacy (ICISSP 2020),* FURNELL, S., MORI, P., WEIPPL, E. & CAMP, O., (eds.), Valletta, Malta, SCITEPRESS – Science and Technology Publications, Lda., pp. 185-194.

Snyman, D.P. and Kruger, H.A. (2020b). Information security behavioural threshold analysis in practice: An implementation framework. *In:* CLARKE, N. & FURNELL, S. (eds.) *Advances in Information and Communication Technology: Proceedings of the 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020.* Springer International Publishing.

Snyman, D.P. and Kruger, H.A. (2020c). A management decision support system for evaluating information security behaviour. *In:* VENTER, H., LOOCK, M., COETZEE, M., ELOFF, M. & ELOFF, J. (eds.) *Information and Cyber Security - 18th International Conference, ISSA 2019, Johannesburg, South Africa, August 15, 2019, Proceedings.* 1st ed.: Springer International Publishing.

Snyman, D.P., Kruger, H.A. and Kearney, W.D. (2018), "I shall, we shall, and all others will: Paradoxical information security behaviour", *Information & Computer Security,* Vol. 26, No. 3, pp. 290-305.

Sommestad, T., Karlzén, H. and Hallberg, J. (2017), "The theory of planned behavior and information security policy compliance", *Journal of Computer Information Systems,* Vol. 59, No. 4, pp. 344-353.

Tsohou, A., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2008), "Investigating information security awareness: Research and practice gaps", *Information Security Journal: A Global Perspective,* Vol. 17, No. 5-6, pp. 207-227.

Van De Mortel, T.F. (2008), "Faking it: Social desirability response bias in self-report research", *The Australian Journal of Advanced Nursing,* Vol. 25, No. 4, pp. 40-48.

Yuryna Connolly, A., Lang, M., Gathegi, J. and Tygar, D. (2017), "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study", *Information & Computer Security,* Vol. 25, No. 2, pp. 118-136.

Chapter 11
-
Summary and conclusion

Chapter table of contents

11.1 Chapter introduction 202

11.2 Synopsis of the study 202

11.3 Contributions of the study 207

11.4 Limitations and directions for future research 209

11.5 Chapter summary 209

11.1 Chapter introduction

Chapter 11 constitutes the final and concluding chapter of this thesis. In this chapter, a synopsis of the study is included, followed by a review of how the research objectives were achieved. The contributions of the study from Chapter 1 are revisited, and some limitations and the opportunities they present for future work are presented.

11.2 Synopsis of the study

This thesis, as a series of papers, comprises some eleven chapters. In the first chapter, the study was introduced and a brief description of the research design and methodology was presented. Subsequently, a literature review chapter was included to highlight predominant themes from literature relating to the research subject of this study. Thereafter, eight research articles were incorporated as the main body of this research in five main categories: exploratory investigation, investigating alternative strategies through application, formalising methodology, practical applications, and artefact development.

Chapter 1 was employed as an introduction to the study. The research was contextualised through a brief discussion on the gaps in the current state of research to which this study can contribute. This resulted in the proposed primary and secondary research questions, the aim and objectives, and research design. The study endeavoured to answer the primary research question: *How can behavioural threshold analysis be employed as an aid for managing the human factor in information security group behaviour?* The following secondary research questions (sub-questions) were identified to support the answer to the primary question:

- *What is the current state of behavioural information security with specific regard to the models and methods to address the human factor in information security?*
- *Can behavioural threshold analysis be applied to assess information security group behaviour?*
- *How can generic behavioural threshold analysis be improved for applications in the context of information security?*
- *How can behavioural threshold analysis be established as a novel approach for evaluating information security group behaviour?*
- *Can this novel approach, based on the formalised methodology, be successfully applied in practical real-world contexts to assess information security group behaviour?*
- *How can this approach be embodied as a supporting tool to contribute to the theory of behavioural information security and the management of the human factor in practice?*

Derived from the primary research question, the main aim of the study was to *develop a mechanism whereby information security behavioural threshold analysis may be used as a tool to contribute to the management of the human factor in information security.* The secondary aims translated into the following objectives:

1. *Conduct* a literature review on topics relating to human behaviour, information security, and behavioural threshold analysis;
2. *Perform* an initial assessment of the suitability of behavioural threshold analysis for information security by experimenting with the application of the model within this context;
3. *Determine* best practices for data collection for behavioural threshold analysis when it is applied to information security;
4. *Apply* behavioural threshold analysis in a real-world setting to assess an organisation's information security and evaluate the newly adapted approach at the same time;

5. *Construct* and *validate* a formal methodology and provide practical guidance for applications in information security;
6. *Evaluate* the applicability of employing behavioural threshold analysis to assess group behaviour, based on other theoretical models of group behaviour to *substantiate* its validity;
7. *Compare* different industries in terms of their information security behavioural threshold analysis results, related to the difference in environments;
8. *Contribute* to the practice of behavioural information security by automating implementations of the identified methods whereby behavioural threshold analysis may be employed as a tool for information security management; and
9. *Contribute* to the theory and practice of behavioural information security by creating and *validating* a framework for evaluating the proposed approach.

Chapter 2 was used to pursue the first of the research objectives (**Objective 1**, *conduct* literature review). Chapters 3-10 contained research articles that included their own sections on related literature. Chapter 2 is therefore an abridged version thereof. The main themes that were summarised included information security in general, behavioural information security, with a focus on the models and methods that are used in literature to evaluate information security behaviour, and behavioural threshold analysis. By establishing the literature review, the **first** secondary research question on the *current state of behavioural information security* was answered.

The **second** research sub-question on the *applicability of behavioural threshold analysis in the context of information security* was answered through pursuing **Objective 2** (*perform* initial assessment of generic approach) in Chapter 3, Article I by conducting an exploratory investigation and performing an initial assessment of the approach in this context. The journal article, *The application of behavioural thresholds to analyse collective behaviour in information security,* describes the process that was followed to apply the generic approach and reflect on the resulting evaluation. New opportunities were identified to improve upon the generic approach that informed the subsequent secondary research question.

Improving the generic behavioural threshold analysis approach was expressed as two research articles that answer the **third** research sub-question:

The first was a conference paper entitled *Optical polling for behavioural threshold analysis in information security* (Chapter 4, Article II) and was used to describe how the generic approach could be improved upon by changing the way in which data is collected. A new strategy, referred to as optical polling, was evaluated through its application in a case study. The positive

results helped determine best practices for data collection with respect to the unique requirements for behavioural threshold analysis in information security as per **Objective 3** (*determine* best practices for data collection).

The second, published as *I shall, we shall, and all others will: Paradoxical information security behaviour* (Chapter 5, Article III,), was concerned with **Objective 4** (*Apply* behavioural threshold analysis, *assess* organisation security group behaviour). The first application of behavioural threshold analysis in an industry setting was used to fine-tune the information security topics and the presentation thereof to respondents. The successful evaluation of the organisation's information security by means of the newly adapted approach indicated that it was now ready to be formalised.

The **fourth** of the secondary research questions envisaged e*stablishing behavioural threshold analysis as a novel approach for evaluating information security group behaviour.* This was done by addressing **Objective 5** (*Construct* and *validate* methodology). In Chapter 6, Article IV, the formalisation of the methodology under the title of *Behavioural threshold analysis: Methodological and practical considerations for applications in information security*, is described. It contributes to the existing body of knowledge by firstly *constructing* the novel measurement instrument that meets the specialised requirements that behavioural threshold analysis demands for its application in information security. Secondly, by *validating* the instrument through examining its performance by means of case studies, the rigour of the proposed approach is ratified. The methodology is the first of the *theoretical artefacts* as described in the *research design* in Chapter 1.

After the approach was established and formalised, the **fifth** research sub-question was answered through completing Objectives 5 and 6 to answer whether the approach could *successfully be applied in practical real-world contexts to assess information security group behaviour*.

Objective 6 (*Evaluate* the approach for other models, *substantiate* validity) is concerned with the robustness of information security behavioural threshold analysis when it is applied in contexts that differ from its original intention. In Chapter 7, Article V, investigates using behavioural threshold analysis to *evaluate* information cascades and sequential decision-making is investigated. This shows that the model is indeed robust enough for application in different contexts. This conference paper was entitled *Theorising on information cascades and sequential decision-making for analysing security behaviour*.

Given that the approach was proven to be applicable in different contexts, it was envisioned that behavioural threshold analysis could be used to *compare* the security behaviour of different groups. The book chapter, *Contextual factors in information security group behaviour: A comparison of two studies* (Chapter 8, Article VI), addresses **Objective 7** (*Compare* different industries). A comparison was made between industry workers and university students in terms of their contextual environments and their reported information security behaviour. These two investigations further served as evidence of the real-world applicability of the approach.

The **sixth** and final secondary research question relates to the practical contributions of this research. This is achieved by the *embodiment of the approach as a supporting tool to contribute to the theory of behavioural information security and the management of the human factor in practice*. Once more, there are two objectives (Objectives 8 and 9) that are used to answer this question.

The first of the two (**Objective 8**, *Contribute* a tool for information security management), *contributes* to the practice of behavioural information security through the creation of a *practical software artefact*. The established methodology was encapsulated in a decision support system that can be used to facilitate the application of information security behavioural threshold analysis by the management of an organisation. This decision support system was presented in Chapter 9 as Article VII. This published book chapter is entitled *A management decision support system for evaluating information security behaviour*.

The final objective (**Objective 9**, *Contribute* and *validate* and implementation framework) *contributes* to bridging the gap between research and practice. Article VIII presents a framework that provides guidance for the application of behavioural threshold analysis to evaluate real-world information security group behaviour in Chapter 10. The framework was validated through a combination of two qualitative evaluation methods, supported by evidence from the preceding peer-reviewed published results of this study. A journal article was accepted for publication under the title *Collective information security behaviour: A technology-driven framework*.

Through completing the research objectives and answering the research sub-questions, the primary aim of this study was realised and a definitive answer to the primary research question was provided. The contributions of this study are summarised in the following section.

11.3 Contributions of the study

The main contribution of this study is the development of a novel mechanism for evaluating information security group behaviour. This was achieved by adopting an approach from the field of sociology, which was previously not applied in the field of information security, and adapting it to the unique and specialised requirements for evaluating information security group behaviour. The approach is based on the theoretical underpinning of threshold models of collective behaviour, and its practical counterpart, behavioural threshold analysis. Furthermore, a behavioural model that is often used in information security research, *i.e.*, the theory of planned behaviour, was extended by using it to contextualise the threshold models of collective behaviour in terms of the extant information security behaviour approaches.

This new approach contributes to the management of the human factor in information security by applying behavioural threshold analysis to identify the current state of information security in an organisation and to predict eventual information security group behaviour. Organisational management can employ this newly established approach to identify information security problem areas in the organisation and, depending on the magnitude of the various problem areas and immediacy of the associated risks, determine where to focus corrective measures and interventions to address them. This typically involves using the information to tailor security awareness campaigns to specifically address the identified issues and the option to choose to limit the focus on non-essential topics to reduce instances of security fatigue. Following the abovementioned interventions, the approach can be used as a follow-up test to gauge the efficacy of the intervention by once more assessing the collective information security behaviour of the group.

During the development and establishment of the approach, new knowledge was contributed to the existing body of literature by publishing the findings and contributions in journals, conference proceedings, and book series. These contributions include:

- Contributing the first ever application of generic behavioural threshold analysis to evaluate information security group behaviour. This exploratory investigation confirms the suitability of the approach and contributed new avenues for exploration in this context. The approach was contextualised in terms of the prevailing behavioural models from literature;
- Identified novel data collection methods that provide for the specialised requirements for data collection of behavioural threshold analysis, as applied in information security. Optical polling was recognised as an approach to data collection that addresses issues such as survey fatigue, and social desirability that are commonly associated with self-reporting questionnaires and questions of a sensitive nature;

- Identified information security focus areas, *i.e.*, security topics, for applications of behavioural threshold analysis in information security and determining how these topics should be presented to obtain the best quality data from respondents.;
- Contributed a theorisation on the application of behavioural threshold analysis to assess information cascades and sequential decision-making in information security behaviour. It was shown that the approach is robust enough to evaluate information security group behaviour even if the underlying theoretical assumptions are different to that of the threshold models of collective behaviour; and
- Identified contextual factors that contribute to the formation of information security group behaviour by applying behavioural threshold analysis in different contextual settings, *i.e.,* a corporate environment and university residence setting.

The development of research artefacts contributed to both the literature (through publication), theory, and practice of the management of the human factor in information security. These contributions include three artefacts as follows:

- The first theoretical artefact proposes a formal methodology for the application of behavioural threshold analysis as a mechanism to evaluate information security group behaviour. This contributes to both the underlying theory and resulting practice. The methodology provides a point of departure for future researchers and practitioners who are interested in applying the approach in their specific settings by specifying guidelines for the construction of an appropriate measurement instrument and considerations for applications in practice.
- A practical artefact that comprises a software decision support system can be considered the penultimate contribution. This decision support system encapsulates the methodology and (partially) automates the process of applying behavioural threshold analysis in an information security setting. This contributes to the practice of behavioural information security by empowering (possibly lay) management to conduct evaluations of the information security behaviour in their organisations.
- The final contribution of this study is a theoretical artefact with practical implications. A framework was developed to facilitate the application of information security behavioural threshold analysis in practice. Practitioners, who are interested in applying the approach in organisations, can use this framework as a guide on how to do it successfully. The guidelines provide direction on identifying the relevant security topics, customising the measurement instrument, and the validation of the rigour of the results. Complementary to the framework, a novel contribution was made by synthesising an information security framework evaluation

method by combining two qualitative methods from literature. Future research can employ this method of evaluation to assess whether newly developed frameworks are fit for purpose.

11.4 Limitations and directions for future research

The articles that are presented in this thesis are organised in a coherent structure as presented in Figure 1.3 in Chapter 1. This structure relates to the research objectives and how the researcher sought to address these objectives through the research articles. Issues that were identified upon completion of one paper were addressed in the subsequent papers. This allows for concrete answers to the primary and secondary research. However, some remaining limitations and the opportunities they provide for future work are briefly stated below:

- The practical applications of behavioural threshold analysis were chiefly performed in two contextual settings, a corporate environment (workers at a utility company) and an academic environment (students living together in a university residence). Future studies could investigate information security group behaviour in other differentiated contexts.
- The theory of planned behaviour was used to contextualise behavioural threshold analysis in behavioural information security. Other behavioural models were also considered, but were not specifically applied in this context. Incorporating such other theories in future research, could provide previously unobserved insights into information security group behaviour dynamics.
- Behavioural threshold analysis is essentially an aggregation of the thresholds that are inherent to each individual in the group where it is applied. As such, it is expected that the big five personality traits (extraversion, agreeableness, openness, conscientiousness, neuroticism) might play a major role in personal thresholds when it comes to information security. This is an avenue of investigation that could be considered for future work.

11.5 Chapter summary

Chapter 11 is the final chapter of this thesis. A synopsis of the study was presented. In the synopsis, the research questions, aims and objectives were reiterated and how these were achieved was discussed. The chapter was concluded with the limitations of the study and the opportunities they present for future research directions were envisioned.

Appendix A – Group behaviour in cybersecurity (*Encyclopedia of Cryptography, Security and Privacy*)

The article presented in this appendix is the full version of the encyclopaedia article that was used to describe behavioural threshold analysis in Chapter 2.

Article for
Encyclopedia of Cryptography, Security and Privacy

Group Behavior in Cybersecurity

Dirk Snyman[1*], Hennie Kruger[2]
[1] North-West University
dirk.snyman@nwu.ac.za
[2] North-West University
hennie.kruger@nwu.ac.za
[*]Corresponding author

Synonyms

Lemming effect; herding behavior; collective behavior; information cascades.

Definition

Group behavior in cybersecurity, refers to the interaction between two or more individuals, where they are exposed to the cybersecurity behavior and actions of others. This mutual interaction influences the behavior of the members of the group, and ultimately the collective behavior of the group in terms of cybersecurity.

Background – Group behavior

The human aspect of cybersecurity is an ever-present occurrence that needs to be factored into cybersecurity policy and management strategies. The way an individual behaves in terms of cybersecurity, is based on determinants such as his/her motivations, convictions, and intentions. These determinants are the result of influences that affect the individual and originate from the environments in which (s)he functions. Behavior is, therefore, a product of the context in which it occurs. Typically, a person does not function solely in isolation with specific regards to their role within an organization. Much of the everyday existence is in the company of others, i.e. (s)he is part of a group. Given enough impetus between group members, the eventuality is that most members of the group will start to behave in a similar, if not the same, manner. This convergence of behavior is often referred to as the lemming effect or herding behavior which means that a person will follow the behavior of the group without much forethought, even against his/her own better judgment. This phenomenon of group behavior has been recognized as a prevailing human factor in cybersecurity.

Theory – Threshold models of collective behavior

The way group behavior is formed from the actions of the individuals that comprise the group may be understood by employing a theory on the formation of group behavior. Formally, the model is termed threshold models of collective behavior. This theory was developed by Granovetter (1978) in the field of Sociology. The premise of the theory is that the behavior of a person in a group setting is guided by an inborn threshold for participating in a specific behavior. Such a threshold refers to the proportion of other group members that must exhibit, or be believed to exhibit, the behavior, before the individual is stimulated to also perform the behavior.

When someone is confronted with two discrete behaviors with two distinct outcomes, usually participation or abstention, (s)he will unconsciously compare his/her own threshold level with the number of others they perceive as already performing the behavior. If the number of others that behave in a certain way

exceed their threshold for participation, (s)he will be swayed to join in the behavior. This process continues with each subsequent group member that also must make the binary, contrasting decision of partaking or not and participation will grow until the group (or at least a significant percentage) performs the behavior. This growth and the eventual group behavior can be modelled by applying behavioral threshold analysis (BTA), based on the description of Growney (1983).

Application – Example in cybersecurity

An illustrative example of the application of BTA, as applied in cybersecurity, is presented here. This example is intended to be instructive of the underlying methodology of analyzing cybersecurity group behavior (Snyman and Kruger 2019) and is presented here in a hypothetical setting.

Scenario – An organization has identified that password sharing among employees has become a noticeable problem which has to be addressed. To quantify the extent of password sharing, and the future extent thereof if no intervention is made, BTA is employed.

Behavioral threshold analysis – BTA aggregates the inherent thresholds that group-members have towards participating in cybersecurity group behavior. The thresholds (expressed as a percentage) for the individuals comprising the group is determined by means of a short measurement instrument (questionnaire) on password sharing (or other relevant cybersecurity behavior) that is distributed to all the group members. The measurement instrument is presented below in Table 1. Note the layout of the question and answer-grid; it is important to elicit effective and truthful thresholds.

Table 1. Example measurement instrument

Percentage of colleagues who share their passwords	How inclined would you be to also share your organization password, given the percentage of colleagues who share their passwords?			
	Never	Somewhat inclined	Strongly inclined	Always
0—10%	1	2	3	4
11—20%	1	2	3	4
21—30%	1	2	3	4
31—40%	1	2	3	4
41—50%	1	2	3	4
51—60%	1	2	3	4
61—70%	1	2	3	4
71—80%	1	2	3	4
81—90%	1	2	3	4
91—100%	1	2	3	4

Based on the responses that were received on the questionnaire, the resulting individual behavioral thresholds are aggregated by creating a cumulative threshold table. An illustrative example of a cumulative threshold table is presented in Table 2.

Table 2. Cumulative threshold table

Threshold (%)	Individuals with given threshold (%)	Individuals with a threshold not more than the given threshold (%)
0	0	0
10	4	4
20	10	14
30	15	29
40	20	49
50	12	61
60	10	71
70	15	86
80	4	90
90	0	90
100	0	90
Individuals with no threshold (i.e. will never participate) (%)	10	

Note the number of respondents with no reported threshold for participation. This happens when a respondent selects "Never" for all threshold intervals as per the measurement instrument (Table 1), i.e. no matter how many others perform a behavior, (s)he will not be persuaded to join in. Respondents with no threshold are excluded from further calculations.

The cumulative thresholds from Table 2 are then plotted in a behavioral threshold graph in contrast to an equilibrium line (a uniform distribution of cumulative thresholds such that $x = y$) as presented in Fig. 1.

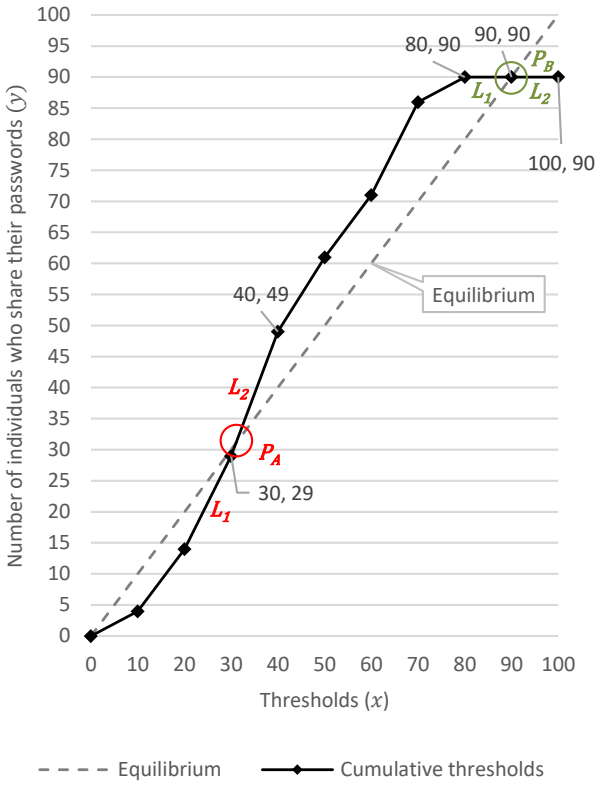


Fig. 1. Cumulative threshold graph

Results – The interpretation of a behavioral threshold graph is dependent on the intersection(s) (P_A and P_B) of the threshold graph with the equilibrium line. Each intersection of the two lines represents a possible equilibrium in which the group behavior stabilizes, i.e. the number of participants in the behavior does not continue to grow or decline. For an intersection to be an actual equilibrium, the line segments to the left (L_1) and right (L_2) of said intersection must have a gradient

$$m_{L_1}, m_{L_2} = \frac{\Delta y}{\Delta x} < 1.$$

This implies that only intersections where the threshold graph intersects the equilibrium line from above will satisfy the requirement as an intersection from below will always be

$$m > 1 \ for \ L_1,$$

e.g. Intersection P_A (as shown on in Fig. 1) does not satisfy the requirements for equilibrium. However, the behavior of password sharing among employees reaches equilibrium at P_B because

$$m_{L_1}, m_{L_2} = 0 < 1,$$

and the participation rate is said to be stable against both increase and decrease.

The relevance of the cumulative thresholds reaching a behavioral equilibrium to the cybersecurity behavior of password sharing, is that the equilibrium at point $P_B(90{,}90)$ indicates that the participation rate of password sharing is likely to increase until 90% of the employees are sharing their passwords. The group behavior will become stagnant at this ultimate participation rate unless an external stimulus (i.e. a cybersecurity awareness campaign) is utilized to change the behavior.

Discussion – A discussion on using BTA to analyze group behavior in cybersecurity, is presented here in terms of the advantages it presents and some challenges in its application.

Advantages – BTA considers the behavior of people in groups and not just the behavior of individuals in seclusion like most other behavioral theories; it may be employed as a preventative measure in cybersecurity management, i.e. current behavioral trends in troublesome security behavior may be identified, and forecasts may be made on future behavior to predict participation growth in the absence of targeted interventions; cost and time savings through tailored security awareness campaigns with a specific focus on behaviors which have been identified as imperative through BTA; the effectiveness of interventions may be gauged by means of the relative ease of repeatability of BTA as both a pre and post intervention assessment of group cybersecurity behavior.

Challenges – BTA requires that the members of the group have a working knowledge of the behavior of other group members and works best if performed in a relatively small group or organizational division. Also, the results cannot be extrapolated to a greater population and is only relevant to the surveyed group. Furthermore, the approach is sensitive to external contextual factors in a group setting which may influence its results.

Open problems and Future directions

Social desirability refers to a bias in self-reporting questionnaires where respondents report only behavior that place them in a good light or answer in a manner which they perceive as correct or expected rather than answering truthfully (Van de Mortel 2008). The success of cybersecurity BTA is dependent on the truthful reporting of thresholds by individuals in an organization. While attempts exist to address the management of this phenomenon and its influence on BTA (Snyman and Kruger 2019), it remains an open problem in the broader field of human aspects in cybersecurity.

Future research into respondent bias, such as social desirability, may provide new mechanisms to correct for such occurrences and limit its influence on the reliability of the results of BTA. New applications of BTA in different industries may help to further augment its robustness through fine-tuning the approach, as well as the underlying measurement instrument and new survey approaches.

Cross-References

Behavioral Security; Cybersecurity awareness; Information Security Culture; Psychology of Cybercrime

References

Granovetter M (1978) Threshold models of collective behavior. American Journal of Sociology. 83:1420-1443

Growney JS (1983) I will if you will: Individual thresholds and group behavior - Applications of algebra to group behavior. Modules in Undergraduate Mathematics and Its Applications - Tools for Teaching. COMAP Inc., Bedford, MA

Snyman DP, Kruger HA (2019) Behavioural threshold analysis: Methodological and practical considerations for applications in information security. Behaviour & Information Technology. 38:1-19

Van de Mortel TF (2008) Faking it: Social desirability response bias in self-report research. The Australian Journal of Advanced Nursing. 25:40-48

Appendix B – Behavioural thresholds in the context of information security (HAISA2016)

The article presented in this appendix is the original published conference paper of which the extension was presented in Chapter 3.

Proceedings of the Tenth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2016)

Behavioural Thresholds in the Context of Information Security

D.P. Snyman and H.A. Kruger

North-West University, Potchefstroom, South Africa
{dirk.snyman;hennie.kruger}@nwu.ac.za

Abstract

This research presents the exploratory application of behavioural threshold theory on group behaviour related to information security. Behavioural threshold analysis is presented as a possible tool for aiding the development of security awareness programs. Generic behavioural threshold analysis is presented and then applied in the domain of information security by collecting data on the behavioural thresholds of individuals in a group setting and how they influence each other when it comes to security behaviour. The results of behavioural threshold analysis are presented in order to illustrate the feasibility of the approach as an aid for the development of security awareness programs.

Keywords

Information Security; Human Behaviour; Behaviour Threshold Analysis; Security Culture; Information Security Awareness Programs

1. Introduction

On the terrain of information security research, one of the prevailing themes is that of the human factor. Humans have even been branded to be the weakest link in the fragile information security chain (Soomro *et al*., 2016; Tsohou *et al*., 2015; Yildirim *et al*., 2011). In fact, in a recent summative study of literature pertaining to information security management, Soomro *et al.* (2016) found the human factor to be one that is recurrently identified and researched and is often classified under themes like "human aspects in information security" (Safa *et al*., 2016), "information security awareness" (Tsohou *et al*. 2015), and "information security culture" (Dhillon *et al.*, 2016). The influence of this factor continues to have a far reaching impact on the security and integrity of computerised systems due to the inherent imperfections that humans exhibit when compared to technical layers of security (Richardson, 2010; 2008; Berger, 2012). People can be easily influenced by circumstances and they may divulge sensitive information (sometimes unwittingly, other times with specific intent) that could have a detrimental effect on the security and integrity of the systems with which they interact (Richardson, 2010). One way to deal with these shortcomings (in terms of information security) is to ensure that security awareness programs are implemented in organisations. The goal of such programs is to educate and instruct the members in an organisation about issues regarding information security and to influence their behaviour, or the reigning information security culture, in a positive manner (Tsohou *et al*., 2015). Information security culture is said to be the system of shared patterns or beliefs, in terms of

information security, held by members of an organisation. The security culture of an organisation is governed by a shared system of beliefs, influenced by the members of the organisation (Dhillon *et al*., 2016).

Having security awareness programs that function effectively is crucial in managing the information security culture of any organisation. Developing and employing these programs take time and effort which make them costly. Security awareness programs should therefore be tailored to fit the group to ensure that the programs succeed in their goal. The approach highlighted by Tsohou *et al*. (2015) would be to analyse the behaviour in the organisation through the lens of different behavioural models to determine the reason why the individual, and later the group, behaves in a certain way. The reasons for the way in which behaviour within an organisation is formed are not always overt, but according to Tsohou *et al*. (2015), behaviour of the individual and the group may be influenced by cognitive and cultural biases. These biases affect the way in which they (the organisation as individuals and as a group) adopt information security regulation and policies. By keeping these factors in mind, security awareness programs may be optimised.

Granovetter (1978) presents a behavioural model based on the premise that group behaviour is determined by the influence that individuals have on one another. Specifically how an individual reacts to the actions (or absence of actions) of others (see Section 2.2). This reaction is said to be based on an intrinsic threshold that an individual has to participate, given the number of others that already participate. This behavioural model may prove useful to assess security culture and determine how the individual and the group is influenced by peer behaviour (Herath and Rao, 2009). E.g. if high personal thresholds for an information security related topic (like password security) is noted, it would suggest that users are unlikely to be influenced by the behaviour of others. This would indicate that little focus on password security is warranted in a security awareness program. Conversely, if a low personal threshold is noted, users should be more likely to be influenced by the behaviour of others. Security awareness programs should therefore have its focus on the relevant topics in order to influence security behaviour in a positive way. This should contribute to the economics of security awareness by only including suitable topics in security awareness programs in order to limit the high cost (in terms of time and money) usually associated with the development of such programs. Furthermore, the modern user gets overloaded with security information and has become security fatigued (Furnell and Thompson, 2009) and by tailoring the content of security awareness programs security fatigue may be prevented in order to promote the effectiveness of security awareness programs.

With this in mind, this paper aims to perform an exploratory investigation into the feasibility of behavioural threshold analysis as a possible aid in developing the right (especially content-wise) security awareness programs for a given group or organisation. In order to achieve the abovementioned aim this paper is structured as follows: Section 2 describes literature from related work pertaining to security awareness programs, behavioural thresholds and instruments that can be used to analyse these thresholds. Section 3 demonstrates a typical behaviour threshold

analysis. Section 4 presents an illustrative example of threshold analysis with specific focus on its application in Information Security. Finally, Section 5 summarises the findings of this study and looks towards future directions for this research.

2. Literature review

This section shows cursory examples of the related literature, highlighting issues in security awareness programs, behavioural thresholds, and behavioural threshold analysis techniques.

2.1. Security awareness programs

Security awareness programs play an important part in managing the Information Security culture of an organisation (Tsohou *et al*., 2015). They convey information about the security policies and possible security threats within an organisation. They serve as a mechanism to educate users and create awareness about relevant security issues that face the organisation. It is usually assumed that the users within an organisation are prone to risky behaviour in terms of security because they are unaware that their behaviour is risky, and even when informed to the contrary they are unaware of the potential consequences of their actions. Tsohou *et al*. (2015) further state that even though there are guidelines and standards that govern the development of security awareness programs, they often fail because they fail to provide for the way in which users form ideas and opinions on a cognitive level. By not taking this into account these programs merely bombard the user with information that does not influence the security behaviour of users as it is supposed to do. This cursory overview is due to space limitations. For further reading on security awareness programs, including comprehensive literature surveys, see Safa and Von Solms (2016), Soomro *et al*. (2016), and Lebek *et al*. (2013).

2.2. Behavioural thresholds

Granovetter (1978) (and later Granovetter and Soong (1983)) argues that the preferences, norms or beliefs of an individual are seldom formed without the influence of the environment (especially the interaction with others) in which the individual finds himself. He further argues that these norms can change due to the influence of the behaviour of a group of people, even to such an extent that the behaviour of the individual can change to the exact opposite of said individual's prevailing norms. This phenomenon can occur even without direct confrontation of the individual by any member(s) of the group. This trigger of paradoxical behaviour may be attributed to be due to humans having an inherent threshold for the acceptance of, and participation in behaviour in a group setting. For instance when protesters gather to further a specific cause, emotions and convictions can cause the situation to be volatile. When a core individual or group starts acting violently the situation can easily escalate to a full blown riot. Suddenly all of the (once peaceful) protesters participate in acts of vandalism and the like. E.g. Person A is a peaceful protester and believes in peaceful resolution of differences, however he is willing to

commit to violence if at least a certain critical mass of others in the protest commits to violence. This phenomenon can be translated to an organisational setting where, for example, management want to implement a new information security policy and want to generate acceptance for the policy among the members of the organisation. They need only influence a critical mass of members and the others will follow in acceptance. Contrariwise when a certain critical mass of members deviate from the prescriptive policies, there could be a detrimental effect in the overall compliance as the remaining members will once again follow in example, but in a manner that is contraindicated.

A proposed model by Granovetter (1978) aims to analyse the inherent thresholds of the individuals that make up a group and predict the outcome of situations where a critical mass influences the remainder of individuals. This model is referred to as "Behavioural threshold analysis" and is based on circumstances where the actors (members of a group) only have two discrete and opposing avenues of pursuit. Usually choosing the behaviour in one direction has a supposed positive result and the other has a negative result. The analogy (as explained in above) of either participating in a riot or not participating, is used to emphasise these two opposing views but Granovetter (1978) argues that the model is applicable to any contrasting binary decision. See Granovetter, (1978) and Growney (1983) for further analogical situations.

The inherent personal cost vs. gain of committing to either of these choices is what determines the individual's threshold pertaining to participation or abstention. The perceived cost of participation differs for each individual that a group consists of. Some individuals require little to no motivation to participate in an activity and can be seen as instigators, while others need to be swayed to join in uncharacteristic activity due to the perceived gain outweighing the cost. Some perceive the cost as being infinitely high and will never join in.

The aim of this model is to describe the outcome of a situation given the collection and distribution of individuals (each with their own threshold) that are involved therein by predicting the number of individuals opting for each of the opposing behaviours. As mentioned in the Introduction (see Section 1), this model may be implemented as an aid in determining the content of security awareness programs by analysing the susceptibility of users to influence by others in terms of information security issues. Using this model as a barometer, only relevant information may be included in security awareness programs, possibly saving time and money. The following section describes the typical analysis of recorded thresholds based on the analysis as presented by Growney (1983).

3. Typical threshold analysis

Growney (1983) posits that in order to obtain the individual threshold values from a group a simple standard questionnaire can be employed. The individuals in a group are requested to truthfully respond to a set of questions about two discrete outcomes (see Section 2.2) of a situation in which the individuals as part of a group may find

themselves. The individuals (respondents) are asked to complete a value for *x* in 2(b) of Figure 1. The value quoted represents the inherent threshold for the individual in question.

Questionnaire

1. Choose one of the following outcomes that is preferable:
   a. Outcome A
   b. Outcome B
2. Regardless of the outcome selected above, respond to the following statements:
   a. I will never participate in Action A
   b. I will participate in Action A when at least *x* number/percent of group members choose to participate in Action A.

Figure 1: Threshold questionnaire (Growney, 1983)

After the responses are received from the respondents the responses can be tabulated and represented in a graph format. Threshold analysis (see Section 2.2) can then be performed on the observed values in order to predict the outcome of the behaviour of the group under observation. Observe the following set of cumulative thresholds (Table 1). These thresholds were obtained for an imaginary group of people in an imaginary setting as if they had completed a questionnaire like the one in Figure 1. Let the two mutually exclusive outcomes as mentioned earlier be Outcome A (negative) and Outcome B (positive). The thresholds tabulated in Table 1 represent an individual's threshold to participate in an action (Action A) that will lead to Outcome A. In other words: how many individuals have to perform Action A before the individual, whose threshold is being noted, will join in and also perform Action A. E.g. note the number of individuals with a given threshold of 20. These 15 individuals will be inclined to perform Action A when 20 or more people already participate. The cumulative frequencies (column 3) indicate that there are 30 people in total with the threshold of 20 or less which means that the 15 people with the threshold of 20 will join in Action A. The participating group will continue to grow as long as the thresholds in column 1 are exceeded by the cumulative frequencies in column 3. The complete behavioural threshold analysis is based on the comparison of all the individual behaviour thresholds - noted across the group in question - to a uniform distribution of thresholds said to be the equilibrium. A graphic representation of Table 1 is presented in Figure 2. Note: To simplify the analysis all values have been expressed as percentages and thresholds adjusted to intervals of 10 (Granovetter, 1978; Growney, 1983).

Thresholds	Number of individuals with given threshold	Cumulative frequencies of individuals with a threshold <= given threshold
0	0	0
10	15	15
20	15	30
30	10	40
40	30	50
50	10	80
60	0	90
70	0	90
80	0	90
90	0	90
100	0	90
No Threshold:	10	

Table 1: Threshold analysis (Growney, 1983)

With reference to Figure 2, when observing the threshold line segments to either the left or right of an intersection with the equilibrium line the gradients of these line segments describe the stability of the group's behaviour against deterioration (heading towards Outcome B) or escalation (heading towards Outcome A). When the line segment to the *left* of an equilibrium intersection has a gradient of less than one the equilibrium that has been reached is said to be stable against decrease (towards B) and a segment with a gradient of less than one to the *right*, stable against increase (towards A). If both conditions of line segment with gradients less than one is met, the equilibrium is said to be stable and the group will remain in its current state, otherwise there will be a movement towards one of the extreme outcomes (A vs. B). Upon inspection of the resulting graph (Figure 2) an upward trend with a positive gradient is identified up to the (60, 90) co-ordinates. Thereafter a gradient of 0 (horizontal line segments) is noted for the remainder of the graph. When an equilibrium is reached at the intersection (90, 90) the conditions for a stable equilibrium is reached and no further deterioration or escalation is possible. The following section will present an illustrative example to show how the principles of behavioural threshold analysis (as explained in Section 3) are applied in the context of information security.

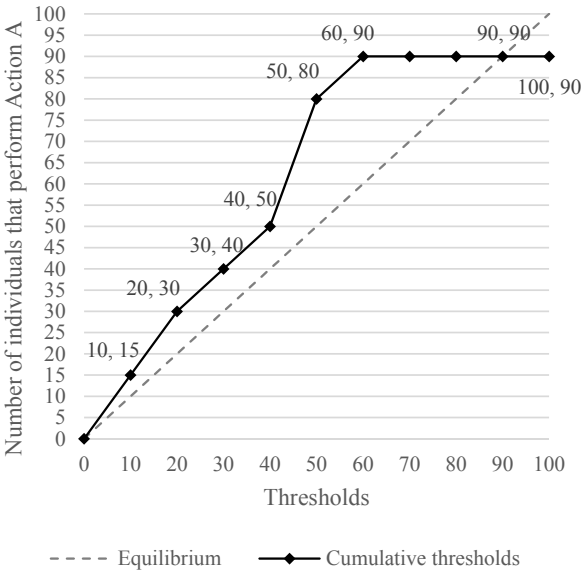


Figure 2: Threshold analysis example (Growney, 1983)

4. Illustrative example of threshold analysis in the context of Information Security

In order to meet the aim of this study (see Section 1) a threshold analysis is to be performed in terms of information security in order to gauge the effectiveness thereof as a tool for the development of security awareness programs. The example mentioned in this section is still in an exploratory phase. It was the very first experiment to test the behavioural threshold analysis concepts in the context of information security. The experiment was carried out with students as a test group and the initial results, which are used here only as an illustration, will be used to improve the security questions that are asked as well as refine the experimental process as a whole.

4.1. Data collection

The questionnaire that is used for data collection for this research was based on the questionnaire that is presented in Section 3. The questionnaire was supplemented with questions to determine basic demographic information such as gender, age etc. This questionnaire was distributed under a group of first year engineering students at a South African university. The questionnaire was hosted on Google Forms to facilitate the distribution of the questionnaire to the students and capture their responses. Out of a possible 70 students, 22 had responded resulting in a response rate of 31.4%. Of these 22 students 13 identified themselves as Male and 9 as

Female. An example of the questionnaire is presented below in Figure 3. The section of the questionnaire that contains questions about demographic information in not shown due to space considerations. Because of the exploratory nature of this research, it was opted to use a simple information security aspect for behavioural threshold analysis. Passwords were used as the basis for the questions as all students need to use passwords on a daily basis and should be familiar enough for them to relate to. Students were asked whether they would share their passwords if enough other students opt to do so and if so, how many students need to share their passwords before they also share their passwords.

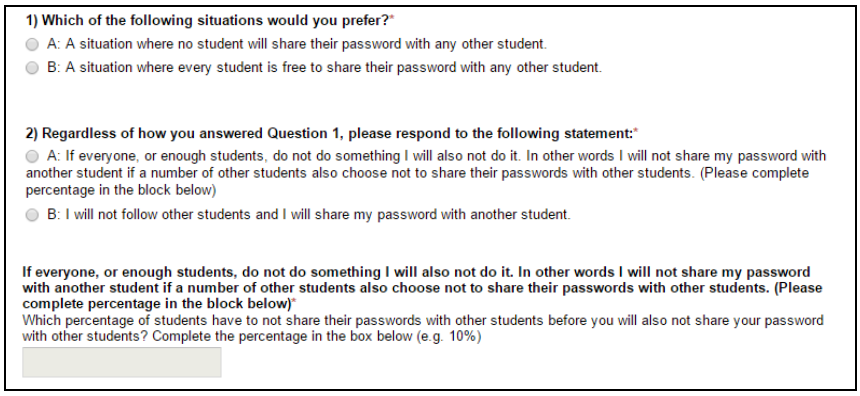


Figure 3: Behavioural threshold questionnaire

Initial pilot runs of this questionnaire proved troublesome with students being unsure of how to answer the questions relating to their password sharing behaviour, specifically question 2(A) as it was not clear to respondents that they needed to nominate a threshold value (as described in Section 2.2) resulting in a majority of unusable responses. This prompted a redesign of the presentation of the questions about their security behaviour. It is noted that the manner in which the questions are structured in this questionnaire (Figure 3) may seem reversed when compared to the example in Section 3 and that seen in literature. This is due to Growney (1983) proposing that issues with responses on the questionnaire, where the question was not understood by the respondents, may be solved by reversing the order in which the different outcomes are presented. This lead to interpretable results that can be displayed in an analogical manner of the way in which behaviour threshold analysis may be implemented in an information security behaviour setting. The questions on information security behaviour, specifically on passwords, still need to be re-evaluated and refined to ensure operability in a real-world analytical setting. The following section presents the results of the group behaviour threshold analysis for the above mentioned questionnaire.

4.2. Results

Figure 4 shows the results of the responses received from the questionnaire from Section 4.1. The resulting graph shows a positive gradient of up to the (10, 9.09)

coordinates where the graph intersects the equilibrium line. The line segment to the left of the intersection with the equilibrium line has a gradient of 0.454 (less than one), which indicates stability against decrease. The line segment to the right of the intersection with the equilibrium line has a gradient of 0 (less than one) which in turn indicates stability against increase. An equilibrium is reached at the intersection and the conditions for a stable equilibrium is met and no further deterioration or escalation is possible.

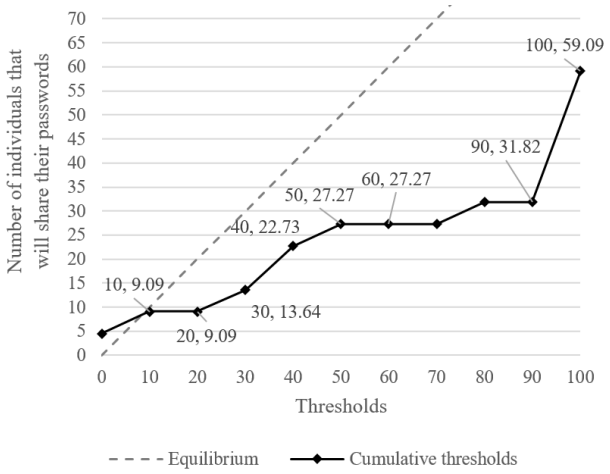


Figure 4: Results for threshold analysis

When this is interpreted in terms of information security and the questions posed in the questionnaire (whether students will share their passwords when other students also do it), there will be an increase in participation to the point where almost 10% of the students are influenced to join in and share their passwords with others. This number should remain stable as there is not enough momentum for this trend to catch on to the other students. This is due to the equilibrium being reached at a point where there are no more growth opportunities where the self-reported thresholds of the students are exceeded and students will not be influenced to join in. The stability in password sharing behaviour that is noted from the analysis may now be used to determine whether "passwords and password confidentiality" is a suitable subject to include in security awareness programs for this specific group. Depending on other considerations in information security that an organisation might have and need to address, they might decide that 10% of users sharing their passwords is a problem that needs addressing immediately (rather than any other current security matters) and opt to include password education in security awareness programs. Inversely, they may decide that other matters are more pressings than the sharing of passwords and because of the stability (i.e. the problem is not a growing one) they may opt to leave password education out of a security awareness program for possible inclusion a later date.

This initial analysis of security behaviour by using behavioural threshold analysis is still in its infancy, but shows promise as a tool for measurement, analysis and prediction of security behaviour and awareness. However there are still problems which would need to be addressed. The measurement instrument (questionnaire) still needs refinement in order to ensure the results obtained is representative of the security behaviour in the group. Respondents may be influenced by social desirability (Fisher, 1993) i.e. they identify one of the two responses as being the "correct" or "expected" one to choose rather than reporting on their true behaviour. The choice of what is to be measured should be investigated as passwords (which were chosen as the basis for the behavioural threshold questionnaire) may already be one aspect of information security that the respondents are too familiar with and may be security fatigued due to overexposure to awareness campaigns which taints their answers to the questionnaire.

5. Conclusion

This paper presents an original inquiry into the application of behavioural thresholds and group dynamics in analysing the human factor of information security. The initial experimental results show that behavioural threshold analysis is feasible in the context of information security and may provide useful guidelines on how to construct information security awareness programs. The threshold analysis method may contribute to security awareness in the following ways: 1) By helping to determine which security issues are easily susceptible to peer pressure or easily influenced by peer behaviour. If such topics can be identified it means that these are the topics that should be concentrated on in security awareness campaigns. 2) By identifying the key issues on which to concentrate in security awareness programs, the threshold analysis method may serve as a countermeasure against security fatigue. 3) Provide a positive contribution to the economics of security awareness, by helping to save time and money. 4) The threshold analysis method can be used later on, after interventions by means of security awareness campaigns, in a follow-up to track progress of security awareness levels. E.g. if 90% of users said they will follow others in doing something that is against Information Security policies, but in the follow-up only 10% say they will follow other and also do something against information security policies, an improvement can be noted. This improvement may indicate success in the security awareness programs. 5) Finally, the threshold analysis method gives a new way to measure the importance of security awareness issues in an organization.

6. References

Berger, U. (2012). CSI/FBI Computer Crime and Security Survey 2011-2012. CSI Computer Security Institute.

Dhillon, G., Syed, R., and Pedron, C. (2016). Interpreting Information Security culture: An organizational transformation case study. Computers and Security, 56, 63-69.

Fisher, R. J. (1993). Social desirability bias and the validity of indirect questioning. Journal of consumer research, 303-315.

Furnell, S., and Thomson, K. L. (2009). Recognising and addressing 'security fatigue'. Computer Fraud and Security, 2009(11), 7-11.

Granovetter, M. "Threshold models of collective behavior." American journal of sociology (1978): 1420-1443.

Granovetter, M., and Soong, R. (1983). Threshold models of diffusion and collective behaviour. Journal of Mathematical Sociology, 9(3), 165.

Growney, J. (1983). I will if you will: Individual thresholds and group behaviour. Applications of algebra to group behavior. Lexington, MA: COMAP, Inc. 108-137.

Herath, T., and Rao, H. R. (2009). Encouraging Information Security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., and Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. In 46th Hawaii International Conference on System Sciences (HICSS), 2978-2987.

Richardson, R. (2008). CSI computer crime and security survey. Computer Security Institute, 1, 1-30.

Richardson, R. (2011). 15th annual 2010/2011 computer crime and security survey. Computer Security Institute, 1-44.

Safa, N. S., and Von Solms, R. (2016). An information security knowledge sharing model in organizations. Computers in Human Behavior, 57, 442-451.

Safa, N. S., Von Solms, R., and Furnell, S. (2016). Information security policy compliance model in organizations. Computers and security, 56, 70-82.

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

Tsohou, A., Karyda, M., and Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of Information Security policies: Recommendations for Information Security awareness programs. Computers and Security, 52, 128-141.

Yildirim, E. Y., Akalp, G., Aytac, S., and Bayram, N. (2011). Factors influencing Information Security management in small-and medium-sized enterprises: A case study from Turkey. International Journal of Information Management, 31(4), 360-365.

Appendix C – The lemming effect in information security (HAISA2017)

The article presented in this appendix is the original published conference paper of which the extension was presented in Chapter 5.

Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

The Lemming Effect in Information Security

D.P. Snyman, H.A. Kruger, and W.D. Kearney

School for Computer Science and Information Systems, North-West University, Potchefstroom, South Africa
e-mail: {dirk.snyman; hennie.kruger}@nwu.ac.za; kearneys@iinet.net.au

Abstract

This research describes the first investigation of the lemming effect in information security by means of behavioural threshold analysis in practice. The analysis of group dynamic indicates that the lemming effect is indeed present in information security behaviour. The analysis thereof can be employed to assist companies in understanding the manner in which employees influence each other in their behaviour in terms of security. By identifying possible problem areas this approach can also assist in directing their information security education endeavours towards the most relevant topics.

Keywords

Information security; lemming effect; human behaviour; behaviour threshold analysis; group psychology.

1. Introduction

Human aspects of information security studies often aim to investigate the underlying behaviour of the end users that interact with information technology systems (Pham *et al.*, 2017). Quite often such studies look to the manner of interaction with information security, both in terms of individuals' actions and pre-suppositions (McCormac *et al.*, 2017), as well as overarching group dynamics and norms that influence and guide such interactions (Bauer and Bernroider, 2017). Concerning the latter, an interesting phenomenon is that of the so-called "lemming effect". The lemming effect refers to the propensity of individuals to follow the behaviour of a group blindly even when the behaviour is assuredly dangerous (Wiedermann *et al.*, 2014). The term is derived from the behaviour of lemmings (small rodents) that are purported in popular culture to follow migration behaviour of the group blindly, even walking off cliffs in droves only to fall to their deaths. In terms of information security, this would involve individuals following the group example in their information security behaviour.

Even though many previous studies exist that investigate information security behaviour (Crossler *et al.*, 2013; Warkentin *et al.*, 2011) and many behavioural theories (i.e., protection motivation theory, theory of planned behaviour, theory of reasoned action, etc.) have been developed that are often used as basis for these studies (Sommestad *et al.*, 2014), there still seems to be room for further exploration. For instance, Dang-Pham *et al.* (2017) argues that these previous studies mainly focus on individualistic cognition of employees and supply limited contextual

details. Furthermore, results and findings are also subject to the theoretical assumptions of the theories employed in the studies (Dang-Pham *et al.*, 2014).

Given the importance of information security and the apparent shortage on approaches that include contextual details, this paper reports a practical application to evaluate the lemming effect by including the context of co-workers instead of focusing on individual cognition on its own. The method that is used to study the lemming effect is based on the application of threshold models of collective behaviour (Granovetter, 1978) and was influenced by the theory of planned behaviour (Snyman and Kruger, 2017a). This method is applied to a large utility corporation in Australia.

The use of behavioural threshold analysis in information security has not been applied in practice before. This paper forms part of a larger research project where the feasibility of behavioural thresholds in information security is investigated. Snyman and Kruger (2016, 2017a) initiated the use of behavioural threshold analysis information security by testing the approach in their exploratory research. They presented the proof of concept as a feasible approach to information security behaviour analysis. This was succeeded by a study on effective data collection methods for threshold analysis (Snyman and Kruger, 2017b). These studies serve as the basis for this research and were used as iterations to refine the process and methodology of behavioural threshold analysis in information security. This current paper differs from the aforementioned initial exploratory research therein that this is the first report on the first practical application of behavioural threshold analysis in information security to be put into practice.

The remainder of the paper serves to describe the process and has the following structure: In Section 2 an introductory background on behavioural threshold analysis is presented. A description of the application of behavioural threshold analysis in information security, with specific reference to the methodology and experimental setup, is shown in Section 3. The results, which were obtained for the experiment described in Section 3, are presented in Section 4 and discussed in Section 5. Finally, Section 6 concludes this report and looks towards future directions for this research.

2. Behavioural threshold analysis

The concept of behavioural thresholds as well as threshold analysis will only be revisited briefly in this section to serve as background information as the concepts were already presented in detail in the previous papers. For a more in-depth review, see Snyman and Kruger (2016).

The foundational idea of behavioural thresholds as presented by Granovetter (1978) is that each individual in a group possesses an internal decision-making mechanism for following group behaviour. This mechanism weighs the personal cost versus gain of participation in the group behaviour, given the number of other group members that are already engaged in the behaviour. The mechanism expresses the willingness to participate as the number of other group members whom should already be

participating in the behaviour before the possible gains outweigh the cost for the individual. This is called the individual's behavioural threshold. When it is known to the individual that more group members are participating in the group behaviour than the number represented by their personal threshold, they will also participate in the group behaviour. This corresponds to the lemming effect that was mentioned in the Introduction. Granovetter (1978) explains the working of the mechanism using an analogy as follows: Within a group of workers in an organisation, a rumour might start circulating. An individual might pay little attention to the credibility of the rumour if it is heard from only one source. When more sources impart the same rumour to the individual, the rumour gains credibility because the number of sources is larger than before. The individual's internal mechanism then determines that if the credibility reaches a critical threshold, i.e. enough sources share the rumour; the individual will also believe and circulate the rumour. The individual's threshold has been exceeded and they will take part in the group action. Therefore, the individual has theoretically succumbed to the lemming effect. In the same way it is applicable to information security, e.g. if enough members of a group share their passwords with other members and the number exceeds an individual's threshold for participation, the individual will also share their password with others. To show the working of the model in action and illustrate the advantages thereof, the model was applied in practice and the following section presents the methodology that was followed.

3. Application of behavioural threshold analysis

The behavioural threshold analysis exercise was conducted with 63 respondents from a large utility corporation. From the existing structures at the corporation, three groupings of employees were identified, i.e. permanent staff, contractors, and management. Participation in this study was voluntary and the questionnaire had a specific consent section in line with acceptable practice. All information supplied by the respondents was strictly anonymous. Ethical clearance for the exercise was obtained from the human resources department and the CEO. Each respondent completed an online questionnaire on their willingness to perform certain information security actions, given the number of others whom also perform the actions.

The application of behavioural threshold analysis to analyse group behaviour in information security presents a unique challenge in terms of the measurement instruments used to gather the relevant behaviour data (Snyman and Kruger, 2017b). This is both in terms of the topics of information security questions that are posed to respondents and how these questions are presented typographically. For the purposes of this application, the following six questions were posed to the respondents (see Table 1).

Focus area	Information security behaviour threshold question
1. Security training	How inclined would you be to also complete voluntary information security training, given the percentage of staff that have completed voluntary information security training?
2. Social media use	How inclined would you be to also spend excessive work time on social media, given the percentage of staff that spend excessive work time on social media?
3. Incident reporting	How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?
4. Internet use	How inclined would you be to also access dubious websites from devices connected to your company network, given the percentage of staff that regularly access dubious websites from devices connected to your company network?
5. Email use	How inclined would you be to also open any unfamiliar email attachments, given the percentage of staff that normally open any unfamiliar email attachments?
6. Password management	How inclined would you be to also share passwords, given the percentage of staff that share their passwords?

Table 1: Information security questions for behavioural threshold analysis

The questions were based on focus areas and topics identified from the Human Aspects in Information Security Questionnaire (HAIS-Q) (Parsons *et al.*, 2017; Parsons *et al.*, 2014). The six focus areas that are shown are neither exclusive nor extensive, but serve to illustrate the suitability of a focus area and related question for behavioural threshold analysis. Depending on the intention of the specific behavioural threshold analysis exercise that is to be conducted, different suitable focus areas (for instance mobile computing) may be identified. For instance, the first focus area and related question in Table 1 is in contrast to the others as it describes positive behaviour, i.e. volunteering for information security training. This focus area and question was added as a control to test the willingness of the respondents to follow others in their behaviour if there was no negative connotation to performing the behaviour. Furthermore, the focus areas of the HAIS-Q are divided into questions that address different aspects of the themes. The *Password management* focus area has questions on "password sharing", "re-using passwords" and "strong passwords" (Parsons *et al.*, 2017). Depending on whether a study has an interest in these specific aspects, they may also be included. However, special attention should be given to the number of questions that are included as each question necessitates ten new responses. Owing to the number of responses, adding an extra question places a relatively higher burden on the respondent in comparison with traditional questionnaires. The number of questions is also contrasted to traditional approaches where multiple questions are employed to test a given aspect (Sekaran and Bougie, 2010). The nature of this model only allows for one question per aspect: *Will you participate if enough others do?*

Each of the questions from Table 1 was answered on a scale of inclination for participation in the specific information security activity, given the percentage of other group members that are known to partake in the activity. An example is presented in Table 2.

Percentage of staff that ignore security incidents by not reporting them.	How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?			
	Never	Somewhat inclined	Strongly inclined	Always
0—10%	1	2	3	4
11—20%	1	2	3	4
21—30%	1	2	3	4
31—40%	1	2	3	4
41—50%	1	2	3	4
51—60%	1	2	3	4
61—70%	1	2	3	4
71—80%	1	2	3	4
81—90%	1	2	3	4
91—100%	1	2	3	4

Table 2: Example of a complete behavioural threshold question

It should be noted that the sample size in this exercise does not follow traditional style for questionnaires which can be summarised as "the more the better". Due to the unique nature of behavioural threshold analysis, it is specifically done in smaller groups. The members of the group have to be aware of the habits and behaviour of others in order to answer the questions about their own thresholds (Growney, 1983). When sample sizes become too large (i.e. start to extend beyond the natural boundaries of organisational departments) the group members no longer have the awareness that is crucial for the correct application of the model and the probability of incorrect answers increases.

As mentioned earlier in Section 2, the threshold for an individual is the number (percentage) of others that have to exhibit a specific behaviour before they will join in. If a respondent indicated that they would be somewhat inclined to participate, given the percentage of the group that do so, that percentage was taken as their individual threshold. This was noted for each respondent and the aggregate of all the respondents' thresholds was used for the behavioural threshold analysis results (see Section 4).

In the earlier, related studies, it was noted that the results might have been affected by social desirability and was ascribed to the sensitive nature of the information security questions being asked as well as how familiar the respondents were with the topics (Snyman and Kruger, 2017a, 2017b, 2016). Social desirability refers to the tendency that many respondents have to answer questions in a manner that they think to be acceptable, rather than truthful (Fisher, 1993). It was therefore deemed necessary to control for this phenomenon to obtain a more accurate view on the predicted group behaviour. A series of additional questions were given to the respondents after completion of the behavioural threshold questionnaire to determine the level of social desirability that they exhibit. The questions to measure social desirability were based on a standardised 33-question measurement instrument, which was developed by Crowne and Marlowe (1964) and later shortened to eight questions by (Ray, 1984). These eight questions were used to measure social desirability in this research. They are presented in Table 3 below.

Social desirability questions
1. Are you always courteous, even to people who are disagreeable?
2. Are you always a good listener, no matter whom you are talking to?
3. Are you quick to admit making a mistake?
4. Have there been occasions when you took advantage of someone?
5. Do you sometimes try to get even rather than forgive and forget?
6. Do you sometimes feel resentful when you do not get your own way?
7. Are you always willing to admit when you make a mistake?
8. Have you sometimes taken unfair advantage of another person?

Table 3: Social desirability questions (Ray, 1984)

The social desirability questions are simply answered with Yes, No, or Unsure. Depending on the specific question either Yes or No will be awarded a score of one or three respectively. Unsure is always scored two. The scores for all of the questions is added together for a score out of a possible 24. The higher the score, the higher the likelihood is that the respondent's answers were influenced by social desirability. For the purposes of this study, only the extreme score of 24 is taken to mean that the respondent was not truthful in the way in which they answered the questions. If a respondent was deemed untruthful, their answers on the information security questions were adjusted towards a higher level of inclination for participation (see Table 2). The level of willingness for participation was adjusted one level higher, i.e. if a respondent with a social desirability of 24 selected their inclination of participation as *somewhat inclined (2)* it was adjusted to *strongly inclined (3)*. This would mean that the individual's threshold for participation is taken at a lower percentage in the cases where the behaviour is seen as a negative information security action. The reverse holds true for positive information security behaviours where the respondents might overstate their willingness for participation. In these cases, the threshold for participation is taken at a higher percentage. For all of the questions in this study, both the adapted and the original thresholds are taken into account in order to illustrate the effect of the adaptation.

The information security behavioural threshold analysis exercise was executed as explained above and following an analysis of the collected data, the results are presented in the following section.

4. Results

This section shows the aggregation of the information security behavioural threshold analysis results that were obtained from the respondents. Due to page restrictions, the results for all of the questions cannot be graphically presented and it was decided that only half of the results (i.e. three questions) will be presented in the behavioural threshold graph format, however, Section 5 presents a discussion of the results that were obtained for each remaining three questions.

The aforementioned graph format represents a plot of the cumulative behavioural thresholds for a corresponding question plotted against a uniform distribution of thresholds called the equilibrium line. The shape of the behavioural threshold graph and the intersection with the equilibrium line allows for an interpretation that may

predict a percentage of members of the group that may eventually participate in the relevant information security behaviour. It should be noted that a detail analysis of all the nuances conveyed by the graph is omitted due to page restrictions and only the crux of the analysis is presented. An overview of other measures and analyses (e.g. information conveyed by gradient measurement of the graph) is presented in (Snyman and Kruger, 2017a).

The results for the three questions that are presented in detail (namely questions 1, 3, and 6 from Table 1), were chosen due to their illustration of 1) the willingness of individuals to follow the positive information security behaviour of others; 2) a situation where the group appears to be unaware of the topic's security issues and individuals are easily influenced to follow the negative information security behaviour of others, in other words where individuals exhibit low thresholds for participation; and finally 3) a situation where the group seems to be sufficiently security aware and individuals should not be easily convinced to follow the bad information security behaviour of others, in other words where individuals exhibit high thresholds for participation. The results are presented one by one in this order.

1) Figure 1 shows the cumulative results for the groups' individual thresholds towards question 1 from Table 1 (hereafter referred to as Q1): *How inclined would you be to also complete voluntary information security training, given the percentage of staff that have completed voluntary information security training?*

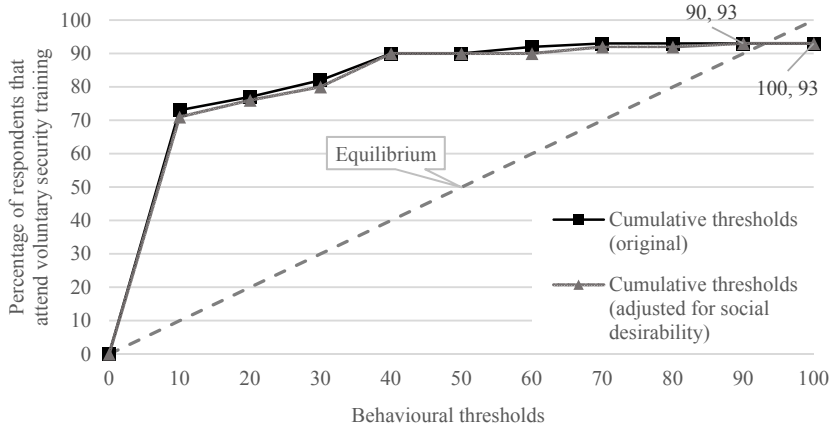


Figure 1: Distribution of behavioural thresholds for Q1

Q1 is an example of a positive influence that members of the group have on one another in the context of information security training. The steep incline and rapid growth in the cumulative behavioural thresholds indicates a *high* willingness (i.e. *low* thresholds) in the members of the group to follow the example of others to also participate in voluntary information security programs. The intersection with the equilibrium line indicates that if the status quo is sustained that the percentage of members that voluntarily participate in security training programs is likely to grow

until 93% of the group takes part. The situation is then unlikely to change as the distribution of thresholds reaches satiety at this point.

2) Figure 2 is a representation of the cumulative thresholds reported for question 3 (Q3) from Table 1: *How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them?* Q3 is an example where the influence of the group would be considered negative. Participation in the behaviour is not recommended as a good practice to promote high levels of information security. In contrast to the steep incline noted in Figure 1, the slower growth in the distribution of cumulative thresholds indicates that the members of the group are less willing than for Q1, but willing none the less, to follow example of others and participate in the group behaviour of not reporting security incidents.

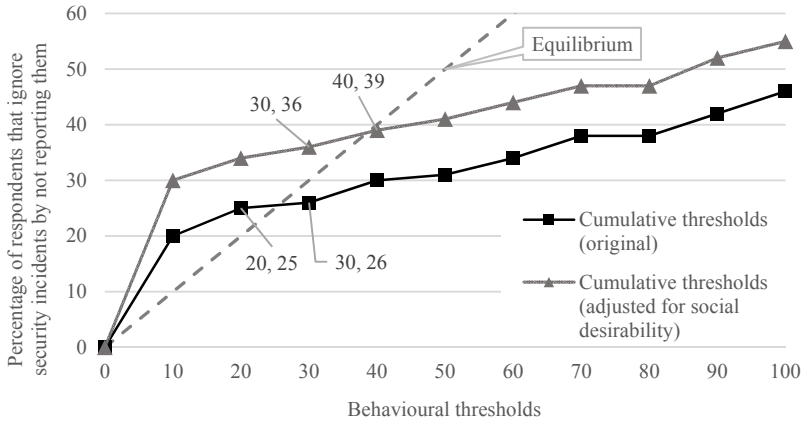


Figure 2: Distribution of behavioural thresholds for Q3

The intersection of the equilibrium line indicates that participation is likely to grow due to the *low* individual thresholds in the group. Participation stabilises with only 39% of the members of the group participating. This distribution of thresholds satisfies the requirements for equilibrium (Snyman and Kruger, 2017a) and the participation rate is unlikely to change unless there is some external influence, like an intervention, that changes the group dynamic.

3) To illustrate the aggregated thresholds for question 6 from Table 1 (Q6: *How inclined would you be to also share passwords, given the percentage of staff that share their passwords?*), Figure 3 is presented. Q6 denotes another example of a negative influence of group behaviour on the individual.

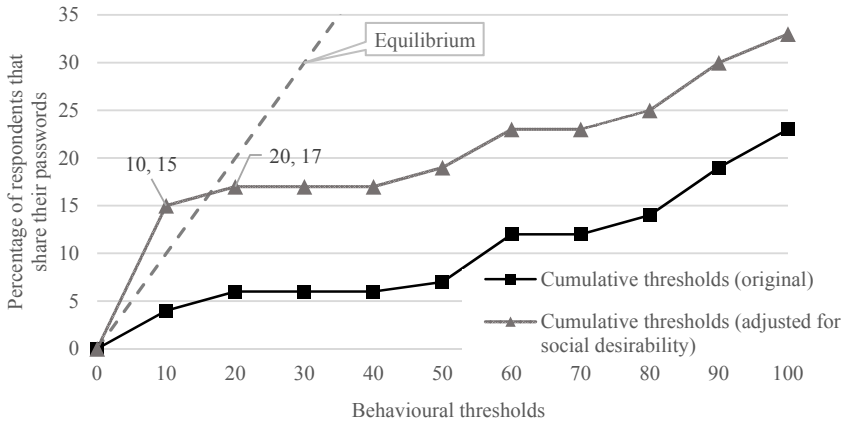


Figure 3: Distribution of behavioural thresholds for Q6

The results for Q6 indicate that the respondents are not willing to follow others in sharing their passwords. The group's unwillingness for participation is because the individual thresholds noted for this example are *high*. The distribution of the original behavioural thresholds never reaches an equilibrium and is indicative of a "dying" behaviour, i.e. no one in the group is likely to exhibit this behaviour. This is indicative of high levels of awareness about the topic conveyed by successful communication through security awareness programs. When the effects of social desirability are taken into account and the thresholds are adjusted, the threshold line intersects the equilibrium line with 17% of the group possibly sharing their passwords.

5. Discussion

Based on the results that are reported in Section 4, this section provides a twofold overview. A discussion is presented in terms of issues relating to this specific research exercise and then remarks of a more general nature relating to behavioural threshold analysis and the lemming effect.

5.1. Specific remarks

The group that was surveyed in this study is shown to be well versed in good information security behaviour. They furthermore exhibit a willingness to be team players in positive behaviour that promotes information security. In spite of the predominantly positive results, there are still some security topics where the lemming effect is observed. One example is the behaviour that was reported for Q3 (Figure 2) in the previous section. The lemming effect causes the individuals to follow group behaviour in not reporting security incidents.

Three questions were already discussed in Section 4, namely Q1 (*security training*), Q3 (*incident reporting*), and Q6 (*password management*). Once again, for space

considerations they are omitted in this instance. In the remaining questions that were posed to the respondents, they exhibited high levels of security awareness in terms of the information security aspects that the questions were based on. The analysis show generally positive results for two of the remaining three questions from Table 1, i.e. *internet use* (Q4), and *email use* (Q5) where the respondents showed *high* threshold levels. They will therefore not easily follow harmful group behaviour in these specific instances. This also points to high levels of security awareness (and good information security training) of staff for these two topics. However, for *social media use* (Q2), the recorded thresholds for participating in-group behaviour were noted to be *low* and individuals are therefore likely to follow the group in its bad behaviour. The topics of *social media use* and *security incidents* should therefore be reviewed by the corporation and reaffirmed through security awareness campaigns.

It was also interesting to note that the respondents exhibit high levels of social desirability. The average social desirability score for the participants was measured at 19/24. Such a high score indicates that there is a high probability that the respondents did not answer the questionnaire in a completely truthful manner. High social desirability might indicate that the respondents overstated their good information security behaviour and understated the negative behaviour that they would rather present in a better light. This can be attributed to the sensitive nature of the information security topics included in the questionnaire. The individual might also already be aware of expected behaviour and answers in accordance thereto.

Information security awareness programs serve to educate the members of an organisation of the potential information security threats. They also serve to promote good practices and identify practices that should be avoided. In the case of *social media use* and *incident reporting* it was observed that a percentage, 31% and 39% respectively, of the group is likely to be inclined to participate in negative information security practices. By including topics relevant to this behaviour in information security awareness programs, the percentage should see a decrease. It was shown that the group is willing to participate in such programs, even doing it voluntarily. This should contribute to the success of security awareness programs that are conducted in the corporation.

5.2. General remarks

The results show that the individual in a group is likely to follow the majority example in specific cases with reference to group information security behaviour. This indicated that the lemming effect is indeed present and, when analysed, can be useful to help evaluate group information security behaviour. Behavioural threshold analysis provides a formal measure to capture contextual information for an individual's security behaviour concerning the behaviour of co-workers. This context provides a broader view on information security behaviour than the traditional focus on individual cognisance. By measuring the lemming effect and predicting probable group behaviour, it provides a tool to identify possible risk areas. The identified risks can help focus the efforts of information security awareness programs.

Given the positive contributions of behavioural threshold analysis there are some points that still warrant careful consideration. Collecting data for behavioural threshold analysis poses a unique challenge to elicit useful answers from respondents. As mentioned earlier, the sensitive nature of information security questions often leads to high levels of social desirability. By tailoring the data collection instrument for this specific application the occurrence of social desirability can be somewhat addressed. Furthermore, the uniqueness of the instrument does not allow it to be tested for statistical validity and reliability as with traditional questionnaires. This is due to the specific manner in which the questions are structured to determine the respondent's behavioural threshold. The answers that the respondents provide may also vary to a large degree where they are often completely willing to follow the behaviour of others, or completely opposed to it. Another factor to keep in mind is the relative levels of influence that different members of the group have. An individual might be more inclined to follow the example of friends or prominent figures as opposed to just another employee they barely know.

6. Conclusion and future work

This paper presented the first application of information security behavioural threshold analysis to measure the lemming effect in practice. Given the number of factors that have an influence on this analysis the results should be handled carefully. Further research into these topics is warranted. Consideration might be given to other social theories that explain the influence of a group on an individual such as social capital theory and social cognition theory. The aforementioned notwithstanding, the results indicate the presence of the lemming effect in information security behaviour and that the effect can be measured with the use of behavioural threshold analysis as presented in this research. Furthermore, the results give a good indication of the levels of security awareness of the group in question and helps determine areas in which awareness still needs development.

7. References

Bauer, S. and Bernroider, E.W. (2017), "From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization", *Data Base for Advances in Information Systems,* Vol. 48, No. 3, pp. 1-24.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future Directions for Behavioral Information Security Research", *Computers & Security,* Vol. 32, No. 2013, pp. 90-101.

Crowne, D.P. and Marlowe, D. (1964), "The Approval Motive"*, Wiley*, *New York*.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2014), "Towards a Complete Understanding of Information Security Misbehaviours: A Proposal for Future Research with Social Network Approach", *Australasian Conference on Information Systems (ACIS)*.

Dang-Pham, D., Pittayachawan, S. and Bruno, V. (2017), "Applications of Social Network Analysis in Behavioural Information Security Research: Concepts and Empirical Analysis", *Computers & Security,* Vol. 68, No. 2017, pp. 1-15.

Fisher, R.J. (1993), "Social Desirability Bias and the Validity of Indirect Questioning", *Journal of Consumer Research,* Vol. 20, No. 2, pp. 303-315.

Granovetter, M. (1978), "Threshold Models of Collective Behavior", *American Journal of Sociology,* Vol. 83, No. 6, pp. 1420-1443.

Growney, J.S. (1983), "I Will If You Will: Individual Thresholds and Group Behavior - Applications of Algebra to Group Behavior", *Modules in Undergraduate Mathematics and Its Applications - Tools for Teaching,* Vol. No., pp. 108-137.

Mccormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017), "Individual Differences and Information Security Awareness", *Computers in Human Behavior,* Vol. 69, No. 2017, pp. 151-156.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., Mccormac, A. and Zwaans, T. (2017), "The Human Aspects of Information Security Questionnaire (Hais-Q): Two Further Validation Studies", *Computers & Security,* Vol. 66, No. 2017, pp. 40-51.

Parsons, K., Mccormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (Hais-Q)", *Computers & Security,* Vol. 42, No. 2014, pp. 165-176.

Pham, H., Brennan, L. and Richardson, J. (2017), "Review of Behavioural Theories in Security Compliance and Research Challenge", *Proceedings of the Informing Science and Information Technology Education Conference, Vietnam*, COHEN, E., ed., Santa Rosa, CA, USA, Informing Science Institute, pp. 65-76.

Ray, J.J. (1984), "The Reliability of Short Social Desirability Scales", *The Journal of Social Psychology,* Vol. 123, No. 1, pp. 133-134.

Sekaran, U. and Bougie, R. (2010), "Research Methods for Business: A Skill Building Approach"*, John Wiley & Sons*.

Snyman, D.P. and Kruger, H.A. (2016), "Behavioural Thresholds in the Context of Information Security", *Tenth International Symposium on Human Aspects of Information Security & Assurance*, CLARKE, N. L. & FURNELL, S. M., eds., Frankfurt, Germany, Plymouth University, pp. 22-32.

Snyman, D.P. and Kruger, H.A. (2017a), "The Application of Behavioural Thresholds to Analyse Collective Behaviour in Information Security", *Information & Computer Security,* Vol. 25, No. 2, pp. 152-164.

Snyman, D.P. and Kruger, H.A. (2017b), "Optical Polling for Behavioural Threshold Analysis in Information Security", *International Conference on Information and Knowledge Engineering (IKE'17)*, ARABNIA, H. R., DELIGIANNIDIS, L., HASHEMI, R. & TINETTI, F. G., eds., Las Vegas, USA, CSREA Press, pp. 39-45.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies", *Information Management & Computer Security,* Vol. 22, No. 1, pp. 42-75.

Warkentin, M., Johnston, A.C. and Shropshire, J. (2011), "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention", *European Journal of Information Systems,* Vol. 20, No. 3, pp. 267-284.

Wiedermann, W., Niggli, J. and Frick, U. (2014), "The Lemming-Effect: Harm Perception of Psychotropic Substances among Music Festival Visitors", *Health, Risk & Society,* Vol. 16, No. 4, pp. 323-338.

Appendix D – External contextual factors in information security behaviour (ICISSP2020)

The article presented in this appendix is the original published conference paper of which the extension was presented in Chapter 8.

External Contextual Factors in Information Security Behaviour

D. P. Snyman[a] and H. A. Kruger[b]
School of Computer Science and Information Systems, North-West University, 11 Hoffman Street, Potchefstroom, South Africa

Keywords: Information Security Behaviour, Contextual Factors, Human Factor in Information Security.

Abstract: Human behaviour is often considered to be irrational, difficult to understand, and challenging to manage. This phenomenon has a direct impact on the way in which humans behave when confronted with information security which, in turn, complicates how security is to be managed. This research attempts to investigate the role that contextual factors play in how humans behave, specifically with regards to information security. Contextual factors are identified that influence human behaviour in general. These factors are conceptualised in relation to existing models of behaviour and subsequently mapped to information security behaviour. A practical research exercise, relating to information security behaviour, is conducted with a university residence as the contextual environment. The specific contextual factors, and how they relate to information security, are discussed. Information security behavioural threshold analysis is employed to evaluate the impact of the identified contextual factors on the residence's security behaviour. The results are reflected upon, based on the results from the threshold analysis. The paper concludes by highlighting the contributions that were made towards understanding contextual factors in information security.

1 INTRODUCTION

The digitalisation of everyday activities is rapidly expanding to include even the most basic day-to-day interactions with people and (previously undigitized) systems (Scholl, 2018). This has given rise to an enhanced awareness and responsibility that regulators and governments have in providing frameworks that facilitate and prescribe the protection of the information and privacy of individuals, for instance, the General Data Protection Regulation in Europe. Similarly, organisations have a heightened responsibility and, given the regulatory frameworks, a level of accountability in safeguarding the information of customers and employees alike.

While these developments in information security enhancement are noble in concept, the actualisation thereof remains complicated. Even within the strict demands on organisations and their adherence thereto, one of the prevailing threats to the information security of the end-users remains the users themselves. One would argue that when individuals are given the opportunity to protect their privacy and information security interests they would do so with due consideration. However, this is rather the exception than the rule given the occurrence of phenomena like the privacy paradox, i.e. the wilful disclosure of one's private information, even when such disclosure is known to be ill-advised (Barth et al., 2019). This unpredictability of the human factor in information security remains difficult to understand and therefore difficult to manage. In an attempt to gain better insight into the reasons for inconsistent and often contradictory behaviour, information security and privacy research is often concerned with the underlying factors that drive behaviour when people are presented with the abovementioned digitised interactions (Scholl, 2018).

Among the different approaches to analyse information security behaviour, psychological models are often employed to explain the way in which the thought processes work that eventually lead to a specific behaviour or course of action. Most studies on human behaviour focus on the internal thought processes and motivations that inform intention and, eventually, the behaviour of a person. Some or other psychological theory or model of behaviour is usually employed as a guiding

[a] https://orcid.org/0000-0001-7360-3214
[b] https://orcid.org/0000-0001-8514-4422

Snyman, D. and Kruger, H.
External Contextual Factors in Information Security Behaviour.
DOI: 10.5220/0009142201850194
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 185-194
ISBN: 978-989-758-399-5
Copyright © 2020 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

framework for research in this field. A few of the more commonly used theories include knowledge, attitude, behaviour (KAB), the theory of reasoned action (TRA) (Shropshire et al., 2015), protection motivation theory (PMT) (Parsons et al., 2017), and the theory of planned behaviour (TPB) (Parsons et al., 2017). Such models are usually focussed on the intrinsic processes of an individual's cognition and rarely (if ever) consider the setting that an individual finds themselves in.

In contrast thereto, earlier work by Willison and Warkentin (Willison and Warkentin, 2013) postulates that understanding the mutual interaction of thought processes and organisational context is important to effectively employ information security controls in an organisation. This is confirmed by more recent literature (Kroenung and Eckhardt, 2015; Johnston et al., 2019; Wu et al., 2019) which has further identified that there is an ongoing need for approaches and methods that bridge the gap in information security research by both understanding the context of an individual and, where applicable, factoring contextual factors into any analysis that attempts to quantify information security behaviour.

In an attempt to contribute to filling the abovementioned gap, the aim of this research is therefore to 1) theorise on the external factors (i.e. external to an individual) that influence information security behaviour, and 2) to present the application of a model that takes context into account and predicts information security behaviour of a group.

The remainder of the paper is structured as follows: Section II describes factors that typically influence human behaviour, and thereafter Section III shows how these factors relate to information security behaviour. In Section IV, a cursory introduction into a model that considers contextual factors in information security behaviour is presented along with the findings of a real-world application thereof. The study concludes in Section V with a reflection on the study and a look ahead to possible future work.

2 CONTEXTUAL FACTORS IN HUMAN BEHAVIOUR

In the preceding Introduction, the need to conceptualize and understand the contextual factors that influence information security behaviour was highlighted. In order to eventually bring about a discussion of these factors in terms of information security, a discussion of contextual factors is first presented here in general terms, i.e. factors that influence everyday behaviour.

In a recent study, Kirova and Thanh (2019), based on the influential earlier work of Belk (1975), investigate the contextual factors that influence smartphone use. They identify five common aspects of all circumstances that can be used to identify the influences that are exerted upon an individual. These aspects are listed below:

- *Physical milieu;*
- *Social milieu;*
- *Perspective of elapsed (or remaining) time;*
- *Individual predisposition; and*
- *Individual intention.*

Even though these factors are all conceptualised as being contextual in nature and they all contribute to the experience and environment in which behaviour is to be actualised, for the purposes of this paper they may be classified as being either an intrinsic or an extrinsic factor, i.e. intrinsic or extrinsic to an individual. The contextual factors may be grouped as follows in Table 1.

Table 1: Categorisation of contextual factors in behaviour.

Contextual factors in behaviour	
Extrinsic factors	***Intrinsic factors***
Physical milieu	Perspective of elapsed (or remaining) time
Social milieu	Individual predisposition
	Individual intention

As mentioned before, when psychological theories and models are compared to the classification of the contextual factors in Table 1, one commonality may be identified. Many of these theories are centred around the intrinsic factors, e.g. individual predisposition (which relates to intention). Intention is one of the core indicators which guides behaviour in the TPB. The extrinsic factors are not explicitly provided for in these frameworks.

Given that intrinsic factors are already considered in these theories, this research focusses on the extrinsic factors and how they influence one's behaviour. A short description is provided below for each of the extrinsic factors from Table 1:

The *physical milieu* is an aspect that is derived from the tangible environment in which an individual finds themselves. This aspect considers the characteristics that define the physical experience that relate to what someone sees, feels (touch), hears, tastes, and smells.

Social milieu refers to the influence that other people have on an individual. They may be present in the environment (direct influence by example) or influence an individual through some other means like through digital interactions. An individual may either be formally acquainted with these influencers (e.g. friends, co-workers, or family) or be wholly unfamiliar (e.g. shop attendants or internet personalities).

Recall that the first aim of this paper is to theorise on external factors in information security behaviour. To satisfy this aim the aforementioned extrinsic contextual factors will be contextualised in terms of information security in the following section.

3 EXTERNAL CONTEXTUAL FACTORS IN INFORMATION SECURITY BEHAVIOUR

Two extrinsic contextual factors in behaviour have been identified in the previous section namely, *physical milieu*, and *social milieu*. In terms of information security behaviour, it is imperative to understand how these external factors manifest in the environments where security behaviour is performed. For instance, the physical milieu does not only relate to aspects that may be observed through one's senses, but also relates to aspects such as access to information, and convenience. Social milieu may also relate to aspects of interactions with others that are more intangible, e.g. body language, and peer pressure. Table 2 shows some typical material examples of the forms which these factors may adopt in relation to information security behaviour. These examples are presented here (and later in Table 3) as conceptualised by the authors based on characteristic information security behaviours and university residence environments, and how they might relate to the extrinsic factors as identified from the work of Kirova and Thanh (2019). The examples listed in this paper are by no means exhaustive and many more may exist.

In a related study, Snyman and Kruger (2017) investigate information security behaviour in terms of the TPB model. What differentiates their study from other studies that are based on the same model, is that the study speculates on the applicability of contextual influences on behaviour alongside the existing intrinsic factors that the model is based on. Such contextual influences are only described in theoretical terms and further investigation was left for future work. In an attempt to build on this initial groundwork, their approach, together with the two external contextual factors identified above, will be used to guide the practical part of this research.

To contextualise the TPB (as applied in (Snyman and Kruger, 2017)) with the current research presented in this paper, a graphical depiction is provided in Figure 1. Figure 1 shows a conceptual diagram of the interaction between the TPB and the external contextual factors. From the figure, it can be seen that the external (extrinsic) factors have an influence on the intrinsic factors. It is in the context of the intrinsic factors that the TPB then describes how attitude, norms and behavioural control guide the eventual behaviour of a person. Snyman and Kruger (2017) further argue that an approach that is able to implicitly capture information about external factors, and use this information in predicting eventual behaviour, are the so-called *Threshold models of collective behaviour* as envisioned by Granovetter (1978).

Table 2: General external factors that influence information security behaviour.

External factors in information security behaviour	
General extrinsic factor	***Example of extrinsic factor that influences security behaviour***
Physical milieu	Ease of access to systems, processes and people. Level of convenience associated with certain tasks. Availability of technical expertise. Presence of security controls.
Social milieu	Peer pressure Presence of co-workers/family/friends. Organisational structure. Required to work together with others. Collective purpose. Exposed to the actions/behaviours of others.

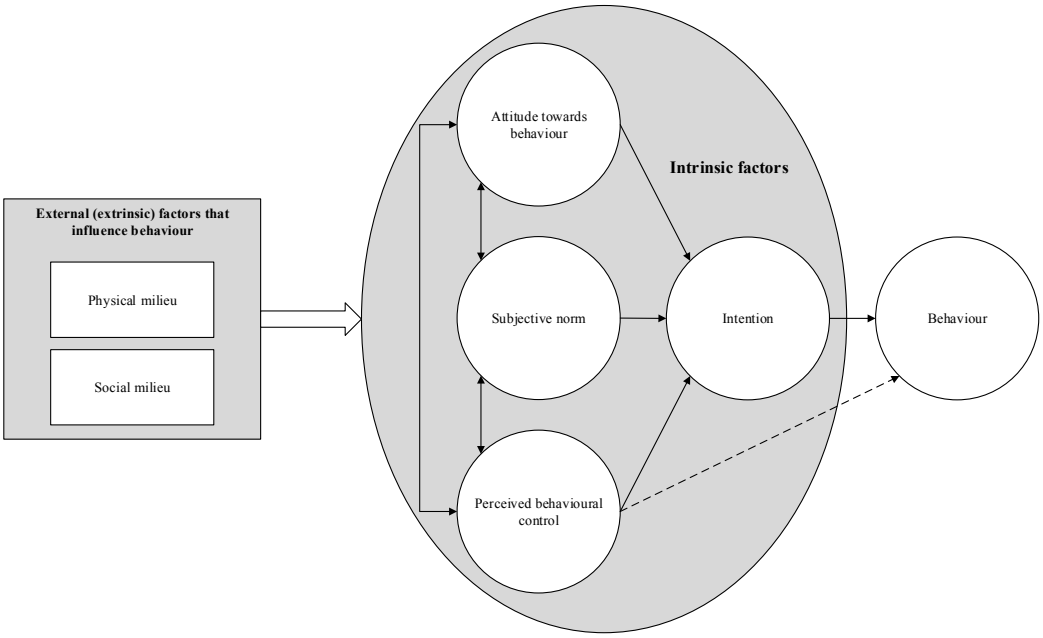


Figure 1: Conceptual model of the influence of contextual factors in relation to the TPB.

He argues, and mathematically motivates, that human behaviour is guided by the example that is set by others, i.e. an extrinsic factor. A person is presumed to always try and increase their utility within a given situation, guided by a perceived cost/benefit trade-off of participating in a certain behaviour, juxtaposed by choosing not to participate. The assumption is made that there are only two opposing options for the behaviour, i.e. no third (or additional) option(s) exists, and one must choose either of the outcomes that participation or abstinence convey.

People are assumed to be rational in their decision-making, always favouring benefit over cost. However, as the number of other people that perform a specific behaviour increases, a mental shift occurs that causes the perceived benefit to rise to a level that exceeds the perceived cost that is associated with the behaviour, even if the contrary was initially true. This pivotal point in the decision-making process may be described by an examination of the concept of behavioural thresholds.

Granovetter (1978) hypothesises that each individual has an intrinsic threshold for participation in behaviour. This threshold may be expressed as the number of other people that should first be engaging in a behaviour before the associated benefit will outweigh the cost in the individual's mind. At this point, it should be noted that when a person perceives the benefit to outweigh the cost from their perspective, without needing any external influence, that they will perform a behaviour of their own accord. Such individuals may be referred to as instigators. They are required, especially in a high-cost situation, to be the catalyst that influences others to follow their example.

In order to apply this theoretical model in a real-world situation, *behavioural threshold analysis* is employed. This analysis entails that the threshold values for participation in a behaviour is known for each of the group members and is dependent on, and specific to, the composition of individuals that constitute the group. The process by which these individual thresholds may be elicited from the group members by means of self-reporting questionnaires is presented in (Snyman and Kruger, 2019). Given the individual thresholds, mathematical aggregation is used to provide an outlook for the eventual group behaviour.

To relate the threshold model and analysis of Granovetter (1978) back to information security, a practical exercise was conducted which is described in the following section.

4 EXPERIMENTAL BACKGROUND

Taking inspiration from a similar exercise which was conducted in an industry setting (Snyman et al., 2018), a behavioural threshold analysis experiment was conducted to examine the information security behaviour of students at a predominantly residential South African university. The experiment was specifically designed with a new set of contextual factors in mind when compared to that of (Snyman et al., 2018). In contrast to the industry setting in (Snyman et al., 2018), the context of the university students is one of living together in a university residence. A description of these specific contextual factors, in reference to the general factors in Table 2, is given below in terms of the *physical milieu* and the *social milieu*.

Physical Milieu – A university residence, as mentioned above, physically consists of common areas (lounges, television rooms, kitchens, laundry rooms, public computer rooms, reception), as well as private sleeping quarters which houses one or two students per room. The close proximity of this kind of living arrangement provides the members of the residence with unprecedented access to the behaviour of others. Both in practical terms that allow the observation of the behaviour of others, and physical terms in which access is afforded to personal and university computers and networks.

A certain level of convenience is conveyed by living in close quarters. For instance, if network access is required after business hours and a person's credentials have expired, it is easy to simply ask any other inhabitant of the residence to supply their details. It is convenient for the borrower as their ability to access the network is instantly restored without the need to contact the help-desk which will not respond in real-time.

Given the combination of different academic levels and technical proficiencies that cohabit, it is probable that someone with a high level of know-how or expertise can readily be found to help circumvent security controls that stand in the way of quickly or conveniently completing a task.

An example of such a circumvention is accessing dubious websites that are restricted on the university network by means of masking their network traffic by employing virtual private networks to third party providers. In these cursory examples, one sees that the physical milieu provides means and opportunity to engage in risky information security behaviour. The social milieu, described below, may help provide the motive.

Social Milieu – University residences are a socially rich environment with a unique culture. This gives rise to many interactions between people that may influence how they behave. In information security terms, this influence may contribute to bad security behaviour in the following ways:

In a residence, there is a constant presence of other people. Even in a private space like sleeping quarters, there might be another resident present. This implies that some actions of an individual, that would normally go unnoticed, are being observed. If they visit a dubious website, someone may be there to observe it. When password sharing occurs between two parties it may be witnessed by any or all of the others present. Therefore, this constant presence may convey an unprecedented sense of awareness of the information security habits of the resident corps. The awareness may set the precedent for future behaviour.

Peer pressure is ever-present in university residences (Johnson et al., 2005; Young and de Klerk, 2008; de Klerk, 2013). A strict hierarchy prevails where a pecking order distinction is made based on the number of years someone has been residing in the specific residence. There is also a specific distinction between junior (usually first-year students or first-time entrants) and senior students. In this hierarchy, juniors have very little autonomy and, especially during an initial orientation, are forced to obey senior residents (de Klerk, 2013). The peer pressure and hierarchy that is present in residences are usually seen as factors in hazing (de Klerk, 2013) and alcohol consumption in literature (Johnson et al., 2005; Young and de Klerk, 2008) but is also applicable to security behaviour. A resident may easily be coerced, through this hierarchical structure and peer pressure, into divulging credentials, not reporting security circumventions, downloading illicit content, etc.

Even though the hierarchy may be seen in a negative light as illustrated above, it may also contribute to a sense of belonging and camaraderie (de Klerk, 2013). There is an implied level of trust associated with shared experiences. This is compounded by the compulsory attendance of events (Johnson et al., 2005; de Klerk, 2013) that are meant to reaffirm the bond between the residents. This trust allows for a false sense of safety where security is concerned. For instance, one might not appropriately scrutinise an email that was (presumably) sent by a confidant and assume it to be safe. The assumption will leave one open to malware and phishing attacks. Extending Table 2, Table 3 summarises the extrinsic factors (as described in Section II) that relate to the context of students living together in a residence.

Table 3: External factors in student residence living that influence information security behaviour.

External factors in information security behaviour		
Extrinsic factor	***Factors in general security behaviour***	***Factors in student security behaviour***
Physical milieu	Ease of access to systems, processes and people. Level of convenience associated with certain tasks. Availability of, and access to expertise. Presence of security controls.	Close quarters living provides access and convenience. Dissemination of security control workarounds from observation and readily available expertise.
Social milieu	Peer pressure from others. Constant presence of co-workers/family/friends. Hierarchy of persons in an organisation. Required to work together with others. Sense of collective purpose. Exposed to the actions/behaviours of others.	Peer pressure, often hierarchy based, from more senior and other residents to disclose private information, e.g. network credentials. Constant presence of other residents, even in private quarters. Security behaviours may be easily observed. Implied trust due to camaraderie and shared experiences (based on compulsory attendance of events) leads to false sense of safety and security.

Information security behavioural threshold analysis from (Snyman and Kruger, 2019) was subsequently implemented in the specific context as described above. For a detail description on behavioural threshold analysis in general terms, the reader is referred to (Granovetter, 1978) as only a brief overview is presented here due to page restriction considerations.

The threshold questionnaires were digitally distributed to 186 residents at a single-sex (male) university residence. Participation was voluntary and all responses were anonymous. Due to the relatively sensitive nature of questions that relate to personal information security behaviour, along with participation not being compulsory, suitable responses were obtained from 52 respondents resulting in a 28% response rate.

The questionnaire consisted of five questions relating to information security behaviours. To cover a range of common information security themes, selected focus areas of the Human Aspects of Information Security Questionnaire (HAISQ) were employed as the topics for the questions (Parsons et al., 2017). The five questions related to *password management*, *incident reporting*, *social media use*, *internet use*, and *email use*.

A four-point Likert scale was used for the question responses. The respondents rate their predisposition for participating in the security behaviour, relative to the percentage of other group members that perform the behaviour (Snyman and Kruger, 2019). This predisposition for participation is used as the behavioural threshold for the respondent. Responses from all the respondents were mathematically aggregated and analysed.

In addition to the questions above that relate to information security, the questionnaire was supplemented with questions relating to biographic information as summarised above. Moreover, the respondents were asked to rank their own confidence (five-point Likert scale) in the use of technology (in broad terms), and more specifically, their confidence in respect to information security.

Of these 52 respondents, 17 were self-identified as first-years (typically 19 years old), 15 as second years (20 years old), 13 as third years (21 years old), and 7 as being fourth-year and above (22 years old and over). Additionally, 7 academic faculties were represented in the responses namely, Faculties of Education, Engineering, Natural sciences, Economics, Health sciences, Humanities, and Law. The distribution of responses per faculty is presented in Figure 2 below.

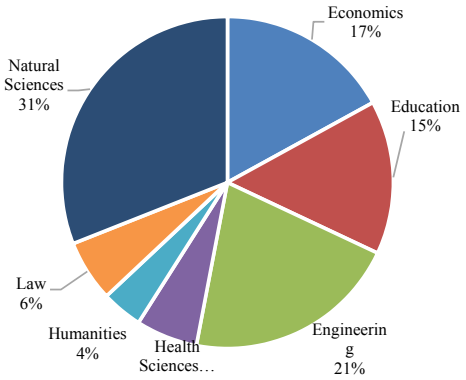


Figure 2: Distribution of responses per faculty.

The relatively low response rate and the possible influence of phenomena such as selection bias notwithstanding, the distribution between four year-groups and seven faculties were considered to be representative enough to allow for the useful application of information security behavioural threshold analysis (Snyman and Kruger, 2019). Thus, no attempt was made to address the possible selection bias in this specific context but may be investigated as a possible extension of this study in future work.

In the following section, a reflection is provided on the aforementioned contextual factors and how they are echoed in the behavioural threshold analysis results.

5 RESULTS AND DISCUSSION

To interpret the behavioural thresholds that were reported by the respondents, the thresholds are aggregated by calculating the cumulative frequencies for each threshold interval. In order to simplify the analysis, behavioural thresholds are grouped into intervals of 10%. These frequencies are then graphed as a line of participation level (y) versus cumulative behavioural thresholds (x). Furthermore, Granovetter (1978) stipulates that the cumulative frequencies of the respondents' behavioural thresholds should be graphed in relation to a uniform distribution of thresholds. This uniform distribution is referred to as the *equilibrium line* and is represented by the $x = y$ line. The intersection (if present) of the two lines may indicate that the group behaviour has reached an equilibrium point, i.e. the number of participants in the behaviour has stabilised. Behaviour that has reached equilibrium will not gain any new participants but neither will any participants desist from their current behaviour.

Once again, due to the page limit, only one of the abovementioned security topics (i.e. *internet use*) can be shown here. Figure 3 shows the behavioural threshold analysis graph for internet use for all the respondents that live in the residence.

Given an initial stimulus like an instigator that sparks the initial participation in a behaviour, the number of people that exhibit the behaviour will most likely grow.

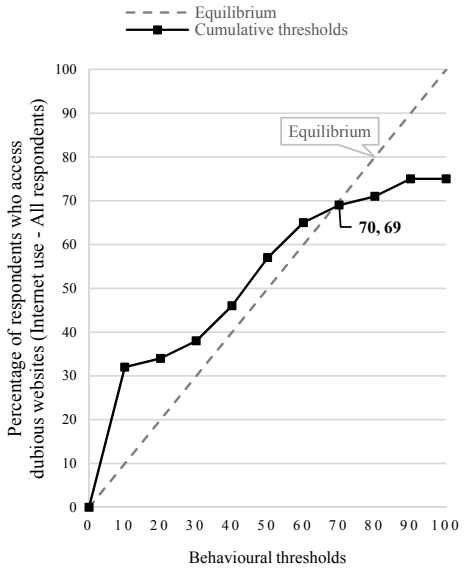


Figure 3: Behavioural threshold analysis graph – Internet use (All respondents).

From Figure 3, participation in inadvisable behaviour, relating to *internet use*, is predicted to increase to a level where 69% of the inhabitants of the residence will be performing the unwanted behaviour if 70% of the group are already performing (or thought to be performing) the behaviour. It should be noted that the 70% do not actually have to exhibit the behaviour. The mere perception that a number of others are performing the behaviour is enough to exceed the individual thresholds.

The number of residents that partake in the behaviour stabilises at this point. This can be deduced from the intersection of the cumulative threshold line with the equilibrium line at the point $(70, 69)$. Granovetter (1978) states that the requirement for equilibrium is that the two line segments to the left and right of the intersection have gradients $(m = \Delta y/\Delta x)$ of less than one.

This implies that an equilibrium state requires the threshold line to intersect the equilibrium line from above. An intersection from below does not constitute an equilibrium state, i.e. the gradient is greater than one. When $m < 1$ to the left of the intersection, the number of participants will not decrease in and of itself. An external influence or stimulus (e.g. information security training or awareness campaigns) is required to reduce the participation rate. In the same manner, to the right of the intersection, the number of participants will not increase.

When relating the participation in *internet use* to the two external contextual factors that were mentioned earlier, i.e. *physical* and *social* factors, the influence thereof becomes apparent. The participation rate of 69% indicates that the respondents, who all live in the residence, are quite willing to follow the example of their fellow residents. Their behavioural thresholds are *low*, i.e. it takes little motivation or the perception that only a few others already perform the behaviour, for them to also perform the behaviour.

On the *physical* level, this may be attributed to the access that the respondents have to technologically knowledgeable peers. An example scenario can include that institutions often employ firewalls and other network tools to prohibit access to websites and other network protocols they deem to be dubious in terms of security or questionable in terms of the content they provide (Miller and Stuart Wells, 2007). Examples of these types of websites include, among others, so-called torrent sites which provide unpaid access to copyrighted materials via peer-to-peer networks. Illegally downloading these materials are a frequent occurrence in tertiary institutions (Gan and Koh, 2006; Lee et al., 2019). Residences provide the ideal environment where these restrictions may be circumvented by a knowledgeable person and the method of access disseminated to others.

The *social factor* then determines how dissemination might take place: The required awareness that such circumventions are possible is created through constant presence and observation.

The person that originally exploited the circumvention is then either coerced to help others bypass the existing security (through peer pressure or levels of hierarchy) or might provide others with the solution willingly because of a sense of solidarity and collective purpose. These factors are therefore reflected in the willingness of 69% of the respondents for accessing dubious websites, given that a critical number of others in the residence already do it.

As mentioned before, the graph in Figure 3 is representative of the predicted behaviour for the entire surveyed group. A question that asks respondents to identify the number of years that they have been living in the residence was added to the questionnaire beforehand which allows one to drill down and identify behaviour for sub-groupings within the greater group. A finer-grained approach allows for a more comprehensive analysis. This allows for pinpointing where different groupings are persuaded to follow security behaviour differently. To illustrate this difference, the same *internet use* example which was presented for all the respondents in Figure 3, is now presented for a smaller grouping in Figure 4, i.e. first-year residents.

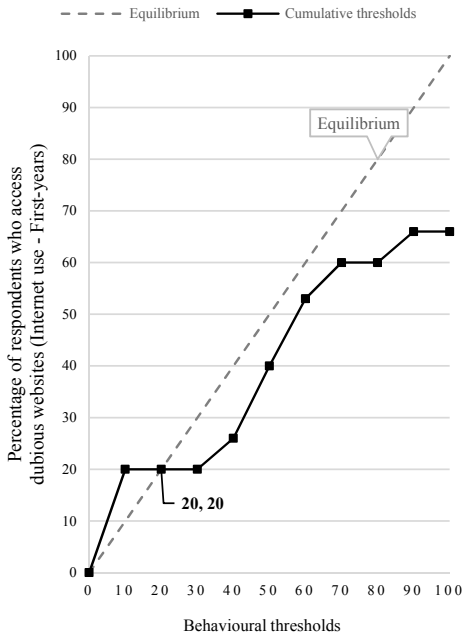


Figure 4: Behavioural threshold analysis graph – Internet use (First-years).

Following the same analysis as described above, it is interesting to see that the predicted participation rate for adopting unwanted *internet use* behaviour for first-years (20%) is considerably lower than that of the greater group at 69%.

This implies that the first-years' thresholds for participation is *higher* in comparison with the greater group. They are therefore less likely to be influenced in participating in the undesirable security behaviour.

In this research, the self-assigned grouping classification of *first-year* is taken to indicate that the respondent has entered the residence for the first time

at the start of the current academic year. This means that, by the time of distributing the questionnaires to the residents, first-years would only have been staying in the residence between one to two months. It stands to reason that the limited time that they were functioning in this environment would mean that the *physical* and *social* factors would not have been experienced as strongly as the other groupings who have typically been living in the residence for at least more than a year.

The concept of access to expertise, as a *physical factor*, only works if there is a certain rapport that exists between the parties. A first-year might not (yet) have the required level of acquaintance or hierarchical standing (*social factor*) that affords this access. Furthermore, first-years do not necessarily have a sense of camaraderie with the senior students in the residence. There have not been enough shared experiences in their frames of reference, but this shared reference does exist between first-years as they have undergone the same orientation period when first joining the residence.

In the final section, the study is summarised. The aims of the study are revisited, and a reflection is provided on the contributions and limitations of this research. A look ahead to possible future work concludes the article.

6 CONCLUSION

In this paper, an investigation was conducted into contextual factors that might influence information security behaviour. Section II described contextual factors that might influence human behaviour. Section III related these contextual factors to information security behaviour. Behavioural threshold analysis, which might consider contextual factors in information security behaviour, was presented in Section IV and selected findings of an application thereof were highlighted.

In Section 1 the original aims of this research were presented and are therefore reflected upon here. These aims are reiterated here and are subsequently discussed. This study aimed to 1) theorise on the external factors (i.e. external to an individual) that influence information security behaviour, and 2) to present the application of a model (behavioural threshold analysis) that takes context into account and predicts information security behaviour of a group. These two aims were addressed as follows:

External contextual factors in information security behaviour - Five contextual factors in human behaviour were identified from literature. The contribution of this research lies therein that these contextual factors were grouped into two categories, i.e. intrinsic factors and extrinsic factors. These categories were then incorporated into a conceptual framework relating to the Theory of Planned Behaviour. Guided by this framework, the external factors were linked with information security behaviour in general. It was then motivated that the Threshold Models of Collective Behaviour and Behavioural Threshold Analysis could be applied to measure security behaviour, given the influences of the external contextual factors.

Information security behavioural threshold analysis – In order to apply the aforementioned behavioural threshold analysis, a research exercise was conducted by distributing questionnaires on group security behaviour at a university residence. This research contributes by using this specific contextual environment to explain what form the two external factors that influence behaviour might take on in terms of security behaviour within a university residence. The results of the behavioural threshold analysis were used to illustrate how the group (and a sub-group) might eventually follow unwanted security behaviour. Lastly, the two external contextual factors were once again discussed with reference to the outcomes of the exercise and how these factors might differ between the main group and the sub-group.

The aims, as reflected upon above, were met amidst certain limitations which should be noted and considered when the findings are interpreted: The study was conducted at one single-sex residence. This means that there is no corroborating evidence, of the influence that these specific external factors have on information security behaviour, from other residences. Furthermore, only the two external contextual factors, i.e. physical and social, were incorporated in the analysis.

These limitations notwithstanding, this research demonstrates that contextual factors (with specific reference to extrinsic factors) play an important role in information security behaviour. These factors may be analysed by employing models such as behavioural threshold analysis. Such an analysis may provide a useful understanding of the human aspect of information security, and related behaviours, in an organisation. Better insight into these factors can contribute to more effective management of the human factor by guiding information security training programs to address specific, rather than generic, security behaviours.

Finally, future studies may consider studying how the intrinsic factors (even though they are

conceptually part of the TPB) are reflected in the behavioural threshold analysis model.

ACKNOWLEDGEMENTS

The authors would like to thank Mr Johan Allers for his assistance in distributing the questionnaire.

REFERENCES

Barth, S., De Jong, M. D., Junger, M., Hartel, P. H. & Roppelt, J. C. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics,* 41, 55-69.

Belk, R. W. 1975. Situational variables and consumer behavior. *Journal of Consumer research,* 2, 157-164.

de Klerk, V. 2013. Initiation, hazing or orientation? A case study at a South African university. *International Research in Education,* 1, 86-100.

Gan, L. L. & Koh, H. C. 2006. An empirical study of software piracy among tertiary institutions in Singapore. *Information & Management,* 43, 640-649.

Granovetter, M. 1978. Threshold models of collective behavior. *American Journal of Sociology,* 83, 1420-1443.

Johnson, A. M., Rodger, S. C., Harris, J. A., Edmunds, L. A. & Wakabayashi, P. 2005. Predictors of alcohol consumption in university residences. *Journal of Alcohol and Drug Education,* 49, 9.

Johnston, A. C., Di Gangi, P. M., Howard, J. & Worrell, J. 2019. It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups. *Journal of the Association for Information Systems,* 20, 186-212.

Kirova, V. & Thanh, T. V. 2019. Smartphone use during the leisure theme park visit experience: The role of contextual factors. *Information & Management,* 56, 742-753.

Kroenung, J. & Eckhardt, A. 2015. The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship. *Information & Management,* 52, 611-627.

Lee, B., Fenoff, R. & Paek, S. Y. 2019. Correlates of participation in e-book piracy on campus. *The Journal of Academic Librarianship,* 45, 299-304.

Miller, C. & Stuart Wells, F. 2007. Balancing security and privacy in the digital workplace. *Journal of Change Management,* 7, 315-328.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. & Zwaans, T. 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security,* 66, 40-51.

Scholl, M. 2018. Awareness in Information Security. *Systemics, Cybernetics and Informatics,* 16, 80-89.

Shropshire, J., Warkentin, M. & Sharma, S. 2015. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security,* 49, 177-191.

Snyman, D. P. & Kruger, H. A. 2017. The application of behavioural thresholds to analyse collective behaviour in information security. *Information & Computer Security,* 25, 152-164.

Snyman, D. P. & Kruger, H. A. 2019. Behavioural threshold analysis: Methodological and practical considerations for applications in information security. *Behaviour & Information Technology,* 38, 1-19.

Snyman, D. P., Kruger, H. A. & Kearney, W. D. 2018. I shall, we shall, and all others will: Paradoxical Information Security Behaviour. *Information & Computer Security,* 26, 290-305.

Willison, R. & Warkentin, M. 2013. Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly,* 37, 1-20.

Wu, P. F., Vitak, J. & Zimmer, M. T. 2019. A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, 1-6.

Young, C. & de Klerk, V. 2008. Patterns of alcohol use on a South African university campus: The findings of two annual drinking surveys. *African Journal of Drug and Alcohol Studies,* 7, 101-112.

Appendix E – Behavioural threshold analysis in practice: An implementation framework (HAISA2020)

The article presented in this appendix is the original published conference paper of which the extension was presented in Chapter 10.

Information Security Behavioural Threshold Analysis in Practice: An Implementation Framework

D. P. Snyman(✉) and H. A. Kruger

School of Computer Science and Information Systems, North-West University, Potchefstroom, South Africa
{dirk.snyman,hennie.kruger}@nwu.ac.za

Abstract. This paper presents the development of a framework for evaluating group behaviour in information security in practice. Information security behavioural threshold analysis is employed as the theoretical foundation for the proposed framework. The suitability of the proposed framework is evaluated based on two sets of qualitative measures (general frameworks and information security frameworks) which were identified from literature. A novel conceptual mapping of the two sets of evaluation measures is presented and used to evaluate the proposed framework. The successful evaluation of the proposed framework, guided by the identified evaluation measures, is presented in terms of positive practical applications, as well as positive peer review and publication of the underlying theory.

Keywords: Information security group behaviour · Framework development · Evaluation

1 Introduction

Many models and frameworks are used throughout information security (InfoSec) literature to determine or explain attitude that individuals exhibit towards InfoSec which is indicative of their eventual behaviour [1]. Such frameworks and models are mainly focussed on the individual's behaviour, and researchers infer that this should apply to group behaviour as well. However, this is not always the case, as there are many other influences on group behaviour, such as the lemming effect, contextual factors, influential people, etc. It is, therefore, not enough to simply expect individual behaviour to be indicative of group behaviour.

To the best of the researchers' knowledge, no framework for analysing and predicting InfoSec group behaviour is currently available in literature. In this paper, a formal framework is proposed for group behaviour in InfoSec. This proposed framework is based in part on aspects found in existing frameworks [1], i.e. norms, beliefs, attitudes, etc. The other integral part of the framework will then consist of those aspects that are specific to group behaviour, i.e. the use of a technique, such as behavioural threshold

© IFIP International Federation for Information Processing 2020
Published by Springer Nature Switzerland AG 2020
N. Clarke and S. Furnell (Eds.): HAISA 2020, IFIP AICT 593, pp. 133–143, 2020.
https://doi.org/10.1007/978-3-030-57404-8_11

analysis (BTA) that considers factors, such as the lemming effect and external contextual factors. This paper represents the culmination of an overarching study in which the use of a BTA approach was conceptualised in terms of group behaviour in InfoSec, and with the abovementioned background in mind, the aim of this study is now firstly, to *formalise a framework for evaluating information security group behaviour in practice, supported by behavioural threshold analysis as the underlying theory* thereby allowing InfoSec practitioners to utilise the approach, and secondly, to *critically evaluate the proposed framework based on qualitative measures from literature.*

The remainder of this paper is structured as follows: In Sect. 2, a brief contextualisation for applying research in practice and a theoretical view on the requirements of a successful framework are presented. In Sects. 3 and 4 the development of the resulting framework and the evaluation thereof, based on the requirements from Sect. 2 are described. A discussion on the general and specific contributions of the resulting framework is presented in Sect. 5 and the paper is concluded in Sect. 6.

2 Literature Review

2.1 Contextualisation

Translating research findings and recommendations of any nature into practice remains an elusive process [2–4]. Some of the reasons why this general disconnect exists between most types of research and the related acceptance thereof in practice include ambiguity in existing research [3, 5]; limited published reflection on implementation [5]; ongoing research is often still inconclusive [4]; decision makers lack the required information [6]; and attitudes and beliefs of individuals [3, 7] which translates to social and cultural resistance to the change associated with implementation.

This disconnect between research and practice has also been identified in the domain of InfoSec [5, 8], where it especially holds true for non-technical aspects of InfoSec such as InfoSec awareness and behaviour. Research into human behaviour (and how it relates to InfoSec behaviour and culture) is often based on, and guided by, theoretical models from the fields of sociology and social psychology. While such models can assist in uncovering the intricacies of behaviour by highlighting complexity and structuring the underlying themes, they do not necessarily provide for simple integration into actionable methods in practice.

The level of success of such an integration is, however, subject to three criteria, namely *Evidence*, *Context*, and *Facilitation* [4] (ECF). In terms of research pertaining to InfoSec (specifically security culture), AlHogail [8] suggests following the STOPE approach [7] to facilitate change when implementing new approaches to effect change in the culture and the eventual underlying behaviour. The dimensions to be adhered to for STOPE are *Strategy*, *Technology*, *Organisation*, *People*, and *Environment*.

These criteria and dimensions are therefore subsequently used to guide and evaluate the development of a framework for applying the BTA approach, in the context of InfoSec, in practice.

2.2 Framework Requirements

The qualitative criteria for evaluating frameworks in general (*Evidence*, *Context*, and *Facilitation*) and for frameworks for InfoSec (STOPE) will be presented here in detail and contextualised in terms of research in general versus InfoSec research. Finally, a mapping of how these two approaches align, and how they relate to this research is presented.

Evidence, Context, and Facilitation
In terms of an implementation framework, the interaction between Evidence (E), Context (C), and Facilitation (F) is said to determine the eventual Successful Implementation (SI) of the framework in practice, i.e. SI is a function of three criteria [4] so that

$$SI = f(E, C, F) \tag{1}$$

The success of the implementation is therefore dependent on the level of maturity by which each of the criteria is met. Each of the criteria and what each represents in terms of a framework is briefly described here. Where applicable, these criteria are already presented in terms of InfoSec:

Evidence - Evidence refers to the level of scrutiny that the model or approach that underpins a framework has undergone. Is there substantiated proof that the model is fit for purpose? [4]

Context - Context is concerned with the setting in which a framework is to be applied in practice. In general, this refers to the physical attributes of the environment such as buildings, people, and processes [9]. However, for the successful implementation of a framework, this view might be too narrow, since in essence context also implicitly refers to intangible qualities, such as individual and group behaviour, and the underlying (security) culture [3, 9].

Facilitation - Implementing research in practice is essentially a process whereby change of some kind is sought to be effected. Change is a process that ought to be facilitated if it is to be successful and long-lived [3]. Such facilitation refers to the understanding of (and ultimately altering) attitudes and behaviours, specifically by leveraging the way in which "an individual is able to influence other individuals' attitudes or overt behaviour" [3, 10]. In terms of InfoSec, Snyman and Kruger [11] hypothesise that while some people may inherently be more influential [3], the behaviour of all individuals exerts influence on the eventual behaviour of a group.

STOPE
InfoSec frameworks may be evaluated by means of a critical evaluation of how well the framework addresses *Strategy*, *Technology*, *Organisation*, *People*, and the *Environment*. Each of these dimensions is briefly explained below, based on the work of AlHogail [8] which contextualises them in terms of InfoSec.

Strategy – Strategy refers to the suggested measures that are applied to effect change within an organisation to improve its overall levels of InfoSec. These approaches may include the implementation of formal plans of action, such as InfoSec policies and guidelines as well as the structured approach of a framework.

Technology – In this context, technological means of addressing InfoSec is referred to as technology. Frameworks should ideally provide for changes or improvements on the technical measures that are used to safeguard systems.

Organisation – The success of strategy is reliant on the underlying security culture of an organisation. This culture and eventual behaviour are often influenced by the way in which an organisation is structured. A framework should provide guidelines for how structures within an organisation will influence the application thereof and, ideally, how structures may be leveraged to achieve the goal of the framework.

People – InfoSec ultimately revolves around people. It is often people that undo security due to unwanted actions. Frameworks should seek to address the human aspect of InfoSec in terms of behaviour, culture and awareness.

Environment – Environment view refers to the greater context in which an organisation has to address InfoSec, and which should be included in the application of a framework. On a macro level, this may include concepts, such as regulatory frameworks and legislation [8], but on a smaller level can refer to the context in which an individual or group behave in terms of InfoSec [9].

Mapping STOPE to ECF

An assessment of the framework evaluation criteria as mentioned in Sects. 2.1 and 2.2 above allows for a combination of the two approaches by means of a conceptual mapping. Table 1 shows the conceptual mapping of STOPE to ECF:

Table 1. Conceptual mapping of STOPE to ECF

Evidence	Context	Facilitation
Peer review combined with resulting STOPE evaluation	O:Organisation P:People E:Environment	S:Strategy T:Technology

From Table 1, it can be seen that the individual views from STOPE could not as easily be mapped to Evidence (ECF), as all these views can contribute in some way to this criterion. It is concerned with the rigour of the underlying model on which a framework is based. It stands to reason then, that in combination with other types of measures that can confirm said rigour (e.g. peer review, or experimentation), evidence can thus be conceptualised as the resulting evaluation that is conveyed by STOPE. However, in the context of this research, Evidence will be used as a freestanding criterion, evaluated on the available peer review, case studies, and successful implementations. For the remaining criteria, the Organisation, People and Environment from STOPE [8] can be directly mapped to Context [3] from ECF. Overlapping themes include people, behaviour, culture, and physical attributes of the environment. In the final instance, Facilitation (ECF) encompasses the strategy and technology views from STOPE. The common concepts from these constructs that can be identified are the approaches for achieving positive change through organisational, technological, and human means.

3 Framework Model and Development

In order to describe the development of the suggested framework, the underlying theoretical model should first be presented. In this section, the aim is to firstly summarise the BTA model as implemented in the greater research project, followed by a description of the resulting framework and its elements.

3.1 Behavioural Threshold Analysis Model

Group behaviour is a complex phenomenon. To analyse this complexity, Granovetter [12] describes a theory called "Threshold models of collective behaviour". The model described by Granovetter is used as the underlying theoretical grounding for the framework. In short, the model takes into account the mechanisms whereby individuals influence the behaviour of each other, i.e. based on an intrinsic inclination of an individual to follow the example of existing group behaviour. This inclination to follow behaviour is conceptualised as the individual's behavioural threshold. The said threshold is expressed as a percentage of group members who perform a behaviour that will sway an individual to participate in the specific behaviour. When the (perceived) participation rate of group members exceeds the behavioural threshold of the individual, the individual will follow the group's example and also perform the behaviour. When participation in group behaviour exceeds an individual's threshold for participation, the individual might even perform group behaviour that is contrary to his/her convictions and predisposition.

Growney [13] describes how the model can be implemented in circumstances where groups of individuals congregate and how the mathematical aggregate of behavioural thresholds may be interpreted to allow for a prediction of eventual group behaviour. The model was successfully applied in InfoSec in earlier, related studies and the reader is referred to these sources for in-depth reading on the application of BTA in InfoSec [11, 14, 15].

3.2 Development of Information Security Group Behaviour Framework

In Sect. 1, reference was made to the first aim of this research, namely, to formalise a framework for the practical application of BTA in InfoSec. To address this aim, Fig. 1 shows the proposed framework for evaluating group behaviour in InfoSec and illustrates the overarching development and categorises different epochs of the framework's development. Each of the epochs is subsequently briefly described below.

1) Theoretical development – This epoch refers to the investigation into group behaviour in InfoSec. It includes a review of the related literature on the following themes: human behaviour in general and in the context of InfoSec; modelling human behaviour, e.g. the theory of planned behaviour, and its employment in security awareness and security culture; and group behaviour (threshold models of collective behaviour) and the analysis thereof (BTA). The development of the underlying theory also comprises the development of methodological and practical guidelines for experimental and practical applications.

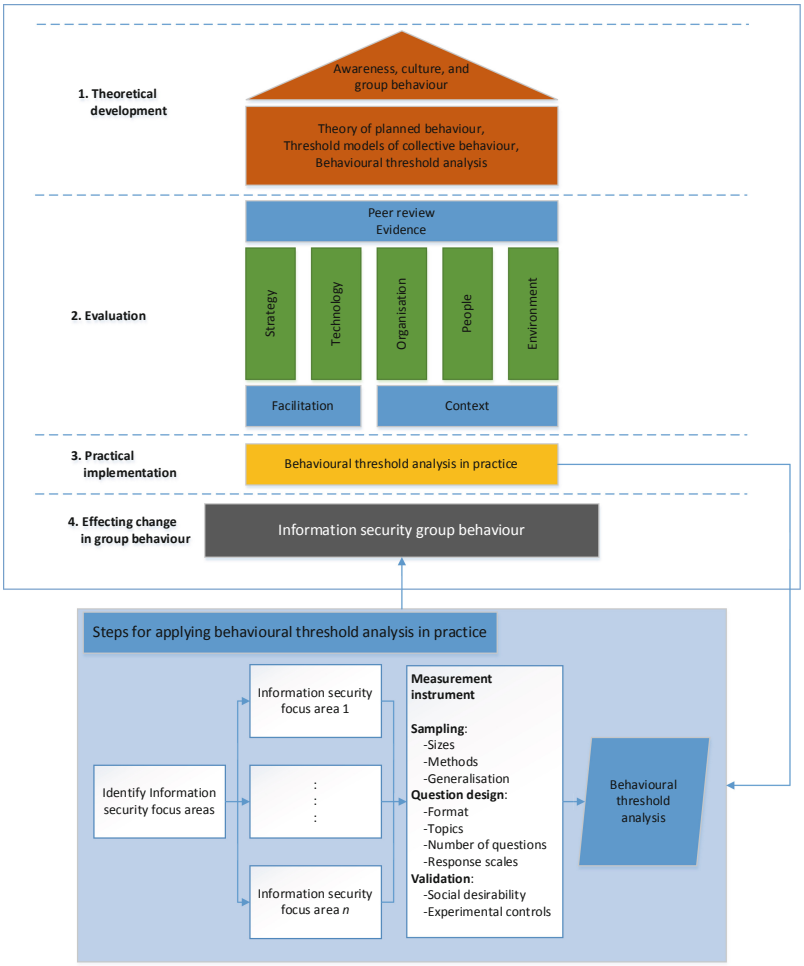


Fig. 1. Framework for the evaluation of information security group behaviour in practice

2) Evaluation – Based on the aforementioned ECF criteria and STOPE views, the evaluation epoch refers to a formal evaluation of the underlying theoretical assumptions and the framework itself. In the following section (see Sect. 4), a formal evaluation of the proposed framework is shown.
3) Practical implementation – After a successful evaluation, evidencing a well-founded theoretical basis and framework, the approach is ready for implementation. The blown-up view shows the minutia of the application of BTA in InfoSec.
4) Effecting change in group behaviour – The results of the BTA application may be interpreted to detect areas of InfoSec that need intervention to improve behaviour.

In the following segment (Sect. 4), how the combination of ECF and STOPE was employed to evaluate the proposed framework is shown.

4 Framework Evaluation

During the related research and the development of BTA as an approach for InfoSec, the requirements for ECF and STOPE were met. In this section, the extent to which peer review and practical applications contribute to the maturity of the framework is described.

4.1 Peer Review and Publication

Table 2 shows the STOPE criteria and ECF views. A critical evaluation and motivation are provided.

The applications of the approach in practice are presented in the following subsection.

4.2 Applications in Practice

Throughout the development of the approach to apply BTA in InfoSec, practical experiments were conducted to test the working of the model within this context. An initial pilot study was conducted to test the feasibility of the model [11]. After further development of the approach and the underlying theoretical foundations, such as the required methodological approach [14], two successful practical applications were conducted.

The first practical application of BTA was conducted at an Australian utility company [15]. The resulting insights and recommendations regarding employees' InfoSec behaviour were communicated in a report to the company. Feedback indicated that the insights were found to be invaluable in guiding the directions of future awareness campaigns.

The second application was in an academic context at a South African University [9]. The results from the exercise correlated with the expected and observed InfoSec behaviour of students in a university residence. The success of these practical applications, the commonalities and differences between the different contexts where the approach was applied, and the reporting publications passing peer review, verifies that this procedure for application (as presented in this framework) is effective.

5 Contributions

A twofold discussion of the successes of the framework is presented here in terms of general and specific contributions to the field of InfoSec.

Table 2. Critical evaluation of the proposed framework

	STOPE criteria	Critical evaluation and motivation	*Evidence* (peer-reviewed publications)
Context	Organisation	One of the main c*ontexts* with which BTA is concerned, is that of the *Organisation*. The ultimate outcome of the successful implementation of the approach is improved levels of InfoSec within any organisation where it is applied. A collection of papers, both in InfoSec journals and conference proceedings, were published that contribute to the rigour of the underlying theoretical model and approaches	Organisation forms part of all of the previous papers [9, 11, 14–18] which cannot be listed here due to space constraints. Refer to the References section for full bibliographical details
	People	BTA is based on the behaviour and interaction of people. All the previous work [9, 11, 14–18] therefore encompasses the *People* view; however one paper is highlighted here: Developing the interrelated concepts of sequential decision-making and information cascades in InfoSec, a novel view of the *context* of how InfoSec behaviour is formed was peer-reviewed, published and presented at an international conference	*Theorising on information cascades and sequential decision making for analysing security behaviour* [17]
	Environment	Given the influence of the *environment*, and its many facets on behaviour, a paper on the *contextual* factors that influence InfoSec behaviour was presented at an international conference after peer review and published in the proceedings	*External contextual factors in information security behaviour* [9]
Facilitation	Strategy	A paper that describes and validates the underlying methodology, including some practical considerations for BTA in InfoSec, was published in a peer-reviewed journal. This contributes to formalising the *strategy* to *facilitate* positive change in InfoSec	*Behavioural threshold analysis: Methodological and practical considerations for applications in information security* [14]

(*continued*)

Table 2. (*continued*)

	STOPE criteria	Critical evaluation and motivation	*Evidence* (peer-reviewed publications)
	Technology	With the aim of facilitating and partially automating BTA, a novel data collection method (optical polling) and decision support system (DSS) were developed. This *technology* can help *facilitate* the practical aspects of the model implementation. The novel data collection and the DSS was presented at an international conference and published as a peer-reviewed book chapter.	*Optical polling for behavioural threshold analysis in information security* [16]; *A management decision support system for evaluating information security behaviour* [18]

5.1 General

This research contributes to the general field of InfoSec by having 1) contributed a methodology for formalising a framework for the analysis of group behaviour in InfoSec; 2) synthesised qualitative measures to critically assess and evaluate frameworks in InfoSec by conceptually mapping methods from literature; and 3) contributed an approach to measure InfoSec group behaviour to improve the management thereof and influence change in behaviour. Supplementary to the general contributions above, certain specific contributions were made and are highlighted next.

5.2 Specific

Reflecting on the specific contributions of this research in terms of the initial research aims relating to the proposed framework, the following is pertinent: 1) BTA is identified as a mechanism to evaluate InfoSec group behaviour and expressed as a well-founded underlying theory for this framework; 2) The framework was critically evaluated in terms of the qualitative measures conceptualised from literature, and furthermore, the approach outlined in this framework was successfully applied in practice which further illustrated the suitability of the framework; 3) The framework can be construed as an instrument for appraising InfoSec awareness in organisations which allows InfoSec practitioners to effect positive change in InfoSec behaviour; 4) A methodology for identifying InfoSec focus areas was identified; and 5) An instrument was contributed that is novel in comparison to existing tools for analysing InfoSec group behaviour with respect to its sensitivity towards the influence of external stimuli, such as contextual factors and the lemming effect.

6 Conclusion

In this paper, a formal framework for the evaluation of group behaviour in InfoSec was presented. The framework is based on BTA as the central theoretical model. Two qualitative evaluation methods for frameworks were identified from literature and contextualised in terms of InfoSec group behaviour. A combination of the two evaluation methods was used to evaluate the fittingness of the proposed framework for analysing InfoSec group behaviour. Based on the resulting evaluation, grounded in scientific peer review, as well as successful applications in practice, the proposed framework was deemed to be fit for purpose.

References

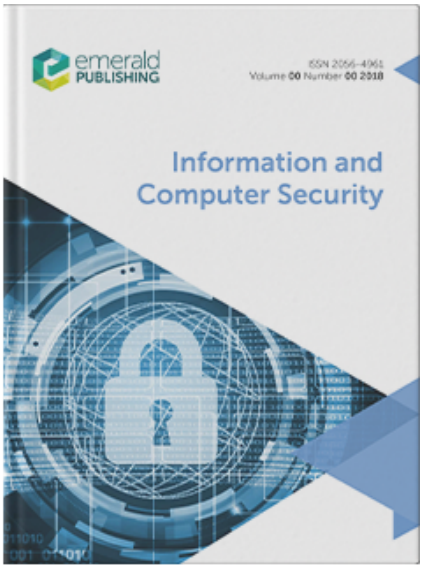
1. Pham, H., Brennan, L., Richardson, J.: Review of behavioural theories in security compliance and research challenge. In: Informing Science and Information Technology Education Conference, Vietnam, pp. 65–76. Informing Science Institute (2017)
2. Grimshaw, J.M., Eccles, M.P., Lavis, J.N., Hill, S.J., Squires, J.E.: Knowledge translation of research findings. Implement. Sci. **7**, 50 (2012). https://doi.org/10.1186/1748-5908-7-50
3. Kent, B.: Implementing research findings into practice: frameworks and guidance. Int. J. Evid.-Based Healthc. **17**, S18–S21 (2019)
4. Kitson, A., Harvey, G., McCormack, B.: Enabling the implementation of evidence based practice: a conceptual framework. BMJ Qual. Saf. **7**, 149–158 (1998)
5. Tsohou, A., Kokolakis, S., Karyda, M., Kiountouzis, E.: Investigating information security awareness: research and practice gaps. Inf. Secur. J.: Glob. Pers. **17**, 207–227 (2008)
6. Haines, A., Donald, A.: Making better use of research findings. BMJ **317**, 72–75 (1998)
7. Bakry, S.H.: Development of security policies for private networks. Int. J. Netw. Manag. **13**, 203–210 (2003)
8. AlHogail, A.: Design and validation of information security culture framework. Comput. Hum. Behav. **49**, 567–575 (2015)
9. Snyman, D.P., Kruger, H.A.: External contextual factors in information security behaviour. In: 6th International Conference on Information Systems Security and Privacy (ICISSP 2020), pp. 185–194. SCITEPRESS – Science and Technology Publications, Lda (2020)
10. Rogers, E.M.: Diffusion of Innovations. Simon and Schuster, New York (2010)
11. Snyman, D.P., Kruger, H.A.: The application of behavioural thresholds to analyse collective behaviour in information security. Inf. Comput. Secur. **25**, 152–164 (2017)
12. Granovetter, M.: Threshold models of collective behavior. Am. J. Sociol. **83**, 1420–1443 (1978)
13. Growney, J.S.: I Will If You Will: Individual Thresholds and Group Behavior - Applications of Algebra to Group Behavior. COMAP Inc., Bedford (1983)
14. Snyman, D.P., Kruger, H.A.: Behavioural threshold analysis: methodological and practical considerations for applications in information security. Behav. Inf. Technol. **38**, 1–19 (2019)
15. Snyman, D.P., Kruger, H.A., Kearney, W.D.: I shall, we shall, and all others will: paradoxical information security behaviour. Inf. Comput. Secur. **26**, 290–305 (2018)
16. Snyman, D.P., Kruger, H.A.: Optical polling for behavioural threshold analysis in information security. In: International Conference on Information and Knowledge Engineering (IKE 2017), pp. 39–45. CSREA Press (2017)

17. Snyman, D.P., Kruger, H.A.: Theorising on information cascades and sequential decision-making for analysing security behaviour. In: 5th International Conference on Information Systems Security and Privacy (ICISSP 2019), pp. 205–212. SCITEPRESS – Science and Technology Publications, Lda., Prague (2019)
18. Snyman, D., Kruger, H.: A management decision support system for evaluating information security behaviour. In: Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (eds.) ISSA 2019. CCIS, vol. 1166, pp. 15–27. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-43276-8_2

Appendix F – Information and Computer Security publication guidelines (Emerald)

In accordance with the General Academic Rules of the North-West University (A.5.10.5), it is a requirement to include author guidelines for papers presented in a thesis. The author guidelines for the articles presented in Chapters 3, 5, and 10, which were accepted, or published in *Information & Computer Security* are presented here. The author guidelines for this journal were obtained from the publisher website[16].

[16] https://www.emeraldgrouppublishing.com/journal/ics#author-guidelines



Information and Computer Security

ISSN: 2056-4961

Submit your paper

Calls for papers

Useful links:

Table of contents

Get a sample article

How to subscribe & buy

Journal description

Information and Computer Security aims to cover the human aspects of security, looking at the impact of user and business behaviours when dealing with security issues. It communicates fresh ideas and cutting-edge research to academics and practitioners.

Aims & scope

Editorial team

Author guidelines

Before you start

For queries relating to the status of your paper pre decision, please contact the Editor or Journal Editorial Office. For queries post acceptance, please contact the Supplier Project Manager. These details can be found in the Editorial Team section.

Author responsibilities

Our goal is to provide you with a professional and courteous experience at each stage of the review and publication process. There are also some responsibilities that sit with you as the author. Our expectation is that you will:

- Respond swiftly to any queries during the publication process.
- Be accountable for all aspects of your work. This includes investigating and resolving any questions about accuracy or **research integrity**
- Treat communications between you and the journal editor as confidential until an editorial decision has been made.
- Read about our **research ethics** for authorship. These state that you must:
  - **Include** anyone who has made a substantial and meaningful contribution to the submission (anyone else involved in the paper should be listed in the acknowledgements).
  - **Exclude** anyone who hasn't contributed to the paper, or who has chosen not to be associated with the research.

Research and publishing ethics

Our editors and employees work hard to ensure the content we publish is ethically sound. To help us achieve that goal, we closely follow the advice laid out in the guidelines and flowcharts on the **COPE (Committee on Publication Ethics) website**.

We have also developed our **research and publishing ethics guidelines**. If you haven't already read these, we urge you to do so – they will help you avoid the most common publishing ethics issues.

A few key points:

- Any manuscript you submit to this journal should be original. That means it should not have been published before in its current, or similar, form. Exceptions to this rule are outlined in our **pre-print and conference paper policies**. If any substantial element of your paper has been previously published, you need to declare this to the journal editor upon submission. Please note, the journal editor may use **Crossref Similarity Check** to check on the originality of submissions received. This service compares submissions against a database of 49 million works from 800 scholarly publishers.
- Your work should not have been submitted elsewhere and should not be under consideration by any other publication.
- If you have a conflict of interest, you must declare it upon submission; this allows the editor to decide how they would like to proceed. Read about conflict of interest in our **research and publishing ethics guidelines**.
- By submitting your work to Emerald, you are guaranteeing that the work is not in infringement of any existing copyright.

Third party copyright permissions

Prior to article submission, you need to ensure you've applied for, and received, written permission to use any material in your manuscript that has been created by a third party. Please note, we are unable to publish any article that still has permissions pending. The rights we require are:

- Non-exclusive rights to reproduce the material in the article or book chapter.
- Print and electronic rights.
- Worldwide English-language rights.
- To use the material for the life of the work. That means there should be no time restrictions on its re-use e.g. a one-year licence.

We are a member of the International Association of Scientific, Technical, and Medical Publishers (STM) and participate in the **STM permissions guidelines**, a reciprocal free exchange of material with other STM publishers. In some cases, this may mean that you don't need permission to re-use content. If so, please highlight this at the submission stage.

Please take a few moments to read our **guide to publishing permissions** to ensure you have met all the requirements, so that we can process your submission without delay.

Open access submissions and information

All our journals currently offer two open access (OA) publishing paths; gold open access and green open access.

If you would like to, or are required to, make the branded publisher PDF (also known as the version of record) freely available immediately upon publication, you should select the gold open access route during the submission process.

If you've chosen to publish gold open access, this is the point you will be asked to pay the **APC (article processing charge)**. This varies per journal and can be found on our APC price list or on the editorial system at the point of submission. Your article will be published with a **Creative Commons CC BY 4.0 user licence**, which outlines how readers can reuse your work.

Alternatively, if you would like to, or are required to, publish open access but your funding doesn't cover the cost of the APC, you can choose the green open access, or self-archiving, route. As soon as your article is published, you can make the author accepted manuscript (the version accepted for publication) openly available, free from payment and embargo periods.

For UK journal article authors - if you wish to submit your work accepted by us to REF 2021, you must make a 'closed deposit' of your accepted manuscript to your respective institutional repository upon acceptance of your article. Articles accepted for publication after 1st April 2018 should be deposited as soon as possible, but no later than three months after the acceptance date. For further information and guidance, please refer to the **REF 2021** website.

You can find out more about our open access routes, our APCs and waivers and read our FAQs on our open research page.

Find out about open

Transparency and Openness Promotion (TOP) Guidelines

We are a signatory of the **Transparency and Openness Promotion (TOP) Guidelines**, a framework that supports the reproducibility of research through the adoption of transparent research practices. That means we encourage you to:

- Cite and fully reference all data, program code, and other methods in your article.
- Include persistent identifiers, such as a Digital Object Identifier (DOI), in references for datasets and program codes. Persistent identifiers ensure future access to unique published digital objects, such as a piece of text or datasets. Persistent identifiers are assigned to datasets by digital archives, such as institutional repositories and partners in the Data Preservation Alliance for the Social Sciences (Data-PASS).
- Follow appropriate international and national procedures with respect to data protection, rights to privacy and other ethical considerations, whenever you cite data. For further guidance please refer to our **research and publishing ethics guidelines**. For an example on how to cite datasets, please refer to the references section below.

Prepare your submission

Manuscript support services

We are pleased to partner with Editage, a platform that connects you with relevant experts in language support, translation, editing, visuals, consulting, and more. After you've agreed a fee, they will work with you to enhance your manuscript and get it submission-ready.

This is an optional service for authors who feel they need a little extra support. It does not guarantee your work will be accepted for review or publication.

Visit Editage

Manuscript requirements

Before you submit your manuscript, it's important you read and follow the guidelines below. You will also find some useful tips in our **structure your journal submission** how-to guide.

Format	Article files should be provided in Microsoft Word format While you are welcome to submit a PDF of the document alongside the Word file, PDFs alone are not acceptable. LaTeX files can also be used but only if an accompanying PDF document is provided. Acceptable figure file types are listed further below.
Article length / word count	Articles should be up to a maximum of 7500 words in length. This includes all text, for example, the structured abstract, references, all text in tables, and figures and appendices. Please allow 280 words for each figure or table.

Article title	A concisely worded title should be provided.
Author details	The names of all contributing authors should be added to the ScholarOne submission; please list them in the order in which you'd like them to be published. Each contributing author will need their own ScholarOne author account, from which we will extract the following details: • **Author email address**. • **Author name**. We will reproduce it exactly, so any middle names and/or initials they want featured must be included. • **Author affiliation**. This should be where they were based when the research for the paper was conducted. In multi-authored papers, it's important that ALL authors that have made a significant contribution to the paper are listed. Those who have provided support but have not contributed to the research should be featured in an acknowledgements section. You should never include people who have not contributed to the paper or who don't want to be associated with the research. Read about our **research ethics** for authorship.
Biographies and acknowledgements	If you want to include these items, save them in a separate Microsoft Word document and upload the file with your submission. Where they are included, a brief professional biography of not more than 100 words should be supplied for each named author.
Research funding	Your article must reference all sources of external research funding in the acknowledgements section. You should describe the role of the funder or financial sponsor in the entire research process, from study design to submission.
Structured abstract	All submissions must include a structured abstract, following the format outlined below. These four sub-headings and their accompanying explanations must always be included: • Purpose • Design/methodology/approach • Findings • Originality The following three sub-headings are optional and can be included, if applicable: • Research limitations/implications • Practical implications • Social implications You can find some useful tips in our **write an article abstract** how-to guide. The maximum length of your abstract should be 250 words in total, including keywords and article classification (see the sections below).

Keywords	Your submission should include up to 12 appropriate and short keywords that capture the principal topics of the paper. Our **Creating an SEO-friendly manuscript** how to guide contains some practical guidance on choosing search-engine friendly keywords. Please note, while we will always try to use the keywords you've suggested, the in-house editorial team may replace some of them with matching terms to ensure consistency across publications and improve your article's visibility.
Article classification	During the submission process, you will be asked to select a type for your paper; the options are listed below. If you don't see an exact match, please choose the best fit: • Original Article • Book Reviews You will also be asked to select a category for your paper. The options for this are listed below. If you don't see an exact match, please choose the best fit: **Research paper.** Reports on any type of research undertaken by the author(s), including: • The construction or testing of a model or framework • Action research • Testing of data, market research or surveys • Empirical, scientific or clinical research • Papers with a practical focus **Viewpoint.** Covers any paper where content is dependent on the author's opinion and interpretation. This includes journalistic and magazine-style pieces. **Technical paper.** Describes and evaluates technical products, processes or services. **Conceptual paper.** Focuses on developing hypotheses and is usually discursive. Covers philosophical discussions and comparative studies of other authors' work and thinking. **Case study.** Describes actual interventions or experiences within organizations. It can be subjective and doesn't generally report on research. Also covers a description of a legal case or a hypothetical case study used as a teaching exercise. **Literature review.** This category should only be used if the main purpose of the paper is to annotate and/or critique the literature in a particular field. It could be a selective bibliography providing advice on information sources, or the paper may aim to cover the main contributors to the development of a topic and explore their different views. **General review.** Provides an overview or historical examination of some concept, technique or phenomenon. Papers are likely to be more descriptive or instructional ('how to' papers) than discursive.

Headings	Headings must be concise, with a clear indication of the required hierarchy. The preferred format is for first level headings to be in bold, and subsequent sub-headings to be in medium italics.
Notes/endnotes	Notes or endnotes should only be used if absolutely necessary. They should be identified in the text by consecutive numbers enclosed in square brackets. These numbers should then be listed, and explained, at the end of the article.
Figures	All figures (charts, diagrams, line drawings, webpages/screenshots, and photographic images) should be submitted electronically. Both colour and black and white files are accepted. There are a few other important points to note: • All figures should be supplied at the highest resolution/quality possible with numbers and text clearly legible. • Acceptable formats are .ai, .eps, .jpeg, .bmp, and .tif. • Electronic figures created in other applications should be supplied in their original formats and should also be either copied and pasted into a blank MS Word document, or submitted as a PDF file. • All figures should be numbered consecutively with Arabic numerals and have clear captions. • All photographs should be numbered as Plate 1, 2, 3, etc. and have clear captions.
Tables	Tables should be typed and submitted in a separate file to the main body of the article. The position of each table should be clearly labelled in the main body of the article with corresponding labels clearly shown in the table file. Tables should be numbered consecutively in Roman numerals (e.g. I, II, etc.). Give each table a brief title. Ensure that any superscripts or asterisks are shown next to the relevant items and have explanations displayed as footnotes to the table, figure or plate.
References	All references in your manuscript must be formatted using one of the recognised Harvard styles. You are welcome to use the Harvard style Emerald has adopted – we've provided a detailed guide below. Want to use a different Harvard style? That's fine, our typesetters will make any necessary changes to your manuscript if it is accepted. Please ensure you check all your citations for completeness, accuracy and consistency. **Emerald's Harvard referencing style** References to other publications in your text should be written as follows: • Single author: (Adams, 2006) • Two authors: (Adams and Brown, 2006) • Three or more authors: (Adams *et al.*, 2006) Please note, '*et al*' should always be written in italics.

	A few other style points. These apply to both the main body of text and your final list of references. • When referring to pages in a publication, use 'p.(page number)' for a single page or 'pp.(page numbers)' to indicate a page range. • Page numbers should always be written out in full, e.g. 175-179, not 175-9. • Where a colon or dash appears in the title of an article or book chapter, the letter that follows that colon or dash should always be lower case. • When citing a work with multiple editors, use the abbreviation 'Ed.s'. At the end of your paper, please supply a reference list in alphabetical order using the style guidelines below. Where a DOI is available, this should be included at the end of the reference.
For books	Surname, initials (year), *title of book*, publisher, place of publication. e.g. Harrow, R. (2005), *No Place to Hide*, Simon & Schuster, New York, NY.
For book chapters	Surname, initials (year), "chapter title", editor's surname, initials (Ed.), *title of book*, publisher, place of publication, page numbers. e.g. Calabrese, F.A. (2005), "The early pathways: theory to practice – a continuum", Stankosky, M. (Ed.), *Creating the Discipline of Knowledge Management*, Elsevier, New York, NY, pp.15-20.
For journals	Surname, initials (year), "title of article", *journal name*, volume issue, page numbers. e.g. Capizzi, M.T. and Ferguson, R. (2005), "Loyalty trends for the twenty-first century", *Journal of Consumer Marketing*, Vol. 22 No. 2, pp.72-80.
For published conference proceedings	Surname, initials (year of publication), "title of paper", in editor's surname, initials (Ed.), *title of published proceeding which may include place and date(s) held*, publisher, place of publication, page numbers. e.g. Wilde, S. and Cox, C. (2008), "Principal factors contributing to the competitiveness of tourism destinations at varying stages of development", in Richardson, S., Fredline, L., Patiar A., & Ternel, M. (Ed.s), *CAUTHE 2008: Where the 'bloody hell' are we?*, Griffith University, Gold Coast, Qld, pp.115-118.
For unpublished conference proceedings	Surname, initials (year), "title of paper", paper presented at [name of conference], [date of conference], [place of conference], available at: URL if freely available on the internet (accessed date). e.g. Aumueller, D. (2005), "Semantic authoring and retrieval within a wiki", paper presented at the European Semantic Web Conference (ESWC), 29 May-1 June, Heraklion, Crete, available at: http://dbs.uni-leipzig.de/file/aumueller05wiksar.pdf (accessed 20 February 2007).

For working papers	Surname, initials (year), "title of article", working paper [number if available], institution or organization, place of organization, date. e.g. Moizer, P. (2003), "How published academic research can inform policy decisions: the case of mandatory rotation of audit appointments", working paper, Leeds University Business School, University of Leeds, Leeds, 28 March.
For encyclopaedia entries (with no author or editor)	*Title of encyclopaedia* (year), "title of entry", volume, edition, title of encyclopaedia, publisher, place of publication, page numbers. e.g. *Encyclopaedia Britannica* (1926), "Psychology of culture contact", Vol. 1, 13th ed., Encyclopaedia Britannica, London and New York, NY, pp.765-771. (for authored entries, please refer to book chapter guidelines above)
For newspaper articles (authored)	Surname, initials (year), "article title", *newspaper*, date, page numbers. e.g. Smith, A. (2008), "Money for old rope", *Daily News*, 21 January, pp.1, 3-4.
For newspaper articles (non-authored)	*Newspaper* (year), "article title", date, page numbers. e.g. *Daily News* (2008), "Small change", 2 February, p.7.
For archival or other unpublished sources	Surname, initials (year), "title of document", unpublished manuscript, collection name, inventory record, name of archive, location of archive. e.g. Litman, S. (1902), "Mechanism & Technique of Commerce", unpublished manuscript, Simon Litman Papers, Record series 9/5/29 Box 3, University of Illinois Archives, Urbana-Champaign, IL.
For electronic sources	If available online, the full URL should be supplied at the end of the reference, as well as the date that the resource was accessed. Surname, initials (year), "title of electronic source", available at: persistent URL (accessed date month year). e.g. Weida, S. and Stolley, K. (2013), "Developing strong thesis statements", available at: https://owl.english.purdue.edu/owl/resource/588/1/ (accessed 20 June 2018) Standalone URLs, i.e. those without an author or date, should be included either inside parentheses within the main text, or preferably set as a note (Roman numeral within square brackets within text followed by the full URL address at the end of the paper).
For data	Surname, initials (year), *title of dataset*, name of data repository, available at: persistent URL, (accessed date month year). e.g. Campbell, A. and Kahn, R.L. (2015), *American National Election Study, 1948*, ICPSR07218-v4, Inter-university Consortium for Political and Social

	Research (distributor), Ann Arbor, MI, available at: https://doi.org/10.3886/ICPSR07218.v4 (accessed 20 June 2018)

Appendix G – Proceedings publication guidelines (IKE'17)

In accordance with the General Academic Rules of the North-West University (A.5.10.5), it is a requirement to include author guidelines for papers presented in a thesis. The author guidelines for the article presented in Chapter 4, which was published in the proceedings of the *International Conference on Information and Knowledge Engineering*, are presented here. The author guidelines for this conference were obtained from the conference website[17].

[17] https://americancse.org/events/csce2017/conferences/ike17/submission_of_papers

IKE'17

IKE'17
HISTORY
SCOPE & TOPICS
IMPORTANT DATES
KEYNOTES/LECTURES
SESSION PROPOSALS
SUBMISSION OF PAPERS
PUBLICATION & INDEXING
PROGRAM COMMITTEE
CO-SPONSORS
CONTACT

Conferences

CONFERENCES
ABDA'17
ACC'17
BIOCOMP'17
BIOENG'17
CSC'17
DMIN'17
EEE'17
ESCS'17
FCS'17
FECS'17
GCC'17
HIMS'17
ICAI'17
ICOMP'17
ICWN'17
IKE'17
IPCV'17
MSV'17
PDPTA'17
SAM'17
SERP'17

Featured Tracks

Innovative Projects for International Collaborations: Investing for the Future (IPIC'17)
Click here for details

4th Doctoral Colloquium & Demos Sessions 2017 (DCDS'17)
Click here for details

Submission of Papers

by admin — last modified May 11, 2017 09:43 PM

Submission of Draft Papers for Evaluation

Prospective authors are invited to submit their papers by uploading them to the evaluation web site at: http://american-cse.org. Submissions must be uploaded by the due date (see **IMPORTANT DATES**) and must be in either MS doc or pdf formats (7 pages for Regular Research Papers; 4 pages for Short Research Papers; 2 pages for Extended Abstract/Poster Papers - the number of pages include all figures, tables, and references).

Each paper will be PEER-REVIEWED by two experts in the field for originality, significance, clarity, impact, and soundness. In cases of contradictory recommendations, a member of the conference program committee would be charged to make the final decision (accept/reject); often, this would involve seeking help from additional referees..

Papers whose authors include a member of the conference program committee will be evaluated using the double-blinded review process. (Essay/philosophical papers will not be refereed but may be considered for discussion/panels)..

All reasonable typesetting formats are acceptable (later, the authors of accepted papers will be asked to follow a particular typesetting format to prepare their final papers for publication; these formatting instructions appear at: http://american-cse.org and they conform to the two-column IEEE style format). Papers must not have been previously published or currently submitted for publication elsewhere.

The first page of the paper should include the followings:

- Title of the paper
- Name, affiliation, postal address, and email address of each author (identify the name of the Contact Author)
- Abstract (between 100 and 120 words)
- A maximum of 5 topical keywords that would best represent the work described in the paper
- Write the type of the submission as "Regular Research Paper", "Short Research Paper", or "Extended Abstract/Poster Paper".
- The actual text of the paper can start from the first page (space permitting). Submissions are to be uploaded to the submission/evaluation web site portal at: http://american-cse.org.

Type of Submissions/Papers:

- **Full/Regular Research Papers** (maximum of 7 pages): Regular Research Papers should provide detail original research contributions. They must report new research results that represent a contribution to the field; sufficient details and support for the results and conclusions should also be provided. The work presented in regular papers are expected to be at a stage of maturity that with some additional work can be published as journal papers.
- **Short Research Papers** (maximum of 4 pages): Short Research Papers report on ongoing research projects. They should provide overall research methodologies with some results. The work presented in short papers are expected to be at a stage of maturity that with some additional work can be published as regular papers.
- **Extended Abstract/Poster Papers** (maximum of 2 pages): Poster papers report on ongoing research projects that are still in their infancy (i.e., at very early stages). Such papers tend to provide research methodologies without yet concrete results.

Authors are to conform to the common **CODE OF ETHICS FOR AUTHORS** *(The document for the Code of Ethics is available on the* **submission web site.***) Each paper will be peer-reviewed by two experts in the field for originality, significance, clarity, impact, and soundness. In cases of contradictory recommendations, a member of the conference program committee would be charged to make the final decision (accept/reject); often, this would involve seeking help from additional referees. Papers whose authors include a member of the conference program committee will be evaluated using the double-blinded review process. (Essay/philosophical papers will not be refereed but may be considered for discussion/panels).*

Paper Title* (use style: paper title)

*Note: Sub-titles are not captured in Xplore and should not be used

line 1: 1st Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

line 1: 2nd Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

line 1: 3rd Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

line 1: 4th Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

line 1: 5th Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

line 1: 6th Given Name Surname
line 2: *dept. name of organization (of Affiliation)*
line 3: *name of organization (of Affiliation)*
line 4: City, Country
line 5: email address or ORCID

***Abstract*—This electronic document is a "live" template and already defines the components of your paper [title, text, heads, etc.] in its style sheet. **CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.* (*Abstract*)**

Keywords—component, formatting, style, styling, insert (*key words****)***

I. Introduction (*Heading 1*)

This template, modified in MS Word 2007 and saved as a "Word 97-2003 Document" for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II. Ease of Use

A. Selecting a Template (Heading 2)

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the Microsoft Word, Letter file.

B. Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

A. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Units

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as "3.5-inch disk drive".
- Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- Do not mix complete spellings and abbreviations of units: "Wb/m2" or "webers per square meter", not "webers/m2". Spell out units when they appear in text: ". . . a few henries", not ". . . a few H".
- Use a zero before decimal points: "0.25", not ".25". Use "cm3", not "cc". (*bullet list*)

Identify applicable funding agency here. If none, delete this text box.

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

C. Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

$$a + b = \gamma \tag{1}$$

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use "(1)", not "Eq. (1)" or "equation (1)", except at the beginning of a sentence: "Equation (1) is . . ."

D. Some Common Mistakes

- The word "data" is plural, not singular.
- The subscript for the permeability of vacuum μ_0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter "o".
- In American English, commas, semicolons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
- A graph within a graph is an "inset", not an "insert". The word alternatively is preferred to the word "alternately" (unless you really mean something that alternates).
- Do not use the word "essentially" to mean "approximately" or "effectively".
- In your paper title, if the words "that uses" can accurately replace the word "using", capitalize the "u"; if not, keep using lower-cased.
- Be aware of the different meanings of the homophones "affect" and "effect", "complement" and "compliment", "discreet" and "discrete", "principal" and "principle".
- Do not confuse "imply" and "infer".
- The prefix "non" is not a word; it should be joined to the word it modifies, usually without a hyphen.
- There is no period after the "et" in the Latin abbreviation "et al.".
- The abbreviation "i.e." means "that is", and the abbreviation "e.g." means "for example".

An excellent style manual for science writers is [7].

IV. Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. Authors and Affiliations

The template is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

1) For papers with more than six authors: Add author names horizontally, moving to a third row if needed for more than 8 authors.

2) For papers with less than six authors: To change the default, adjust the template as follows.

a) Selection: Highlight all author and affiliation lines.

b) Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select the correct number of columns from the selection palette.

c) Deletion: Delete the author and affiliation lines for the extra authors.

B. Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is "Heading 5". Use "figure caption" for your Figure captions, and "table head" for your table title. Run-in heads, such as "Abstract", will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named "Heading 1", "Heading 2", "Heading 3", and "Heading 4" are prescribed.

C. Figures and Tables

a) Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence.

TABLE I. TABLE TYPE STYLES

Table Head	Table Column Head		
	Table column subhead	***Subhead***	***Subhead***
copy	More table copy[a]		

[a] Sample of a Table footnote. (*Table footnote*)

Fig. 1. Example of a figure caption. (*figure caption*)

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity "Magnetization", or "Magnetization, M", not just "M". If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write "Magnetization (A/m)" or "Magnetization {A[m(1)]}", not just "A/m". Do not label axes with a ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

ACKNOWLEDGMENT *(Heading 5)*

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first ..."

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an MSW document, this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord "Format" pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.

Appendix H – Behaviour & Information Technology publication guidelines (Taylor & Francis)

In accordance with the General Academic Rules of the North-West University (A.5.10.5), it is a requirement to include author guidelines for papers presented in a thesis. The author guidelines for the article presented in Chapter 6, which was published in *Behaviour & Information Technology*, are presented here. The author guidelines for this journal were obtained from the publisher website[18].

[18] https://www.tandfonline.com/action/authorSubmission?show=instructions&journalCode=tbit20

Journal

Behaviour & Information Technology ›

About this journal

Instructions for authors

Thank you for choosing to submit your paper to us. These instructions will ensure we have everything required so your paper can move through peer review, production and publication smoothly. Please take the time to read and follow them as closely as possible, as doing so will ensure your paper matches the journal's requirements.

AUTHOR SERVICES
Supporting Taylor & Francis authors

For general guidance on every stage of the publication process, please visit our Author Services website.

EDITING SERVICES
Supporting Taylor & Francis authors

For editing support, including translation and language polishing, explore our Editing Services website

SCHOLARONE MANUSCRIPTS™

This journal uses ScholarOne Manuscripts (previously Manuscript Central) to peer review manuscript submissions. Please read the guide for ScholarOne authors before making a submission. Complete guidelines for preparing and submitting your manuscript to this journal are provided below.

This title utilises format-free submission. Authors may submit their paper in any scholarly format or layout. References can be in any style or format, so long as a consistent scholarly citation format is applied. For more detail see the format-free submission section below.

Contents

- About the Journal
- Open Access
- Peer Review and Ethics
- Preparing Your Paper
  - Structure
  - Word Limits
  - Format-Free Submissions
  - Editing Services
  - Checklist
- Using Third-Party Material
- Disclosure Statement
- Clinical Trials Registry
- Complying With Ethics of Experimentation
  - Consent
  - Health and Safety
- Submitting Your Paper
- Data Sharing Policy
- Publication Charges
- Copyright Options
- Complying with Funding Agencies
- My Authored Works
- Reprints

About the Journal

Behaviour & Information Technology is an international, peer-reviewed journal publishing high-quality, original research. Please see the journal's Aims & Scope for information about its focus and peer-review policy.

Please note that this journal only publishes manuscripts in English.

Behaviour & Information Technology accepts the following types of article: original articles, book reviews.

Open Access

You have the option to publish open access in this journal via our Open Select publishing program. Publishing open access means that your article will be free to access online immediately on publication, increasing the visibility, readership and impact of your research. Articles published Open Select with Taylor & Francis typically receive 32% more citations* and over 6 times as many downloads** compared to those that are not published Open Select.

Your research funder or your institution may require you to publish your article open access. Visit our Author Services website to find out more about open access policies and how you can comply with these.

You will be asked to pay an article publishing charge (APC) to make your article open access and this cost can often be covered by your institution or funder. Use our APC finder to view the APC for this journal.

Please visit our Author Services website or contact openaccess@tandf.co.uk if you would like more information about our Open Select Program.

*Citations received up to Jan 31st 2020 for articles published in 2015-2019 in journals listed in Web of Science®.
**Usage in 2017-2019 for articles published in 2015-2019.

Peer Review and Ethics

Taylor & Francis is committed to peer-review integrity and upholding the highest standards of review. Once your paper has been assessed for suitability by the editor, it will then be double blind peer reviewed by independent, anonymous expert referees. Find out more about what to expect during peer review and read our guidance on publishing ethics.

Preparing Your Paper

All authors submitting to medicine, biomedicine, health sciences, allied and public health journals should conform to the Uniform Requirements for Manuscripts Submitted to Biomedical Journals, prepared by the International Committee of Medical Journal Editors (ICMJE).

Structure

Your paper should be compiled in the following order: title page; abstract; keywords; main text introduction, materials and methods, results, discussion; acknowledgments; declaration of interest statement; references; appendices (as appropriate); table(s) with caption(s) (on individual pages); figures; figure captions (as a list).

Word Limits

Please include a word count for your paper. There are no word limits for papers in this journal.

Format-Free Submission

Authors may submit their paper in any scholarly format or layout. Manuscripts may be supplied as single or multiple files. These can be Word, rich text format (rtf), open document format (odt), or PDF files. Figures and tables can be placed within the text or submitted as separate documents. Figures should be of sufficient resolution to enable refereeing.

- There are no strict formatting requirements, but all manuscripts must contain the essential elements needed to evaluate a manuscript: abstract, author affiliation, figures, tables, funder information, and references. Further details may be requested upon acceptance.
- References can be in any style or format, so long as a consistent scholarly citation format is applied. Author name(s), journal or book title, article or chapter title, year of publication, volume and issue (where appropriate) and page numbers are essential. All bibliographic entries must contain a corresponding in-text citation. The addition of DOI (Digital Object Identifier) numbers is recommended but not essential.
- The journal reference style will be applied to the paper post-acceptance by Taylor & Francis.
- Spelling can be US or UK English so long as usage is consistent.

Note that, regardless of the file format of the original submission, an editable version of the article must be supplied at the revision stage.

Taylor & Francis Editing Services

To help you improve your manuscript and prepare it for submission, Taylor & Francis provides a range of editing services. Choose from options such as English Language Editing, which will ensure that your article is free of spelling and grammar errors, Translation, and Artwork Preparation. For more information, including pricing, visit this website.

Checklist: What to Include

1. **Author details.** Please ensure everyone meeting the International Committee of Medical Journal Editors (ICMJE) requirements for authorship is included as an author of your paper. All authors of a manuscript should include their full name and affiliation on the cover page of the manuscript. Where available, please also include ORCiDs and social media handles (Facebook, Twitter or LinkedIn). One author will need to be identified as the corresponding author, with their email address normally displayed in the article PDF (depending on the journal) and the online article. Authors' affiliations are the affiliations where the research was conducted. If any of the named co-authors moves affiliation during the peer-review process, the new affiliation can be given as a footnote. Please note that no changes to affiliation can be made after your paper is accepted. Read more on authorship.
2. Should contain an unstructured abstract of 200 words.
3. You can opt to include a **video abstract** with your article. Find out how these can help your work reach a wider audience, and what to think about when filming.
4. Between 3 and 6 **keywords**. Read making your article more discoverable, including information on choosing a title and search engine optimization.
5. **Funding details.** Please supply all details required by your funding and grant-awarding bodies as follows:
   For single agency grants
   This work was supported by the [Funding Agency] under Grant [number xxxx].
   For multiple agency grants
   This work was supported by the [Funding Agency #1] under Grant [number xxxx]; [Funding Agency #2] under Grant [number xxxx]; and [Funding Agency #3] under Grant [number xxxx].

6. **Disclosure statement.** This is to acknowledge any financial interest or benefit that has arisen from the direct applications of your research. Further guidance on what is a conflict of interest and how to disclose it.
7. **Data availability statement.** If there is a data set associated with the paper, please provide information about where the data supporting the results or analyses presented in the paper can be found. Where applicable, this should include the hyperlink, DOI or other persistent identifier associated with the data set(s). Templates are also available to support authors.
8. **Data deposition.** If you choose to share or make the data underlying the study open, please deposit your data in a recognized data repository prior to or at the time of submission. You will be asked to provide the DOI, pre-reserved DOI, or other persistent identifier for the data set.
9. **Supplemental online material.** Supplemental material can be a video, dataset, fileset, sound file or anything which supports (and is pertinent to) your paper. We publish supplemental material online via Figshare. Find out more about supplemental material and how to submit it with your article.
10. **Figures.** Figures should be high quality (1200 dpi for line art, 600 dpi for grayscale and 300 dpi for colour, at the correct size). Figures should be supplied in one of our preferred file formats: EPS, PS, JPEG, TIFF, or Microsoft Word (DOC or DOCX) files are acceptable for figures that have been drawn in Word. For information relating to other file types, please consult our Submission of electronic artwork document.
11. **Tables.** Tables should present new information rather than duplicating what is in the text. Readers should be able to interpret the table without reference to the text. Please supply editable files.
12. **Equations.** If you are submitting your manuscript as a Word document, please ensure that equations are editable. More information about mathematical symbols and equations.
13. **Units.** Please use SI units (non-italicized).

Appendix I – SCITEPRESS proceedings publication guidelines (ICISSP2019/20)

In accordance with the General Academic Rules of the North-West University (A.5.10.5), it is a requirement to include author guidelines for papers presented in a thesis. The author guidelines for the article presented in Chapter 7, which was published in the proceedings of the *International Conference on Information System Security and Privacy* conference for publication in SCITEPRESS proceedings, are presented here. The author guidelines were obtained from the conference website[19].

[19] http://www.icissp.org/Guidelines.aspx

Actions
- **On-line Registration**
- Registration Fees
- Deadlines and Policies
- **Submit Paper**
- Guidelines
- Preparing your Presentation
- Templates
- Glossary
- **Author's Login**
- **Reviewer's Login**
- Ethics of Review

Information
- **Conference Details**
- Important Dates
- Technical Program
- Call for Papers
- Program Committee
- Keynote Lectures
- Best Paper Awards
- **Satellite Events**
- Workshops
- Special Sessions
- Tutorials
- Demos
- Panels
- Doctoral Consortium
- **Partners**
- Academic Partners
- Industrial Partners
- Institutional Partners
- Media Partners
- Partner Events
- Publication Partners
- **Previous Conferences**
- Events
- Abstracts
- Invited Speakers
- Awards
- Books Published

Sponsored by:

INSTICC is Member of:

Logistics Partners:

Guidelines

Submission Guidelines

Authors can submit their work in the form of a complete paper or an abstract.

Complete papers can be submitted as a Regular Paper, representing completed and validated research, or as a Position Paper, portraying a short report of work in progress or an arguable opinion about an issue discussing ideas, facts, situations, methods, procedures or results of scientific research focused on one of the conference topic areas.

An abstract can be submitted to the Abstracts Track, either because the work done represents a very early stage of research, or because the authors wish to present to the audience the results of an already published paper. In the latter case the paper cannot be republished. However, the authors can attach to the abstract a complete paper or a video, if permission to share any such complementing materials is provided. The abstract itself can only have a limited number of characters.

Authors should submit a paper in English, carefully checked for correct grammar and spelling, addressing one or several of the conference areas or topics. Each paper should clearly indicate the nature of its technical/scientific contribution, and the problems, domains or environments to which it is applicable. To facilitate the double-blind paper evaluation method, authors are kindly requested to produce and provide the paper WITHOUT any reference to any of the authors, including the authors' personal details, the acknowledgments section of the paper and any other reference that may disclose the authors' identity.

When submitting a complete paper please note that only original papers should be submitted. Authors are advised to read INSTICC's ethical norms regarding plagiarism and self-plagiarism thoroughly before submitting and must make sure that their submissions do not substantially overlap work which has been published elsewhere or simultaneously submitted to a journal or another conference with proceedings. Papers that contain any form of plagiarism will be rejected without reviews.

All papers must be submitted through the online submission platform PRIMORIS and should follow the instructions and templates that can be found under Guidelines and Templates. After the paper submission has been successfully completed, authors will receive an automatic confirmation e-mail.

Reviewing Process

Complete Papers

All reviews follow a double-blind process. All papers are subject to plagiarism analysis using a software tool prior to review.

All regular papers are reviewed by at least two reviewers, but usually by three or more, and rated considering their: Relevance, Originality, Technical Quality, Significance and Presentation;

The reviewers are also asked to answer a group of questions that may help the authors to improve the paper, should it be accepted, namely: Abstract and Introduction are adequate?, Needs more experimental results?, Needs comparative evaluation?, Improve critical discussion?, Figures are Adequate?, Conclusions/Future Work are convincing?, References are up-to-date and appropriate?, Paper formatting needs adjustment?, Improve English?

Finally, the reviewers can provide some free text observations which was given to the authors and also some free text private observations, made available only to the program chair. Conflicting reviews may require assignment of a new reviewer. In the end the program chairs decide. The author has a period for rebuttal, which triggers a workflow involving the chairs and the reviewers if necessary. All rebuttals are answered but decisions are final.

Position papers follow a similar process but the criteria used for classification are slightly different in order to account for the nature of these papers, i.e. speculative ideas and/or ongoing work not yet fully validated.

Abstracts

The submissions will be screened by a panel of experts, including the conference and program chairs. The reviewers will take into account the relevance of the abstract for the conference, as well as its readability and technical quality, including that of complementing materials, if any is attached.

Conference Paper Formats, including Special Sessions and Workshops

Regular Papers

Submission: It is recommended that Regular Papers are submitted for review with around 8 to 10 pages, with the appropriate font size and page format, including references, tables, graphs, images and appendices. Submissions with less than 4 pages or more than 13 pages will be automatically rejected.

Acceptance: After a double-blind peer review, qualifying Regular Papers may be accepted as either Full Papers or Short Papers.

Presentation: Regular Papers classified as Full Papers are awarded a 25' minutes slot for an oral presentation at the conference. Regular Papers classified as Short Papers are given either a 20' minutes slot for an oral presentation or assigned to present at a Poster Session. Authors who have been assigned an oral presentation, either Full or Short, may however also choose to present at a Poster Session instead, should they prefer it.

Publication: Regular Papers classified as Full Papers will be assigned a 12-page limit in the Conference Proceedings, while Regular Papers classified as Short Papers have an 8-page limit. If absolutely necessary, authors may increase the total number of pages by a maximum of 4

extra pages, for an additional fee. The total number of pages to consider is the number obtained after the paper has been correctly formatted according to the appropriate template. The Conference Proceedings will be published under an ISBN number by SCITEPRESS and include final versions of all accepted papers, adjusted to satisfy reviewers' recommendations. They will be obtainable on paper and digital support, and made available for online consultation at the SCITEPRESS Digital Library. Online publication is exclusive to papers which have been both published and presented at the event.

Indexation: The proceedings will be submitted to SCOPUS, Google Scholar, The DBLP Computer Science Bibliography, Semantic Scholar, Engineering Index (EI) and Web of Science / Conference Proceedings Citation Index for indexation.

Position Papers

Submission: Position Papers should be submitted for review with around 6 or 7 pages, with the appropriate font size and page format, including references, tables, graphs, images and appendices. Submissions with less than 4 pages or more than 9 pages will be automatically rejected.

Acceptance: After a double-blind peer review, qualifying Position Papers will be accepted as Short Papers.

Presentation: Position Papers are given either a 20' minutes slot for an oral presentation or assigned to present at a Poster Session. Authors who have been assigned an oral presentation may however also choose to present at a Poster Session instead, should they prefer it.

Publication: Position Papers will be assigned a 8-page limit in the Conference Proceedings, which will include final versions of all accepted papers, adjusted to satisfy reviewers' recommendations. If absolutely necessary, authors may increase the total number of pages by a maximum of 4 extra pages, for an additional fee. The total number of pages to consider is the number obtained after the paper has been correctly formatted according to the appropriate template. The Conference Proceedings will be published under an ISBN number by SCITEPRESS, on paper and digital support, and made available for online consultation at the SCITEPRESS Digital Library. Online publication is exclusive to papers which have been both published and presented at the event.

Indexation: The proceedings will be submitted to SCOPUS, Google Scholar, The DBLP Computer Science Bibliography, Semantic Scholar, Engineering Index (EI) and Web of Science / Conference Proceedings Citation Index for indexation.

Abstracts

Submission: Authors can submit a 1-page abstract and may include, as complementing material, a previously published paper or a video.

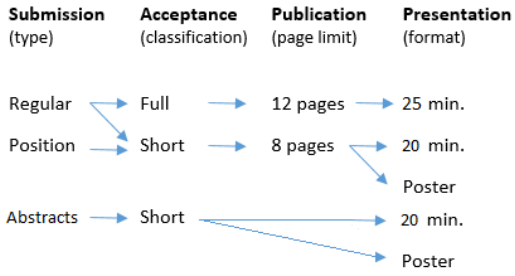
Acceptance: The submissions will be screened by a panel of experts, including the conference and program chairs and can be accepted as Short Papers. Acceptance will indicate, for each paper, also its form of presentation.

Presentation: Abstracts that bring an appropriate complementing material are eligible for oral or poster presentation; otherwise, they are eligible for poster presentation only. Oral presentations are given a 20' minutes time slot. Authors who have been assigned an oral presentation may however choose to present at a Poster Session instead, should they prefer it.

Publication: Abstracts will be advertised in the conference program and in the conference book of abstracts (in the printed and digital version), but not published in the proceedings or included in the Digital Library. Complementary materials will also not be published in the proceedings or included in the Digital Library.

Indexation: Abstracts will not be indexed.

Schematic Summary



INSTRUCTIONS ON HOW TO FORMAT A PAPER TO A SCITEPRESS PUBLISHED PROCEEDING

LANGUAGE

All papers must be in English

ALLOWED NUMBER OF PAGES

The paper must be no longer than:
Twelve (12) pages for full papers
Eight (8) pages for short papers

If needed extra pages may be used. For each extra page a fee will be charged.
Please notice that there is a limit of four (4) extra pages.

PAGE SETUP

Paper Size

A4 (210x297 mm)

Document margins (Please keep these values)

Margins
Top: 3,3 cm
Bottom: 4,2 cm
Left: 2,6 cm
Right: 2,6 cm

Layout
Section start: Continuous
Header: 1,4 cm
Footer: 2,5 cm
Vertical Alignment: Top

IMPORTANT NOTES

Any text or material outside the aforementioned margins **will not be printed**.
Do NOT change the headers and footers. Headers and footers will be added to the document electronically.
No page numbers should be included.

FONT

For best viewing experience the used font must be Times New Roman.

FIRST SECTION - TITLE, AUTHOR(S), AFFILIATION(S), KEYWORDS AND ABSTRACT

General

Text in one column

Title

Align: Center
Linespace exactly at 17pt
Font size: 15pt
Font style: bold
Initial letters Capitalized
In case a subtitle is required, please add a colon (:) just before the subtitle starts. The first of word of the subtitle must have the initial letter capitalized

Authors

Align: Center
Linespace exactly at 13pt
Spacing: before 24pt
Vertical space between authors: 12pt
Font size: 11pt

Affiliations

Align: Center
Linespace exactly at 11pt
Font size: 9pt
Font style: italic
Affiliation should include organisation name, complete address and email.

Keywords

Align: Justify
Linespace exactly at 11pt
Hanging indent 2cm
Spacing: before 48pt
Spacing: after 0pt
Font size: 9pt
Each paper must have at least one keyword with the initial letter capitalized

Abstract

Align: Justify
Linespace exactly at 11pt
Hanging indent 2cm
Spacing: before 12pt
Spacing: after 30 pt
Font size: 9pt
Each paper must have an abstract

SECOND SECTION – PAPER CONTENTS AND REFERENCES

General

Text in two columns
Column width: 7,5 cm
Column spacing: 0,8 cm (Equal column width)
Columns should not have much free blank space.

1 Section Titles*

No dot after the section title number
Align: Left
Linespace exactly at 15pt
Hanging Indent of 0,7 cm
Spacing: before 24pt *(Not applicable to the 1st title section)*
Spacing: after 12pt
Font size: 13pt
Font style: bold
All caps

1.1 Subsection Titles*

Dot only between section and subsection title numbers
Align: Left
Linespace exactly at 13pt
Hanging Indent of 1,0 cm
Spacing: before 11pt *(Not applicable right after a section title)*
Spacing: after 11pt
Font size: 12pt
Font style: bold
Initial letters Capitalized

1.1.1 Sub Subsection Titles*

Dot only between section, subsection and sub subsection title numbers
Align: Left
Linespace exactly at 12pt
Hanging Indent of 1,0 cm
Spacing: before 10pt *(Not applicable right after a subsection title)*
Spacing: after 10pt
Font size: 11pt
Font style: bold
Initial letters Capitalized

Headings

Align: Justify
Linespace single
No identation
Font size: 10pt
Font style: bold
Initial letters Capitalized
Must end with a period

Section Text

Align: Justify
Linespace single
Font size: 10pt
Section, subsection and sub subsection first paragraph without first line indent
Other paragraphs: First line indent of 0,5 cm

Tables

Tables must be properly captioned and numbered sequentially.
All tables must appear within the designated margins or it may span the two columns.
Tables in two columns must be positioned at the top or bottom of the page within margins.
All tables must be centered.
Table caption should follow the format given below:
- Placed above table
- Caption must be centered except when it has more than 1 line, which must be justified
- Font: Times New Roman, 9pt
- Spacing: before 12pt
- Spacing: after 6pt
- No font style such as bold or italic
- The final sentence of a caption must end with a period

Example:
- Table 1: Caption example.

Figures

Figures must be properly captioned and numbered sequentially.
All figures must appear within the designated margins or it may span the two columns.
Figures in two columns must be positioned at the top or bottom of the page within margins.
All figures must be centered.
Figure caption should follow the format given below:
- Placed below the figure
- Caption must be centered except when it has more than 1 line; then it must be justified
- Font: Times New Roman 9pt
- Spacing: before 6pt
- Spacing: after 12pt
- No font style such as bold or italic
- The final sentence of a caption must end with a period

Example:
- Figure 1: Caption example.

Equations

Equations should be placed on a separate line, numbered and centered. An extra line space should be added above and below the equation.
The use of a table with two columns is advisable.

Algorithms and Listings

Algorithms and Listings must be properly captioned and numbered sequentially.
The caption should follow the format given below:
- Caption should be centered except when it has more than 1 line; then it must be justified
- Font: Times New Roman 9pt
- No font style such as bold or italic
- The final sentence of a caption must end with a period

Examples:
- Algorithm 1: Caption example.
- Listing 1: Caption example.

Program Code

Align: Left
Linespace single
Font: Courrier New
Font size: 9pt

Acknowledgements

If any, should be added just before the references as section title without numbering.

Reference Text

Align: Justify
Linespace single
Hanging indent 0.5 cm
Font size: 9pt
References and Citations should follow the Harvard (author, year) system convention.
All references must be cited in the text.

Appendix

If any, should be added just after the references as section title without numbering.

*** The section, subsections and sub subsections numbers must be numbered sequentially. Please avoid using only one subsection within a section.**

Authors' Instructions: Preparation of Camera-Ready Contributions to SCITEPRESS Proceedings

First Author Name[1], Second Author Name[1] and Third Author Name[2]
[1]*Institute of Problem Solving, XYZ University, My Street, MyTown, MyCountry*
[2]*Department of Computing, Main University, MySecondTown, MyCountry*
{f_author, s_author}@ips.xyz.edu, t_author@xy.mu.edu

Keywords: The paper must have at least one keyword. This paragraph should be justified with a linespace of exactly 11-point, special indentation of 2-centimeters and with a spacing before of exactly 48-points. The text should be set in 9-point font size and without the use of bold or italic font style. For more than one keyword, please use a comma as a separator. Keywords must be titlecased.

Abstract: The abstract should summarize the contents of the paper and should contain at least 70 and at most 200 words. It should be set in 9-point font size, justified and should have a hanging indent of 2-centimenter. There should be a space before of 12-point and after of 30-point.

1 INTRODUCTION

Your paper will be part of the conference proceedings therefore we ask that authors follow the guidelines explained in this example and in the file «FormatContentsForAuthors.pdf» also on the zip file, in order to achieve the highest quality possible (Smith, 1998).

Be advised that papers in a technically unsuitable form will be returned for retyping. After returned the manuscript must be appropriately modified.

2 MANUSCRIPT PREPARATION

We strongly encourage authors to use this document for the preparation of the camera-ready. Please follow the instructions closely in order to make the volume look as uniform as possible (Moore and Lopes, 1999).

Please remember that all the papers must be in English and without orthographic errors.

Do not add any text to the headers (do not set running heads) and footers, not even page numbers, because text will be added electronically.

For a best viewing experience the used font must be Times New Roman, on a Macintosh use the font named times, except on special occasions, such as program code (Section 2.3.7).

2.1 Page Setup

The paper size must be set to A4 (210x297 mm). The document margins must be the following:

- Top: 3,3 cm;
- Bottom: 4,2 cm;
- Left: 2,6 cm;
- Right: 2,6 cm.

It is advisable to keep all the given values.

Regarding the page layout, authors should set the Section Start to Continuous with the vertical alignment to the top and the following header and footer:

- Header: 1,4 cm;
- Footer: 2,5 cm.

Any text or material outside the aforementioned margins will not be printed.

2.2 First Section

This section must be in one column.

2.2.1 Title

Use 15-point type for the title, aligned to the center, linespace exactly at 17-point with a bold font style and initial letters capitalized. No formulas or special characters of any form or language are allowed in the title.

Words like “is”, “or”, “then”, etc. should not be capitalized unless they are the first word of the title.

2.2.2 Subtitle

Added on the same line as the title preceded by a colon (:). Use 15-point type for the subtitle, aligned to the center, linespace exactly at 17-point with a bold font style and initial letters capitalized. No formulas or special characters of any form or language are allowed in the subtitle.
Words like “is”, “or”, “then”, etc. should not be capitalized unless they are the first word of the subtitle.

2.2.3 Authors

Author(s) name(s) should be aligned to the center with linespace exactly at 13-point. The text must be set to 11-point.

There should be a spacing before of 24-point.

2.2.4 Affiliations

Affiliation(s) should appear aligned to the center including organisation, address and e-mail.

The linespace must be of exactly 11-point with 9-point of font size and the font style set to italic.

2.2.5 Keywords

Each paper must have at least one keyword. If more than one is specified, please use a comma as a separator. Keywords should appear justified, with a linespace exactly of 11-point, a hanging indent of 2-centimeters, spacing before of 48-point, no spacing after and font size of 9-point.

The sentence must end with a period.

2.2.6 Abstract

Each paper must have an abstract. The abstract should appear justified, with a linespace exactly of 11-point, a hanging indent of 2-centimeters, spacing before of 12-point and after of 30-point, and font size of 9-point.

The sentence must end with a period.

2.3 Second Section

This section must be in two columns.

Each column must be 7,5-centimeter wide with a column spacing of 0,8-centimeter.

The section text must be set to 10-point, justified and linespace single.

Section, subsection and sub subsection first paragraph should not have the first line indent, other paragraphs should have a first line indent of 0,5-centimeter.

2.3.1 Section Titles

The heading of a section title must be 13-point bold in all-capitals, aligned to the left with a linespace exactly at 15-point, hanging indent of 0,7-centimeter and with an additional spacing of 24-point before (not applicable to the first title section of the paper) and 12-point after.

No dot should be included after the section title number.

2.3.2 Subsection Titles

The heading of a subsection title must be 12-point bold with initial letters capitalized, aligned to the left with a linespace exactly at 13-point, hanging indent of 1,0-centimeter and with an additional spacing of 11-point before (not applicable right after a section title) and 11-point after.

Words like “is”, “or”, “then”, etc should not be capitalized unless it is the first word of the subsection title.

No dot should be included after the subsection title number.

2.3.3 Sub Subsection Titles

The heading of a sub subsection title should be in 11-point bold with initial letters capitalized, aligned to the left with a linespace exactly at 12-point, hanging indent of 1,0-centimeter and with an additional spacing of 10-point before (not applicable right after a subsection title) and 10-point after.

Words like “is”, “or”, “then”, etc should not be capitalized unless it is the first word of the sub subsection title.

No dot should be included after the sub subsection title number.

2.3.4 Tables

Tables must appear inside the designated margins or they may span the two columns.

Tables in two columns must be positioned at the top or bottom of the page within the given margins. It is advisable the use of text boxes in this case.

Tables should be properly numbered, centered and should always have a caption positioned above it. Captions with one line should be centered and if it has more than one line should be set to justified. The

font size to use is 9-point. No bold or italic font style should be used. Spacing before and after should be of 12-point and 6-point, respectively.

The final sentence of a caption must end with a period.

Table 1: This caption has one line so it is centered.

Example column 1	Example column 2
Example text 1	Example text 2

Table 2: This caption has more than one line so it has to be set to justify.

Example column 1	Example column 2
Example text 1	Example text 2

Please note that the word “Table” is spelled out.

2.3.5 Figures

Please produce your figures electronically, and integrate them into your document.

Check that in line drawings, lines are not interrupted and have a constant width. Grids and details within the figures must be clearly readable and may not be written one on top of the other.

Figure resolution should be at least 300 dpi.

Figures must appear inside the designated margins or they may span the two columns.

Figures in two columns must be positioned at the top or bottom of the page within the given margins. It is advisable the use of text boxes in this case.

Please do not use indentation and set the figure layout to in line with text.

Figures should be properly numbered, centered and should always have a caption positioned under it. Captions with one line should be centered and if it has more than one line should be set to justified. The font size to use is 9-point. No bold or italic font style should be used. Spacing before and after should be of 6-point and 12-point, respectively.

The final sentence of a caption must end with a period.

Figure 1: This caption has one line so it is centered.

Figure 2: This caption has more than one line so it has to be set to justify.

Please note that the word “Figure” is spelled out.

2.3.6 Equations

Equations should be placed on a separate line, numbered and centered. An extra line space should be added above and below the equation.

The numbers accorded to equations must appear in consecutive order inside each section or within the contribution, with number enclosed in brackets and set on the right margin, starting with the number 1.

The use of a table with two columns is advisable.

Example:

$$a = b + c \tag{1}$$

2.3.7 Algorithms and Listings

Algorithms and Listings captions should be properly numbered, font size 9-point and no bold or italic font style should be used. Captions with one line should be centered and if it has more than one line should be set to justified.

2.3.8 Program Code

Program listing or program commands in text should be set in typewriter form such as Courier New.

Example of a Computer Program in Pascal:

```
begin
    Writeln('Hello World!!');
End.
```

The text must be aligned to the left with the linespace set to single and in 9-point type.

2.3.9 Reference Text and Citations

References and citations should follow the Harvard (Autor, date) System Convention (see the References section). As example you may consider the citation (Smith, 1998). Besides that, all references should be cited in the text. No numbers with or without brackets should be used to cite or to list the references.

References should be set to 9-point, justified, with a single linespace and hanging indent of 0,5-centimenter.

Citations should follow the section text format (see file FormatContentsForAuthors.pdf).

For more instructions about the references and citations usage please see the appropriate link at the conference website.

3 COPYRIGHT FORM

For the mutual benefit and protection of Authors and Publishers, it is necessary that Authors provide formal written Consent to Publish and Transfer of Copyright before publication of the Book. The signed Consent ensures that the publisher has the Author's authorization to publish the Contribution.

The copyright form is located on the authors' reserved area.

The form should be completed and signed by one author on behalf of all the other authors.

4 CONCLUSIONS

We hope you find the information in this template useful in the preparation of your submission.

ACKNOWLEDGEMENTS

If any, should be placed before the references section without numbering.

REFERENCES

Moore, R., Lopes, J., 1999. Paper templates. In *TEMPLATE'06, 1st International Conference on Template Production.* SCITEPRESS.

Smith, J., 1998. *The book*, The publishing company. London, 2nd edition.

APPENDIX

If any, the appendix should appear directly after the references without numbering, and not on a new page.

Appendix J – Springer book chapter publication guidelines

In accordance with the General Academic Rules of the North-West University (A.5.10.5), it is a requirement to include author guidelines for papers presented in a thesis. The author guidelines for the articles presented in Chapters 8 and 9, which were published or submitted for publication in a Springer book series, are presented here. The guidelines were obtained from the publisher website[20].

[20] ftp://ftp.springernature.com/cs-proceeding/svproc/guidelines/Springer_Guidelines_for_Authors_of_Proceedings.pdf

Guidelines for Authors of Papers to be Published in Springer Computer Science Proceedings

1 Scope of This Document

You will find here Springer's guidelines for the preparation of proceedings papers to be published in one of the following series:

- Lecture Notes in Computer Science (LNCS), incl. its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), and LNCS Transactions (contact: lncs@springer.com);
- Communications in Computer and Information Science (CCIS) (contact: ccis@springer.com);
- IFIP Advances in Information and Communication Technology (IFIP AICT), formerly known as the IFIP Series (ifip@springer.com);
- Lecture Notes of the Institute for Computer Sciences, Social Informatics and Tele-communications Engineering (LNICST) (lnicst@springer.com);
- Lecture Notes in Business Information Processing (LNBIP) (contact: lnbip@springer.com)

2 Preparation of Your Paper

Your contribution may be prepared in LaTeX or Microsoft Word. Please use the templates provided on the authors' page.
We need all source files (LaTeX files with all the associated style files, special fonts and eps files, or Word or rtf files) and the final pdfs of all of the papers. Please note that we cannot accept Framemaker files. LaTeX users should avoid self-defined environments and should provide references as Bbl files to avoid omission of data during conversion from Bib to Bbl. Please use the bibliographic style MathPhySci for computer science proceedings. It is not possible to have hyperlinks in references.

The volume editors, usually the program chairs, will be your main points of contact for the preparation of the volume.

2.1 Structuring Your Paper

Affiliations, Email-Addresses, and ORCIDs. The affiliated institutions, including town/city and country, are to be listed directly below the names of the authors. Multiple affiliations should be marked with superscript Arabic numbers, and they should each start on a new line. We encourage authors to insert their ORCIDs in superscript next to their names (please see the LaTeX and Word templates for examples).

The corresponding author, i.e., the author responsible for checking the final proof and for signing the copyright form on behalf of all of the authors, should be clearly

marked in the header of the paper. The inclusion of the corresponding author's email address is mandatory. In order to streamline communication during the publication process, there should not be more than one corresponding author per paper.

We strongly recommend that all authors include their email addresses in their papers. These will be used by Springer to provide authors with a personal MySpringer account (See Sect. 7), where they can download a free PDF of the entire proceedings volume.

Headings. Headings should be capitalized (i.e., nouns, verbs, and all other words except articles, prepositions, and conjunctions should be set with an initial capital) and should, with the exception of the title, be aligned to the left. Only the first two levels of section headings should be numbered, as shown in Table 1. The respective font sizes are also given in Table 1. Kindly refrain from using "0" when numbering your section headings.

Table 1. Font sizes of headings. Table captions should always be positioned *above* the tables.

Heading level	Example	Font size and style
Title (centered)	**Lecture Notes**	14 point, bold
1st-level heading	**1 Introduction**	12 point, bold
2nd-level heading	**2.1 Printing Area**	10 point, bold
3rd-level heading	**Run-in Heading in Bold.** Text follows	10 point, bold
4th-level heading	*Lowest Level Heading.* Text follows	10 point, italic

Words joined by a hyphen are subject to a special rule. If the first word can stand alone, the second word should be capitalized.

Here are some examples of headings: "Criteria to Disprove Context-Freeness of Collage Languages", "On Correcting the Intrusion of Tracing Non-deterministic Programs by Software", "A User-Friendly and Extendable Data Distribution System", "Multi-flip Networks: Parallelizing GenSAT", "Self-determinations of Man".

Lemmas, Propositions, and Theorems. The numbers accorded to lemmas, propositions, and theorems, etc. should appear in consecutive order, starting with Lemma 1. Please do not include section counters in the numbering like "Theorem 1.1".

2.2 Length of Papers

The most common types of papers accepted for publication are full papers (10–20+ pages) and short papers (6+ pages), where a page constitutes 300-400 words. We only wish to publish papers of significant scientific content. Very short papers (of fewer than 4 pages) may be moved to the back matter. Such papers will neither be available for indexing nor visible as individual papers on SpringerLink. They will, however, be listed in the Table of Contents.

2.3 Fonts

We aim to publish all proceedings papers in full-text xml. Our xml templates for LaTeX are based on CMR, our xml templates for Word are based on Times. We ask you to use the font according to the template used for your papers. Papers using other fonts will be converted by our typesetters.

2.4 Page Numbering and Running Heads

There is no need to include page numbers or running heads; this will be done at our end. If your paper title is too long to serve as a running head, it will be shortened. Your suggestion as to how to shorten it would be most welcome.

2.5 Figures and Tables

It is essential that all illustrations are clear and legible. Vector graphics (rather than rasterized images) should be used for diagrams and schemas whenever possible. Please check that the lines in line drawings are not interrupted and have a constant width. Grids and details within the figures must be clearly legible and may not be written one on top of the other. Line drawings are to have a resolution of at least 800 dpi (preferably 1200 dpi). The lettering in figures should not use font sizes smaller than 6 pt (~ 2 mm character height). Figures are to be numbered and to have a caption which should always be positioned under the figures, in contrast to the caption belonging to a table, which should always appear above the table. Figures and Tables should be cross referred in the text.

Captions are set in 9-point type. If they are short, they are centered between the margins. Longer captions, covering more than one line, are justified. Captions that do not constitute a full sentence, do not have a period.

If screenshots are necessary, please make sure that the essential content is clear to the reader.

Remark 1. In the printed volumes, illustrations are generally black and white (halftones). Colored pictures are welcome in the electronic version free of charge. If you send colored figures that are to be printed in black and white, please make sure that they really are also legible in black and white. Some colors show up very poorly when printed in black and white.

2.6 Formulae

Displayed equations or formulae are centered and set on a separate line (with an extra line or half line space above and below). Equations should be numbered for reference. The numbers should be consecutive within the contribution, with numbers enclosed in parentheses and set on the right margin. Please do not include section counters in the numbering. If you are using Word, please use the Math function of Word 2007, Word

2010 or Word 2013, or MathType or the Microsoft Equation Editor with Word 2003, to create your equations, and insert the math objects in your Word document in an editable format through MathType or MsWord equation editors.

$$x + y = z \tag{1}$$

Equations should be punctuated in the same way as ordinary text.

2.7 Footnotes

The superscript numeral used to refer to a footnote appears in the text either directly after the word to be discussed or – in relation to a phrase or a sentence – following the punctuation mark (comma, semicolon, or period).[1]

For remarks pertaining to the title or the authors' names, in the header of a paper, symbols should be used instead of a number (see first page of this document). Please note that no footnotes may be included in the abstract.

2.8 Program Code

Program listings or program commands in the text are normally set in typewriter font.

2.9 Citations by Number

Arabic numbers are used for citation, which is sequential either by order of citation or by alphabetical order of the references, depending on which sequence is used in the list of references. The reference numbers are given in brackets and are not superscript. Please observe the following guidelines:

- Single citation: [9]
- Multiple citation: [4-6, 9]. The numbers should be listed in numerical order.
- Sequential citation by order of citation: reference 7 cannot be cited before reference 5, for example.
- If an author's name is used in the text: Miller [9] was the first …

Please write all references using the Latin alphabet. If the title of the book you are referring to is, e.g., in Russian or Chinese, then please write (in Russian) or (in Chinese) at the end of the transcript or translation of the title. All references cited in the text should be in the list of references and vice versa.

If more than six authors are listed in one particular reference, this will be shortened and "et al." will be inserted.

In order to permit cross referencing within SpringerLink, and between different publishers and their online databases, Springer standardizes the format of the references according to the requirements for CrossRef (http://www.crossref.org/). The

[1] The footnote numeral is set flush left and the text follows with the usual word spacing.

reference section is included in the metadata of the paper on SpringerLink, increasing the visibility of the referenced papers and facilitating research considerably.

We strongly encourage you to include DOIs (Digital Object Identifiers) in your references. The DOI is a unique code allotted by the publisher to each online paper or journal article. It provides a stable way of finding published papers and their metadata. The insertion of DOIs increases the overall length of the references section.

2.10 Ethics and Permissions

If figures, tables, animations or text quotations from copyrighted works (including websites) are included in your paper, permission must be obtained from the copyright holder (usually the original publisher) and the author(s) for both the print and the online format, and full references must be included. Please take a look our Rights, permissions, licensing page for more details.

Papers submitted for publication must present original work by the authors themselves that has not previously been submitted or published elsewhere. Your paper may be checked by our plagiarism-checking tool on its arrival at Springer. We would encourage you to refer to the Publishing Ethics page on our website.

If, following publication, we find that plagiarism has been committed, the paper on SpringerLink is given a "retracted" stamp, and an erratum explaining the reasons for the retraction (i.e., plagiarism) is inserted. In addition, the volume editors and the author's academic supervisors are informed. Please note that a retracted paper remains visible, with its "retracted" stamp. It does not simply disappear.

2.11 Avoidance of Self-plagiarism

A certain overlap in scientific content between articles by the same author is standard practice and to be expected. However, it is essential that transparency is retained and appropriate references included. Permission must be obtained from other publishers, where appropriate.

3 Additional Information Required from Authors

3.1 Copyright Form

A semi-prefilled copyright form is usually available from the conference website. Please send your signed copyright form to your conference publication contact, either as a scanned PDF or by fax or by courier. The corresponding author (one per paper), who must match the corresponding author marked in the header of the paper, should sign the form on behalf of all of the authors of a particular paper, having gained their permission to do so. He or she signs for and accepts responsibility for releasing the material on behalf of any and all co-authors. Digital signatures are not acceptable. The corresponding author should be available to check the paper before it is published. Please note that once a paper has been delivered to Springer, changes relating to the

authorship of the paper cannot be made. Authors' names cannot be added or deleted, their order cannot be changed, and the corresponding author cannot be altered.

3.2 Correct Representation of Author Names

Authors' names should be written out in full in the header of the paper. They are shortened by us to "initials surname" in the running heads and take the form "surname, given name" in the author index. If you or any of your co-authors have more than one family name, it should be made quite clear how your name is to be displayed in the running heads and the author index. All authors should write their given names in front of their surnames at the tops of their papers. If you only have one (main) name, please make sure that this name is written out in full in the running heads, when you check your final PDF. Names and affiliations cannot be changed once a paper has been published. Also, if you have more than one paper in the volume, please check that your name has been written consistently throughout.

3.3 ORCID Identifier

Springer is the first publisher to implement the ORCID identifier for proceedings, ultimately providing authors with a digital identifier that distinguishes them from every other researcher. ORCID (Open Researcher and Contributor ID) hosts a registry of unique researcher identifiers and a transparent method of linking research activities to these identifiers. This is achieved through embedding ORCID identifiers in key workflows, such as research profile maintenance, manuscript submissions, grant applications and patent applications. Apply for an individual ORCID at www.orcid.org and include it in the header of your paper. Your ORCID will be replaced by the ORCID icon, which will link from the eBook to the actual ID in the ORCID database. As a result, only the ORCID icon will appear in the printed book.

3.4 Embedded Videos in Proceedings and Electronic Supplementary Material

Springer now offers authors the option of including embedded videos in their papers. Please refer to this page for the technical requirements. See here for an example of an animated figure.

Authors must not violate privacy and confidentiality rules and, as always, permission must be sought for use of third-party content. All types of Electronic Supplementary Material (ESM), including videos, should be sent with the authors' files. If videos are to be embedded, unequivocal instructions as to their positioning must be included. If no indication is given, the video will be stored at the end of the paper.
Slides that complement a paper may be included as ESM. We do not publish slides as an alternative to full scientific papers.

3.5 Data Publishing

Springer encourages authors to validate the results presented in their papers by means of data and, in addition to ESM, we can accommodate links to data or code within the papers published in our proceedings. If the conference organizers have chosen to make use of Springer Nature's figshare repository, authors will be asked to upload their data and code to a special branded area of this repository. Here are the branded areas for Euro-Par, TACAS, ISWC, and ECML PKDD, for example.

Permanent DOIs are assigned to the data and code stored in Springer Nature's figshare repository and links are set up between the paper on SpringerLink and the data or code. Authors of such papers should include a data citation in their references section (an example is given in the references section of this document) and a data availability statement in their paper. Details are provided by the conference organizers. The upload of the data to figshare is usually requested approximately one week before the final submission date for the papers.

4 Typesetting of Your Paper at Springer

Please make sure that the paper you submit is final and complete, that any copyright issues have been resolved, that the authors listed at the top of the chapter really are the final authors, and that you have not omitted any references. Following publication, it is not possible to alter or withdraw your paper on SpringerLink. Kindly note that we prefer the use of American English.

4.1 What Will Be Done with Your Paper

If the templates and instructions have been followed closely, then only very minor alterations will be made to your paper. The format of the paper will be checked by our typesetters, and if, for example, vertical spacing has been inserted or removed, then this will be remedied. In addition, running-heads, final page numbers, and a copyright line are inserted, and the capitalization of the headings is checked and corrected if need be. References not adhering to the style required for CrossRef (http://www.crossref.org/) are reformatted and, if available, DOIs (Digital Object Identifiers) are added. (We would encourage you to include DOIs in your references.) Light technical copyediting may also be performed.

4.2 Proof Reading Stage

Once the files have been worked upon, our typesetters send a copy of the final PDF of each paper to its corresponding author. The corresponding author is asked to check through the final PDF to make sure that no errors have crept in during the transfer or preparation of the files. Only errors introduced during the preparation of the files will be corrected. Particular attention should be paid to the references section.

If the typesetter does not receive a reply from a particular corresponding author, within the timeframe given (usually 72 hours), then it is presumed that the author has found no errors in the paper. The tight publication schedule of our proceedings does not allow us to send reminders or search for alternative e-mail addresses.

In some cases, it is the corresponding volume editor or the publication chair who checks all of the PDFs. In such cases, the authors are not involved in the checking phase.

The purpose of the proof is to check for typesetting or conversion errors and the completeness and accuracy of the text, tables, and figures. Substantial changes in content, e.g., new results, corrected values, title and authorship, are not possible and cannot be processed.

The proofs of the cover, inside-cover pages, front-matter pages and author index are sent to the volume editors.

5 Online Publication in SpringerLink

All Springer proceedings papers are published in our digital library, SpringerLink. Only subscribers to Springer's eBook packages or to the electronic book series are able to access the full-text PDFs of our online publications and the ePub full-text XML versions. Front and back matter, as well as abstracts and references, are freely available for all users. The online version of your paper will be available before the conference, unless the proceedings are to be published following the event. Please inform your conference contact if we need to delay the online date, because a patent application is underway.

6 Open Access and Open Choice

At Springer, we offer the option of open access publishing for entire proceedings volumes or for individual proceedings papers. The latter is referred to as "open choice". If you are interested in open choice, kindly inform your conference contact well in advance of publication. The conference contact will liaise with Springer and provide you with details of pricing and conditions. Springer will need your invoicing address and the CC-BY Consent to Publish form together with your final files.

7 MySpringer – A Service for Springer Authors and Editors

If you have included your email address in the header of your paper, you will receive an email from Springer (roughly four weeks after publication of the volume) linking you to your personal "MySpringer" page. From here, you will be able to download the pdf of the entire volume. You will find more details on this page. If the email address in the header is a life-long address, then Springer will be able to make all of your publications accessible from one single page.

Springer authors and volume editors are entitled to 40% off the list price of any Springer publication. Details on how to make use of this privilege are given on the author's "MySpringer" page.

8 Book Metrics

The book metrics for Springer publications are now available on Springer.com and SpringerLink. These give details on the number of citations, downloads, and readers at paper level and at book level. Please see Springer.com/bookmetrix for more details.

9 Checklist of Items to Be Sent to Your Conference Contact

- The final source files, incl. bbl files, images, etc. (no older source files)
- A final PDF file corresponding exactly to the final source files.
- A copyright form, signed by hand by the corresponding author on behalf of all of the authors of the paper.
- A suggestion for an abbreviated running head, if appropriate.
- Information about correct representation of authors' names, where necessary.

Acknowledgments. This should always be a run-in heading and not a section or subsection heading. It should not be assigned a number. The acknowledgments may include references to grants or support received in relation to the work presented in the paper. Authors should make sure that they have included all necessary acknowledgements before sending the files. Updates at a later stage are not possible.

Appendix

If a paper includes an Appendix, it should be placed in front of the references. If it has been placed elsewhere, it will be moved by our typesetters. If there is only one, it is designated "Appendix"; if there are more than one, they are designated "Appendix 1," "Appendix 2," etc.

Appendixes should be referred to in the text. The content of an appendix is contained within the sections subordinated to the major heading "Appendix." The language and styling rules for the text also apply to the appendixes. The form of numbering of tables, figures, and equations in an appendix should be the same as in the body of the article, continuing the numbering used there.

References (in MathPhySci, to be used for computer science proceedings)

1. Smith, T.F., Waterman, M.S.: Identification of common molecular subsequences. J. Mol. Biol. **147**, 195–197 (1981). doi: 10.1016/0022-2836(81)90087-5

2. May, P., Ehrlich, H.-C., Steinke, T.: ZIB structure prediction pipeline: composing a complex biological workflow through web services. In: Nagel, W.E., Walter, W.V., Lehner, W. (eds.) Euro-Par 2006. LNCS, vol. 4128, pp. 1148–1158. Springer, Heidelberg (2006). doi:10.1007/11823285_121
3. Foster, I., Kesselman, C.: The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, San Francisco (1999)
4. Czajkowski, K., Fitzgerald, S., Foster, I., Kesselman, C.: Grid information services for distributed resource sharing. In: 10th IEEE International Symposium on High Performance Distributed Computing, pp. 181–184. IEEE Press, New York (2001). doi: 10.1109/HPDC.2001.945188
5. Foster, I., Kesselman, C., Nick, J., Tuecke, S.: The physiology of the grid: an open grid services architecture for distributed systems integration. Technical report, Global Grid Forum (2002)
6. National Center for Biotechnology Information. http://www.ncbi.nlm.nih.gov
7. Nechaev, Y., Giuliano, C., Corcoglioniti, F.: SocialLink: knowledge transfer between Social Media and Linked Open Data. Figshare (2017), https://doi.org/10.6084/m9.figshare.5235823

Contribution Title

First Author[1][0000-1111-2222-3333] and Second Author[2][1111-2222-3333-4444]

[1] Princeton University, Princeton NJ 08544, USA
[2] Springer Heidelberg, Tiergartenstr. 17, 69121 Heidelberg, Germany
lncs@springer.com

Abstract. The abstract should summarize the contents of the paper in short terms, i.e. 150-250 words.

Keywords: First Keyword, Second Keyword, Third Keyword.

1 First Section

1.1 A Subsection Sample

Please note that the first paragraph of a section or subsection is not indented. The first paragraphs that follows a table, figure, equation etc. does not have an indent, either.

Subsequent paragraphs, however, are indented.

Sample Heading (Third Level). Only two levels of headings should be numbered. Lower level headings remain unnumbered; they are formatted as run-in headings.

Sample Heading (Forth Level). The contribution should contain no more than four levels of headings. The following Table 1 gives a summary of all heading levels.

Table 1. Table captions should be placed above the tables.

Heading level	Example	Font size and style
Title (centered)	**Lecture Notes**	14 point, bold
1st-level heading	**1 Introduction**	12 point, bold
2nd-level heading	**2.1 Printing Area**	10 point, bold
3rd-level heading	**Run-in Heading in Bold.** Text follows	10 point, bold
4th-level heading	*Lowest Level Heading.* Text follows	10 point, italic

Displayed equations are centered and set on a separate line.

$$x + y = z \tag{1}$$

Please try to avoid rasterized images for line-art diagrams and schemas. Whenever possible, use vector graphics instead (see Fig. 1).

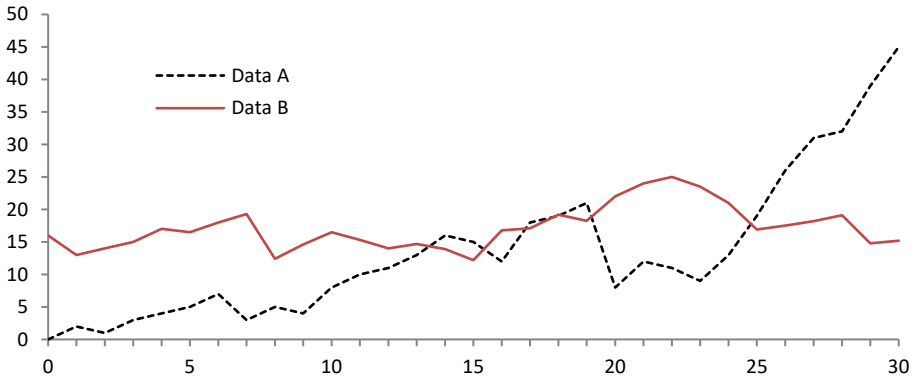


Fig. 1. A figure caption is always placed below the illustration. Short captions are centered, while long ones are justified. The macro button chooses the correct format automatically.

For citations of references, we prefer the use of square brackets and consecutive numbers. Citations using labels or the author/year convention are also acceptable. The following bibliography provides a sample reference list with entries for journal articles [1], an LNCS chapter [2], a book [3], proceedings without editors [4], as well as a URL [5].

References

1. Author, F.: Article title. Journal 2(5), 99–110 (2016).
2. Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016).
3. Author, F., Author, S., Author, T.: Book title. 2nd edn. Publisher, Location (1999).
4. Author, F.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010).
5. LNCS Homepage, http://www.springer.com/lncs, last accessed 2016/11/21.

Appendix K – Information security behavioural threshold analysis measurement instrument

The questionnaire that was developed to evaluate information security group behaviour in Chapter 6, is presented in this appendix.

Behavioural Thresholds in Information Security

Dear Respondent,

Thank you for your participation in completing this survey. The survey should not take more than 10 minutes.

The questionnaire forms the basis for a research project on behavioural thresholds in information security. This kind of research has never been done before in the context of information security and constitutes ground breaking and pioneering work in the field.

Participation in this survey is completely voluntary. The information provided by you in this questionnaire will be used for research purposes. The survey is completed anonymously and it cannot be used in a manner which would allow identification of your individual responses. The organisation you work for will also not be identified.

The following page provides more detail on the study and an informed consent form for participation.

Yours,

Dirk Snyman
Lecturer
Computer Science and Information Systems, North-West University
Email: dirk.snyman@nwu.ac.za
Contact number: +27 82 367 3778

* Required

Informed consent form (ICF)

RESEARCH STUDY: BEHAVIOURAL THRESHOLDS IN INFORMATION SECURITY

1. GENERAL: Participation in this study is voluntary. If you wish to decline or withdraw at any time, you may do so. If you agree to participate in the study, you are not likely to experience any risk or unique discomfort from answering these surveys. You will not receive any payment or direct personal benefit or reward from this research.

All participants will need to complete this ICF in order get access to the online surveys generated through Google Forms website. Once the online surveys are completed, the researcher will utilise the data for statistical summaries and other modes of analysis.

2. PURPOSE: The purpose of this study is to determine how the actions of people in a group influence the attitude and behaviour of an individual within the group in terms of information security. This study will ask you to complete a series of questions regarding an individual's personal inclination about certain information security related scenarios.

Should you have any questions before, during, or after your participation, please send an email to the researcher under CONTACT DETAILS below.

The results of this study will contribute to scientific knowledge and promote better management of information security within organisations, but will probably have no benefits or risks to you as a participant. The entire study should take less than 10 minutes to complete.

3. CONFIDENTIALITY: Any information that you provide will be kept strictly private, confidential, and anonymous. Your name will not be recorded with your survey responses in any way and as such no response can be connected to an individual. Results from this study will be presented as statistical summaries and other analysis results, but no information will be presented about individual participants/respondents.

4. CONTACT DETAILS:
Dirk Snyman
Lecturer
Computer Science and Information Systems, North-West University
Email: dirk.snyman@nwu.ac.za
Contact number: +27 82 367 3778

I give my consent to voluntarily participate in this study. I have read and understood the above information. *

☐ I agree

Biographic information

Organisational position *

Choose

Instructions

The overall goal of this study is to determine collective behaviour in the context of information security. In other words, how inclined people would be to follow the example of others. Your honest responses are important and there are no correct or incorrect answers.

The questionnaire should take no longer than 10 minutes to complete.

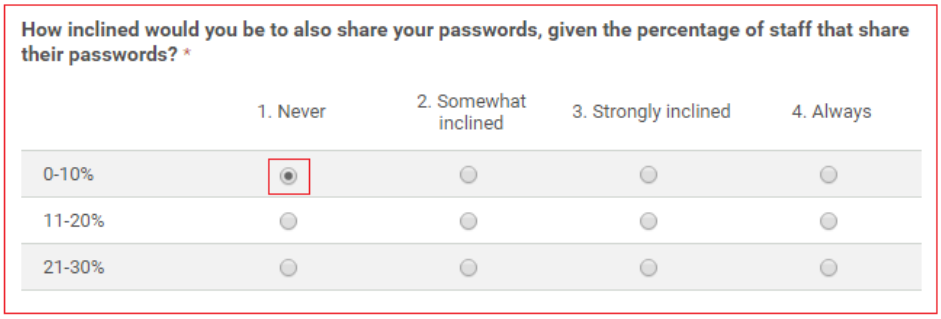
The purpose of the first six questions is to determine how inclined you would be to engage in similar behaviour of your colleagues given that you are aware of their behaviour or actions.

There are only six questions (as explained below) for six information security aspects, followed by eight short questions answered with only Yes, No or Unsure. These eight questions are used to measure patterns of thought and the influence it has on the inclination to follow the behaviour of others.

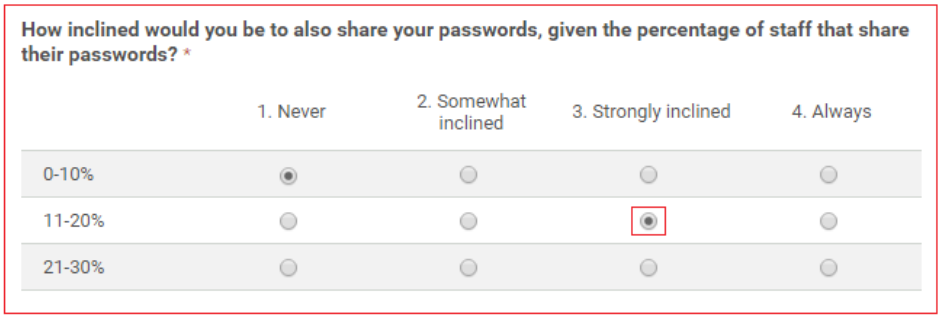
Each of the following six question is answered on a grid where you must indicate on a scale from 1 (Never) to 4 (Always) your inclination to act in the same way as your colleagues.

For example:

If 0-10% of your colleagues engage in password sharing, on a scale of 1-4, how inclined would you be to also share passwords.



and then, if 11-20% of your colleagues engage in password sharing, on a scale of 1-4, how inclined would you be to also share passwords.



Please answer the question for each interval from 0-100% for each of the six question grids.

1. Information security training

How inclined would you be to also complete voluntary information security training, given the percentage of staff that have completed voluntary information security training? *

	1. Never	2. Somewhat inclined	3. Strongly inclined	4. Always
0-10%	○	○	○	○
11-20%	○	○	○	○
21-30%	○	○	○	○
31-40%	○	○	○	○
41-50%	○	○	○	○
51-60%	○	○	○	○
61-70%	○	○	○	○
71-80%	○	○	○	○
81-90%	○	○	○	○
91-100%	○	○	○	○

2. Password management

How inclined would you be to also share passwords, given the percentage of staff that share their passwords? *

	1. Never	2. Somewhat inclined	3. Strongly inclined	4. Always
0-10%	○	○	○	○
11-20%	○	○	○	○
21-30%	○	○	○	○
31-40%	○	○	○	○
41-50%	○	○	○	○
51-60%	○	○	○	○
61-70%	○	○	○	○
71-80%	○	○	○	○
81-90%	○	○	○	○
91-100%	○	○	○	○

3. Social media use

How inclined would you be to also spend excessive work time on social media, given the percentage of staff that spend excessive work time on social media? *

	1. Never	2. Somewhat inclined	3. Strongly inclined	4. Always
0-10%	○	○	○	○
11-20%	○	○	○	○
21-30%	○	○	○	○
31-40%	○	○	○	○
41-50%	○	○	○	○
51-60%	○	○	○	○
61-70%	○	○	○	○
71-80%	○	○	○	○
81-90%	○	○	○	○
91-100%	○	○	○	○

4. Incident reporting

How inclined would you be to also ignore security incidents by not reporting them, given the percentage of staff that ignore security incidents and do not report them? *

	1. Never	2. Somewhat inclined	3. Strongly inclined	4. Always
0-10%	○	○	○	○
11-20%	○	○	○	○
21-30%	○	○	○	○
31-40%	○	○	○	○
41-50%	○	○	○	○
51-60%	○	○	○	○
61-70%	○	○	○	○
71-80%	○	○	○	○
81-90%	○	○	○	○
91-100%	○	○	○	○

5. Internet use

How inclined would you be to also access dubious websites from devices connected to your company network, given the percentage of staff that regularly access dubious websites from devices connected to your company network? *

	1. Never	2. Somewhat inclined	3. Strongly inclined	4. Always
0-10%	○	○	○	○
11-20%	○	○	○	○
21-30%	○	○	○	○
31-40%	○	○	○	○
41-50%	○	○	○	○
51-60%	○	○	○	○
61-70%	○	○	○	○
71-80%	○	○	○	○
81-90%	○	○	○	○
91-100%	○	○	○	○

6. Email use

How inclined would you be to also open any unfamiliar email attachments, given the percentage of staff that normally open any unfamiliar email attachments? *

	1. Never	2. Somewhat inclined	3. Strongly inclined	4. Always
0-10%	○	○	○	○
11-20%	○	○	○	○
21-30%	○	○	○	○
31-40%	○	○	○	○
41-50%	○	○	○	○
51-60%	○	○	○	○
61-70%	○	○	○	○
71-80%	○	○	○	○
81-90%	○	○	○	○
91-100%	○	○	○	○

7. General behavioural patterns

Thank you for completing the information security questions! Please answer the following eight short questions by only selecting Yes, No, or Unsure. As with the previous questions, these responses are completely anonymous. The purpose of these eight short questions is to try and match general behavioural patterns with actual behaviour. *

	Yes	No	Unsure
1. Are you always courteous, even to people who are disagreeable?	○	○	○
2. Are you always a good listener, no matter whom you are talking to?	○	○	○
3. Are you quick to admit making a mistake?	○	○	○
4. Have there been occasions when you took advantage of someone?	○	○	○
5. Do you sometimes try to get even rather than forgive and forget?	○	○	○
6. Do you sometimes feel resentful when you don't get your own way?	○	○	○
7. Are you always willing to admit when you make a mistake?	○	○	○
8. Have you sometimes taken unfair advantage of another person?	○	○	○

All done!

Optional: Is there any feedback that you would like to give the researchers? Please use the space provided below.

e.g. The process was difficult to understand, etc.

Your answer

Page 1 of 12

Get link

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Google Forms