Risk homeostasis as a factor in Information Security

WD Kearney

20020066

Thesis submitted for the degree *Philosophiae Doctor* in Computer Science at the Potchefstroom Campus of the North-West University

Promoter: Prof HA Kruger

October 2016

Acknowledgements

First and foremost I would like to thank God for allowing this body of work to take place.

I would like to express my sincere gratitude to my supervisor Prof. Hennie Kruger. His continuous support of this study and related research, his patience, motivation, and immense knowledge all made this possible.

Last but not the least, I would like to thank my family, especially my beautiful wife Michele for supporting me throughout this undertaking.

Preface

In accordance with rule A.5.1.1.2 of the "*General Academic Rules*" of the North-West University, this thesis is submitted in article format. Five articles are included in this thesis.

1. Kearney, W.D. and Kruger, H.A. 2013. A framework for good corporate governance and organisational learning – an empirical study. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 2(1):36-47.
2. Kearney, W.D. and Kruger, H.A. 2013. Phishing and organisational learning. *In* SEC2013, IFIP AICT 405, *eds.* Janczewski, L.J., Wolf, H. and Shenoi, S. p379-390.
3. Kearney, W.D. and Kruger, H.A. 2014. Considering the influence of human trust in practical social engineering. The 13th International Information Security for South Africa Conference (ISSA 2014).
4. Kearney, W.D. and Kruger, H.A. 2016. Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, 61:46-58.
5. Kearney, W.D. and Kruger, H.A. 2016. Theorising on risk homeostasis in the context of information security behaviour. *Information and Computer Security*. (Accepted for publication).

The co-author of the articles in the thesis, Prof HA Kruger (Promoter), hereby give permission to the candidate, Mr WD Kearney, to include the articles as part of a PhD thesis. The role of the co-author was kept within reasonable limits and comprises of critical feedback and discussion of ideas and concepts as well as general guidance to the candidate's research effort. This thesis therefore serves as fulfilment of the requirements for the PhD degree in Computer Science within the School of Computer, Statistical and Mathematical Sciences in the Faculty of Natural Sciences at the North-West University, Potchefstroom campus.

Abstract

Information security has become a complex human-driven science. There is widespread recognition of the fact that technology on its own no longer offers complete solutions to the information security problem and that the human aspect of information security is the most important determinant of information security success. Despite this acknowledgement and the large number of research projects that deals with the human aspects of information security, there are still no absolute solutions for what may seem to be very basic information security behaviour problems. The so-called privacy paradox or knowing-doing gap is a good example of a problem that remains something of a mystery. This type of problem refers to users with a high level of security awareness but who are easily persuaded to reveal confidential information (e.g. passwords) when asked for it. It therefore appears that the information security behaviour problem requires the use and implementation of new models, approaches and techniques to manage and understand information security risks and behaviour.

In this study that was conducted at a large, multi-billion dollar utility company with more than 3500 IT users and over 2 million customers, a number of human information security aspects were investigated. These studies have culminated into a recommendation that risk homeostasis as a theory should be considered as a factor in information security, both as an explanatory and a prediction framework for information security behaviour. An initial study had been performed to develop a framework to identify key dimensions in good corporate governance in order to ensure that appropriate objectives are identified and focused on. Practical social engineering (phishing) exercises were then conducted to indicate that information security behaviour often suffers from the privacy paradox. In an effort to understand this paradoxical information security behaviour, a trust survey was conducted and results were explained in terms of the practical phishing experiments. In addition, perceptual differences among users, information technology staff and management were analysed as another explanatory variable. Finally, these different research studies have led to a theoretical consideration of risk homeostasis as a theory that should be considered to explain and predict information security behaviour. This final study also deals with possible problems that may be associated with the risk homeostasis model (e.g. security fatigue) and suggests new approaches (e.g. the slower is faster effect and the automaticity of social behaviour assumption) as ways to deal with them.

The results of the various research activities have led to a number of contributions. The study opens up the prospect of theorising on risk homeostasis as a framework in information security behaviour that can be used to explain and predict information security behaviour, especially the contradictory behaviour of the privacy paradox. A value-focused approach has been developed to determine distinctive and unique security dimensions and objectives. It has been shown how practical security

incidents can create opportunities for organisational learning and, at the same time, empirical evidence has been provided to show the serious challenges that are presented by the privacy paradox. A trust survey confirms the important role that trust plays in information security problems such as the privacy paradox. An investigation into perceptual differences between different groups of people indicated that information security congruence is a prerequisite for a successful information security environment; this has led to a proposed new model for a safe and secure information environment. Finally, the results have contributed to the development of a better and more successful information security framework in the company under study.

Keywords: Risk homeostasis; information security awareness; information security behaviour; privacy paradox; value-focused approach; social engineering; organisational learning; trust; perceptual differences.

Declaration by language editor

HESTER A. VAN DER WALT

PO BOX 20252 NOORDBRUG 2522

Cell: 082 547 7016

ha.vanderwalt@gmail.com

19 April 2016

I hereby declare that I have done the language editing of

the *Abstract* as well as *Chapters 1, 2* and *8*

of the PhD thesis of

WD Kearney

Hester A. van der Walt

B.A.Hons. Practical Linguistics (UNISA)

B.Mus. (NWU)

Accredited member of SATI

SATI number: 1001208

Table of contents

Chapter 1 – Contextualisation and problem statement

Chapter 2 – Literature synopsis

Chapter 3 (Article 1) A framework for good corporate governance and organisational learning – an empirical study

Chapter 4 (Article 2) Phishing and organisational learning

Chapter 5 (Article 3) Considering the influence of human trust in practical social engineering exercises

Chapter 6 (Article 4) Can perceptual differences account for enigmatic information security behaviour in an organisation?

Chapter 7 (Article 5) Theorising on risk homeostasis in the context of information security behaviour

Chapter 8 Summary and conclusion

List of tables

Chapter 1 – Contextualisation and problem statement

Chapter 2 – Literature synopsis

Chapter 3 (Article 1) A framework for good corporate governance and organisational learning – an empirical study

Chapter 5 (Article 3) Considering the influence of human trust in practical social engineering exercises

Chapter 6 (Article 4) Can perceptual differences account for enigmatic information security behaviour in an organisation?

List of figures

Chapter 1 – Contextualisation and problem statement

Chapter 3 (Article 1) A framework for good corporate governance and organisational learning – an empirical study

Chapter 4 (Article 2) Phishing and organisational learning

Chapter 5 (Article 3) Considering the influence of human trust in practical social engineering exercises

Chapter 6 (Article 4) Can perceptual differences account for enigmatic information security behaviour in an organisation?

Chapter 7 (Article 5) Theorising on risk homeostasis in the context of information security behaviour

Chapter 8 Summary and conclusion

Chapter 1

Contextualisation and problem statement

If you think technology can solve your security problems, then you don't understand the problems and you don't understand technology. (Bruce Schneier)

1.1 Introduction

Chapter 1 serves as an introduction and guides the reader into the research project by presenting and explaining the following:

- Background and contextualisation
- Problem statement
- Research aims and objectives
- Research paradigm, design and methodology
- Thesis layout and structure
- Contribution of the study

The thesis is submitted in article format; therefore, each article in the subsequent chapters has their own references as part of the article. At the end of Chapter 1, a reference section for literature sources that have been used specifically in this chapter will thus be presented.

1.2 Background and contextualisation

Information security has become a complex human-driven science. Although technology plays a significant role in protecting information and information-related assets, it is very often the human aspect of information security that determines the success of information security campaigns. It is widely acknowledged that information security has become a function of human aspects such as knowledge, attitude and behaviour; this is a well-researched topic (Frangopoulos et al., 2014; Furnell and Clark, 2012; Parsons et al., 2010; Safa et al., 2016).

In an effort to address human behaviour in information security, some researchers argue that the solution lies in the existence and quality of an information security policy (Bulgurcu et al., 2010; Ifinedo, 2014; Sommestad et al., 2014). An area that is closely related to information security policies and the compliance of such policies is information security awareness. Studies on information security awareness often concentrate on how to raise information security awareness (Alnatheer, 2015; Da Veiga, 2015), how to measure these levels (Chandrashekar et al., 2015; Keser and Gulduren, 2015), and how to monitor and manage the security awareness levels (Rantos et al., 2012; Spandonidis, 2015).

Studies that deal with information security awareness and policies often lead to more research projects that focus on security culture. There exist a significant number of studies in this area, including research

on information security culture definitions (Alhogail and Mirza, 2014); information security culture frameworks (Alhogail, 2015); the information security culture assessment process (Da Veiga and Martins, 2015); and critical success factors for an information security culture (Alnatheer, 2015).

Another trend in information security research is that researchers and decision makers tend to use psychological, sociological and other models from the social sciences in an effort to gain more insight into the intricacies of human information security behaviour (Crossler et al., 2013; Enrici et al., 2010; Tsohou et al., 2015). There are a number of these theories that are regularly applied in the context of information security. According to Lebek et al. (2013), the primary behavioural theories (based on the number of publications) are the theory of reasoned action (TRA), the theory of planned behaviour (TPB), the general deterrence theory (GDT) and protection motivation theory (PMT). The TRA and TPB frameworks concentrate on a user's behavioural intention and are often combined with other theories to explain aspects of information security awareness (Gundu and Flowerday, 2013) or information security policy compliance (Bulgurcu et al., 2010; Ifinedo, 2012; Siponen et al., 2007). The GDT and PMT theories are based on fear and fear-arousing communication and are also regularly applied in information security behaviour studies (Crossler, 2010; D'Arcy et al., 2008; Herath and Rao, 2009a; Jansen, 2015). Another theory that falls within the category of psychological models is the risk homeostasis framework, which is a behavioural adaptation theory that was introduced by Wilde (1994). According to this theory, people will accept a certain level of risk until the situation changes, for example by introducing new or additional safety measures. People will then change their behaviour to compensate for a change in risk levels. There is, surprisingly, little in literature on risk homeostasis in the context of information security. Pattinson and Anderson (2004) performed a short and introductory study on this, whereas Stewart (2004) also refers to risk homeostasis in his recommendations on how to treat risk. Other researchers mention risk homeostasis only briefly as a possible theory to explain information security behaviour (Albrechtsen and Hovden, 2009; Parsons et al., 2010). It appears that the features offered by the risk homeostasis model, as well as the similarities it bears to other regularly studied psychological models, do offer new and additional opportunities to information security researchers and decision makers to understand and manage risky and paradoxical behaviour of information technology users. It is also clear that this approach has not been explored sufficiently by information security specialists.

There are a myriad of other human factors that are also studied regularly in the context of information security, either on their own or combined with other theories and factors. One of the prominent human factors is trust. Jensen (2015) states that trust may be considered as a soft security property that interacts with other perceptual, attitudinal and behavioural factors. Trust therefore seems to be a key element in information security behaviour and examples of studies pertaining to trust can be found in Shaik and Sasikumar (2015) and Sicari et al. (2015). Closely related to the behavioural theories that have been

mentioned earlier are factors such as fear (Bada and Sasse, 2014) and penalties (Herath and Rao, 2009b). Parsons et al. (2010) performed a study on the human factors in information security and listed a number of factors that may influence a user's perception of risk, for example the availability heuristic, optimism bias and omission bias. The role of these and other cognitive biases has also been studied by other researchers (Tsohou et al., 2015).

Based on the introductory comments above, it is clear that the different theories, models and factors pertaining to the human aspects of information security receive a lot of attention and are well researched. However, despite these comprehensive efforts, there still exists a concept such as the "privacy paradox" (Kokolakis, 2015) or the "knowing-doing gap" (Cox, 2012). This concept refers to users with a high level of security awareness and appropriately sufficient information security knowledge, but who are easily persuaded to reveal confidential information (e.g. passwords) when asked for it. It may take only one incident of social engineering to prove the privacy paradox. The latter brings social engineering (and specifically phishing) to the forefront as another security risk that is directly linked to human information security behaviour. Although it is a real threat that can cause serious damage, it has also become an opportunity for training and raising of security awareness levels. The use of practical tests has become popular as an effective way in making users aware of the dangers of phishing and social engineering. Examples of such practical phishing experiments can be found in Dodge et al. (2007), Hasle et al. (2005), Jagatic et al. (2007) and Steyn et al. (2007). Practical phishing tests should, however, not be limited to a mere count of users who were caught, but should rather be aimed at understanding behaviour and creating a climate for learning. Albrechtsen (2003) contends that these types of security incidents and experiments present great opportunities to learn and improve information security.

Whilst this study is concerned with the human aspect of information security, it is noteworthy that technology may also play a role in human behaviour. The cost of acquiring new technology and the ease with which technological solutions can be used are examples of how technology may impact on information security behaviour. New technology brings new challenges and one of the concepts that are of particular interest to information security is disruptive technology. This refers to new ways of doing things that disrupt or overturn traditional business methods and practices (Business Dictionary, 2015). An example is the internet in the age of post office mail – this clearly implies new security threats that require different security behaviours. Gartner (2015) confirms the importance of disruptive technology and lists risk-based security and self-protection as a new information technology reality that emerges as part of the top 10 strategic technology trends for 2015.

Given the above introductory background and contextualisation, this study was designed to investigate a number of security aspects; it eventually culminated, though, in a recommendation that risk homeostasis as a theory should be considered as a factor in information security, both as an explanatory

and as a prediction framework for information security behaviour. The specific issues that were addressed and investigated will be detailed in the problem statement section (Section 1.3), but in summary, the study included the following: An initial study had been performed to develop a framework to identify key dimensions in good corporate governance in order to ensure that appropriate objectives are identified and focused on. Practical social engineering exercises were then conducted to indicate that information security behaviour often suffers from the privacy paradox. In an effort to understand this paradoxical information security behaviour, a trust survey was conducted and results were explained in terms of the practical phishing experiments. In addition, perceptual differences among users, information technology staff and management were analysed as another explanatory variable; this resulted in a proposed safe and secure information security model. Finally, these different research studies have led to a theoretical consideration of risk homeostasis as a theory that should be considered to explain and predict information security behaviour. This final study also deals with possible problems that may be associated with the risk homeostasis model (e.g. security fatigue) and suggests new approaches (e.g. the slower is faster effect and the automaticity of social behaviour assumption) as ways to deal with them. All empirical work was carried out at a large, geographically dispersed utility company (detailed in Section 1.5). The ensuing sections will formalise the contextualisation that are presented here into a problem statement and research objectives.

1.3 The problem statement

Information security is a function of technology and human aspects. Despite numerous technical advances in the field of information technology, human behaviour remains the principle determinant of information security. Safa et al. (2016) emphasise that modern-day organisations should take the human aspects of information security into consideration if they want to mitigate the risk of security incidents. Guidelines offered by them include information security knowledge sharing; collaboration; conscious care behaviour; and complying with information security policies. The human aspect of information security has been widely acknowledged and there are a significant number of studies that call for a more holistic approach to information security (Soomro et al., 2016) or studies that attempt to provide new directions and guidelines for behavioural information security research (Crossler et al., 2013). With this in mind, together with the motivating contextualisation in Section 1.2, this study aims to investigate various human aspects of information security in an effort to provide new insights into the challenges of problems such as the privacy paradox.

1.3.1 The research question

This study is guided by the following primary research question:

Is the understudied risk homeostasis theory (in the context of information security) a factor that can explain the paradoxical information security behaviour of users?

According to Pattinson and Anderson (2004), risk homeostasis is a management theory and the essence of information security is to manage risk. However, apart from the short paper by these authors, there is very little in literature on risk homeostasis in the context of information security.

1.3.2 The research sub-questions

The primary research question in Section 1.3.1 is supported by four additional research sub-questions. These sub-questions were formulated to facilitate the research activities that ultimately led to the achievement of the study's objectives.

The four sub-questions are as follows:

(i) *What are the appropriate dimensions of good corporate governance?*

A framework is needed in order to ensure that the correct and appropriate high-level objectives from a risk perspective are identified and to confirm that information security is indeed one of the fundamental areas of good corporate governance. This sub-question provides the foundation for the research in the problem domain.

(ii) *Can practical social engineering experiments be used as an indication of human behaviour and at the same time initiate an organisational learning process?*

This sub-question is intended to show that despite the comprehensive security awareness efforts, there still exist significant (and perhaps serious) challenges in the information security area, for example the privacy paradox. Furthermore, to ensure that specific security incidents do not become a once-off event, the research sub-question also suggests that organisations could make use of various organisational learning models to enhance the awareness and educational value of such practical experiments.

(iii) *Does human trust play a role in the privacy paradox?*

One of the salient aspects of information security that is linked to humans is trust. The purpose of sub-question three is to consider the influence of human trust in practical social engineering exercises in order to determine whether or not it plays a role in the privacy paradox.

(iv) *Are perceptual differences significant in information security behaviour?*

The last sub-question provides an opportunity to further explain and understand the contradictory behaviour of people. By analysing the risk perceptions of different groups of people, it becomes possible to suggest a safe and secure information model that is based on information security congruence between groups of people.

Each of the four research sub-questions contributes to the realisation of the primary research question on risk homeostasis as a factor in information security. Figure 1.1 depicts the relationship between the sub-questions and the way in which this relationship applies to the overall research objective.

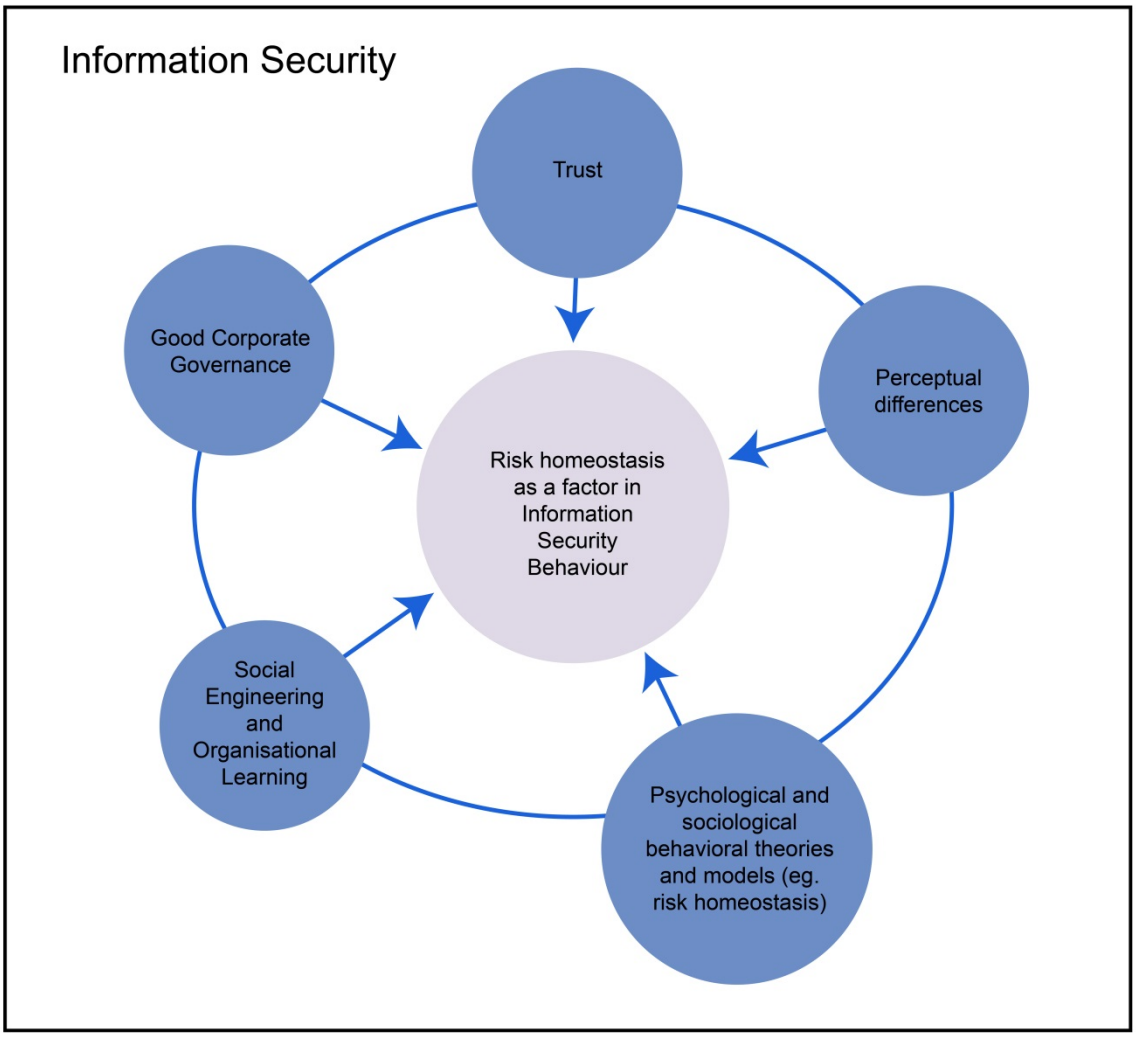


Figure 1.1: High-level relationship between the primary research problem and sub-problems

1.4 Research aims and objectives

The research questions that have been formulated in Section 1.3 can be translated into the following formal objectives of the study:

The primary objective is to research the link between risk homeostasis and aspects of information security and information security behaviour. To achieve the primary objective, the following secondary objectives will be addressed:

- The construction of an appropriate framework that can be used to identify unique dimensions of good corporate governance
- A demonstration of how a security incident (social engineering) can create opportunities for organisational learning
- An investigation into the role of trust as a possible explanatory variable in the privacy paradox

- A study of the influence of perceptual differences in contradictory information security behaviours

1.5 Research paradigm and methodology

According to Collis and Hussey (2014), a "research paradigm is a framework that guides how research should be conducted based on people's philosophy and their assumptions about the world and the nature of knowledge". Accordingly, Section 1.5 maps out the plan or framework that was used to construct the proposed solutions to the primary and secondary research objectives.

The metaphor of the research onion (Saunders et al., 2003) is used to illustrate how the core of the research was considered in relation to the different research design elements (the layers of the research onion). Saunders's research onion was adapted and used in the form suggested by Durandt (2015). A graphical depiction of this adapted form is shown in Figure 1.2.

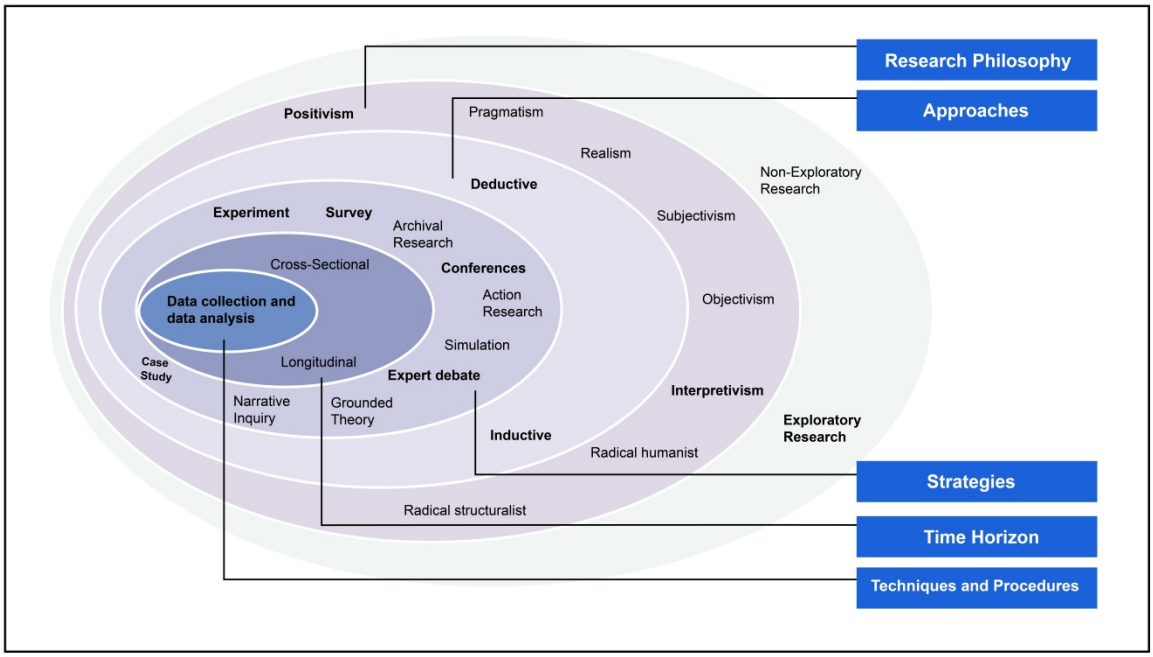


Figure 1.2: The research onion (Durandt, 2015)

The subsequent sub-sections will describe each layer briefly as it applies to this study.

1.5.1 Exploratory research

The purpose of the inquiry into the research design of this study is characterised by exploration. Exploratory research is the most useful in problems that address a subject where there is a significant level of uncertainty, in other words, where there is very little existing research on the subject matter (Van Wyk, nd). According to Van Wyk, typical questions asked in exploratory studies are, "What are the critical success factors of ...?", "What are the distinguishing features of ...?" and "What are the

reasons for ....?" As the very outer layer of the research onion, exploratory research is therefore appropriate for the topic studied in this research project, as there is very limited research on the subject matter (namely risk homeostasis in the context of information security). Furthermore, the research sub-questions (Section 1.3.2) were designed to answer exploratory questions such as "What are the factors, the reasons and the features in the privacy paradox and how does the risk homeostasis theory relate to it?"

1.5.2 Research philosophy

This study adopted a combination of the positivist philosophy and the interpretivist philosophy. Positivism maintains that the world is ordered and can be studied objectively (Oates, 2006). It is generally associated with empirical knowledge and data collection methods may include surveys, experiments and numerical methods. In contrast to this, interpretivist research is characterised by the existence of multiple realities (Oates, 2006) and focuses on exploring subjective and often ambiguous facts surrounding human actions and understanding. The research questions in this study require empirical knowledge that has been obtained from respondents, as well as the interpretation of qualitative data from interviews. There is also a strong pragmatic approach that allows for a combination of qualitative and quantitative methods (Teddlie and Tashakkori, 2003).

1.5.3 Research approach

Although there are elements of a deductive approach in this study, the primary approach leans towards a more inductive approach. Saunders et al. (2003) state that an inductive approach is where one would collect data and develop a theory as a result of the data analysis. In addition, they argue that the inductive approach would be particularly concerned with the context in which events are taking place and that a study of a small sample of subjects might be more appropriate.

Owing to the presence of both deductive and inductive elements, a mixed-methods research design was implemented. A mixed-method approach is explained by Creswell (2003) as one in which the researcher tends to base knowledge claims on pragmatic grounds. It employs strategies of inquiry that involve the collection of data, either simultaneously or sequentially, to best understand research problems. The data collection also involves the gathering of both numeric information and text information, in other words, both quantitative and qualitative information.

1.5.4 Research strategies

The research strategies employed in this study utilise a number of different approaches and techniques. A case study approach was followed, as empirical work was carried out at a large utility company. Saunders et al. (2003) state that the case study approach has considerable ability to generate answers to the questions, "Why?", "What?" and "How?" Other strategies include practical experiments (e.g. to

investigate social engineering) as well as surveys (e.g. to gauge trust levels and to determine perceptual differences). Conferences and expert debate also form a significant part of the research strategies. Some of the concepts and related work have been presented since 2005 (see Table 1.1, Section 1.5.6), whereas some of the work has also been published prior to the start of the formal study (see Table 1.1, Section 1.5.6). During the formal study, research results were also presented at conferences and published in journals (see Table 1.1, Section 1.5.6). All these research outlets present excellent opportunities to perform exploratory research by means of international reviewer comments and personal networking events. Expert debate was a very useful strategy, as literature on the primary objective (namely risk homeostasis in information security) was not readily available. Apart from feedback received from reviewers and other networking opportunities, there were also ongoing informal discussions with business colleagues and formal discussions with respondents and management in the company under study.

1.5.5 Time horizon

The empirical work performed in this study may be regarded as a cross-sectional (short-term) study. During the practical social engineering experiments, the trust survey and the perceptual differences survey, an information snapshot was taken – this information represented a cross-sectional set of information. However, the experiments were performed over a period of time; for example, a first social engineering experiment was followed-up after a couple of months to determine whether there was a change in behaviour or not. In an effort to explain the observed security behaviour, a trust survey was conducted and later on followed by a perceptual differences survey. Taking this into account, the information could also be described as longitudinal (i.e., research over a longer period of time).

The topic of security awareness and behaviour had been studied since 2005. These studies formed the basis and preparation for the formal study that commenced in 2013. To put the amount of work into context, some of the more significant research results prior to the formal study are also given here (Table 1.1).

The timeline of the study can be summarised as follows:

Pre-preparatory studies	**Purpose**	**Output results**
2005-2012	Application of an information security awareness measuring tool in a mining environment	Kruger, HA and Kearney, WD. Measuring information security awareness: A West Africa gold mining environment case study. Information Security South Africa (ISSA) conference. (2005).

	Further demonstration of the model to measure information security awareness levels	Kearney, WD and Kruger HA. The development and application of a model to measure information security awareness. *In* Proceedings of the CACS2005 Oceania Conference. ISBN: 1-86308-124-0. Perth, Western Australia. (2005).
	Development of a general framework that can be used for measuring security awareness levels	Kruger, HA and Kearney, WD. A prototype for assessing information security awareness. Computers & Security, 25:289-296. (2006).
	Identification of the most important areas to include in an information security awareness programme	Kruger, HA and Kearney, WD. Consensus ranking – an ICT security awareness case study, Computers & Security, 27:254-259. (2008).
	Use of a value-focused approach to develop a framework for good corporate governance	Kruger, HA and Kearney, WD. Effective corporate governance – a case study using a value-focused approach, *In* Proceedings of the 21st Conference of the South African Institute for Management Scientists (SAIMS). (2009).
Formal research project	**Purpose**	**Output results**
2013	A value-focused approach to identify unique dimensions to be evaluated in good corporate governance	Kearney, WD and Kruger, HA. A framework for good corporate governance and organisational learning – an empirical study. International Journal of Cyber-Security and Digital Forensics, 2(1):36-47. (2013). *(Chapter 3)*
2013	Showing how a security incident (social engineering) can create opportunities for organisational learning	Kearney, WD and Kruger, HA. Phishing and organisational learning. LJ Janczewski, HB Wolfe and S Shenoi (*Eds.*): Security and Privacy Protection in Information Processing Systems, SEC2013, IFIP AICT 405, (Springer), pp. 379-390. *(Chapter 4)*
2014	Investigation of the role of trust in security breaches	Kearney, WD and Kruger, HA. Considering the influence of human trust in practical social engineering exercises. Information

		Security South Africa (ISSA) conference. (2014). *(Chapter 5)*
2015-2016	Investigation of perceptual differences as an explanatory variable in information security behaviour and proposition of a safe and secure information security model	Kearney, WD and Kruger, HA. Can perceptual differences account for enigmatic information security behaviour in an organisation? Computers & Security, 61:46-58. (2016). *(Chapter 6)*
2015-2016	Putting risk homeostasis in perspective in the context of information security behaviour and creating an opportunity to theorise and provide new insights to strategic security decision makers	Kearney, WD and Kruger, HA. Theorising on risk homeostasis in the context of information security behaviour. Information and Computer Security (Accepted 2016). *(Chapter 7)*

Table 1.1: Timeline of the study

1.5.6 Data collection and data analysis

The final layer of the research onion is concerned with the practicalities of data collection and data analysis. A number of data sets were generated during the study. These data sets include qualitative data to construct the framework for good corporate governance; quantitative data for the two social engineering exercises; and a mix of quantitative and qualitative data pertaining to the trust and perceptual differences surveys. The final research output on risk homeostasis in the context of information security was based on literature sources and the data generated from the other experiments and surveys. It should be noted again that each research question was reported in a peer-reviewed paper and that the data collection and data analysis for each one of them were detailed in the respective papers (Chapters 3-7 in the dissertation). This section will therefore only present a high-level summary of the data collection and analysis activities.

The study was conducted at a large, multi-billion dollar entity with more than 3 500 IT users and supplying essential services to over 2 million customers. To put the size of the company further into perspective, it is noteworthy to mention that during the last financial year, it had over 750 million AU$ in capital works and over 850 million AU$ in direct operating expenditure. With regard to its external IT presence, the company recorded 1.4 million visitors to its website and answers over 800 000 telephone calls from customers annually. The company was selected for the following reasons:

- It is a large company.
- The company makes use of state-of-the-art technology.
- The workforce is relatively well educated.

- The company maintains an excellent information security awareness and training programme for all employees.
- Top management supports and has bought into the research project.
- The organisation already has an ongoing program of internal control testing including phishing exercises and penetration attacks.

Participants in the research activities were users and employees of the company under study. Sample sizes for the different tests and surveys were determined in the following way:

- The corporate governance study: Seven senior staff members (ranging from managers to directors) were interviewed. This sample size was determined by a "saturation point", which is a standard stopping rule for qualitative research. Glaser and Strauss (1967) use the term "theoretical saturation", which means that no additional data are found by the researcher for a specific category in a study. It is, of course, true that one would never know whether the next interviewee would be able to provide new information or not (which is also true in the case of questionnaires). Statistically speaking, it might also be argued that the sample size is not sufficient. It was, however, decided to keep to the generally accepted qualitative procedure, utilising the saturation-point stopping rule. The nature of the project in which a value-focused analysis was performed does not require many responses from many different respondents.
- The two social engineering tests: All employees received a phishing email message. In this case, the tests were not performed on a sample but rather on the complete population.
- The trust survey: A sample size of 40 users was selected, based on recommendations and input from management. This sample size was also large enough to comply with the saturation-point stopping rule.
- The perceptual differences survey: A sample size of 60 people was chosen. This group was divided into three separate groups of 20 each, representing management, IT staff and users. The decision to involve 60 participants was motivated by similar studies in literature, all using less than 60 participants (see Chapter 6); this was also in line with management recommendations.

Data collection for the different tests and surveys were carried out as follows:

- The corporate governance study: Interviews were conducted by using four broad and open questions that have been suggested by Keeney (1994). These questions were specifically developed by Keeney for studies using the value-focused thinking technique. The four questions are the following (details are in Chapter 3):
    i. What would you regard as important aspects in good corporate governance?
    ii. What would you do or implement to ensure that the application of corporate governance principles is effective?

iii. What are your current concerns regarding effective application of corporate governance principles?

iv. If you have to evaluate the effectiveness of the application of corporate governance principles, how would you do it and how would you know that it is acceptable?

- The two social engineering tests: A phishing email was used. Users were requested to click on a link that would take them to a webpage; here they were asked for their user identification and password. (See Appendixes A and B for the complete email messages.)
- The trust survey: A questionnaire, consisting of 20 questions that are based on management input and certain literature sources, was used (Appendix C). To ensure an appropriate response and to comply with the requirements of a saturation-point stopping rule, the questionnaires were completed on an interview basis. An additional advantage of this approach was that the questions could be explained to respondents; in doing it this way, it could be ensured that all respondents understood the questions in the same manner.
- The perceptual differences survey: A questionnaire that contains 11 questions was completed on an interview basis (Appendix D). The interview protocol that was used is shown in Figure 1.3 below.

Interview protocol

The high-level interview framework that was used during interviews with participants is summarised as follows:

1. Explain to the participant that he/she was selected to take part in a research project on information security and that the selection was influenced by senior management. However, the only influence by senior management was the guidance of a stratification process and their selection was based on random selection from an organisational chart.
2. Explain the goal of the research, namely to gauge perceptions on information security that may ultimately help to explain the privacy paradox. Furthermore, explain that the purpose of the research project is also to evaluate perceptions of respondents to determine whether or not a form of digital divide exists at the organisation. The project forms part of a broader project that investigates possible theories that can be used to explain why social engineering experiments have such levels of success.
3. Explain that the interview will last approximately 30 minutes and consists of a questionnaire containing 11 questions. There are no right or wrong answers and participants may ask for explanations/clarifications at any time.
4. Explain that participation is voluntary and that all responses will be held in strict confidentiality. No reference will be made to any person and results will only be reviewed by the researchers. The persons may also exclude themselves at any time without being penalised.
5. Obtain explicit and informed consent from the participant. Ensure that the consent form is signed.
6. Go through and complete the questionnaire, explaining or answering any questions that the participant may have.
7. Express your thankfulness to and appreciation for the respondent and emphasise that without his/her contribution, the research project cannot be successful. Ensure that the respondent understands that his/her responses will help guide the development of a better and more successful information security framework for the organisation.

Figure 1.3: Interview protocol

Data analysis in some of the research activities was based on a mere count of responses. The qualitative data obtained through interviews in the corporate governance exercise were analysed according to the general technique that is suggested for a value-focused thinking process, that is, to determine means and fundamental objectives (Keeney, 1994). (This technique is detailed in Chapter 3.) Where it was

deemed necessary, appropriate statistical techniques were used in the analysis. Such techniques include basic one-way analysis of variance (ANOVA) tests and the use of effect sizes to determine differences in responses. (The effect size metric is explained in Chapter 7.)

1.6 Ethical considerations

Ethical clearance and top management approval were obtained from the company under study. This was achieved by conducting personal meetings with the CEO, CFO and IT Manager where the purpose, actual steps and possible outcomes of all the tests and surveys were explained. Written consent was given by the CEO (Appendix E). Participation in the study was optional and completely voluntary. All participants signed the measuring instruments used to give their informed consent (example of consent form is included in Appendix D). In addition, the research project was committed to ensure adherence to the following ethical considerations, listed by Allam (2014):

- Ensure that all individuals, entities and reputations included in the research project were assured of privacy and anonymity.
- Ensure the accuracy of all primary data to the highest level of reasonable assurance.
- Ensure that proper recognition was accorded to the original author or owner of all external contributions.
- Ensure that any unanticipated ethical considerations outside of the above were properly evaluated and fairly resolved before their inclusion.

1.7 Thesis outline and structure

This thesis is structured and presented in article format as approved by the North-West University (Potchefstroom Campus) – see also the Preface on page ii. The outline of the thesis is as follows:

Chapter 1: Contextualisation and problem statement

Chapter 1 presents the overarching purpose of the research project, including the problem statement. The chapter introduces the background and contextualisation of the study as well as the research aims and objectives, and the research paradigm and methodology. Ethical considerations are highlighted and attention is paid to the contribution of the study.

Chapter 2: Literature synopsis

Normally, a thesis that is presented in article form has an additional literature review chapter if literature sources for the different articles are not sufficient. In this thesis, comprehensive literature references are provided for each article as well as for Chapter 1. An additional literature review is therefore deemed unnecessary. This chapter presents a high-level summary of literature sources per article and per chapter.

Chapter 3 (Paper 1): A framework for good corporate governance and organisational learning – an empirical study

This chapter is presented in the form of a manuscript that has been published in the International Journal of Cyber-Security and Digital Forensics. The guidelines of this journal are presented in Appendix F.

Chapter 4 (Paper 2): Phishing and organisational learning

Chapter 4 is presented in the form of a manuscript that has been published in Security and Privacy Protection in Information Processing Systems, SEC2013, IFIP, AICT405 (Springer). Author guidelines are presented in Appendix G.

Chapter 5 (Paper 3): Considering the influence of human trust in practical social engineering

This chapter is presented in the form of a manuscript that has been published in Proceedings of the Information Security for South Africa (ISSA), 2014. Author guidelines are presented in Appendix H.

Chapter 6 (Paper 4): Can perceptual differences account for enigmatic information security behaviour in an organisation?

Chapter 6 is presented in the form of a manuscript that has been published in Computers and Security. The guidelines of the journal are presented in Appendix I.

Chapter 7 (Paper 5): Theorising on risk homeostasis in the context of information security behaviour

Chapter 7 is presented in the form of a manuscript that has been accepted for publication by the journal Information and Computer Security. The guidelines of the journal are presented in Appendix J.

Chapter 8: Conclusion

The final chapter of the thesis presents a synopsis of the study and shows how the research objectives were achieved. Limitations of the study and recommendations for further research are also highlighted.

It should be noted that references in Chapters 3-7 are presented according to the requirements of the specific author guidelines of the journals in which the papers were published.

1.8 Contribution of the study

There are multiple unique contributions of this study.

The main and overall contribution is that the study opens up the prospect to theorise on risk homeostasis as a framework in information security behaviour and information security culture that can be used as a model to explain and predict information security behaviour – especially the contradictory behaviour

of the privacy paradox. Nowhere in the literature could any studies be found that discuss risk homeostasis in the context of information security behaviour in the same detail as in this research project. New approaches that have not yet been fully explored in the context of information security were suggested in conjunction with the risk homeostasis model, namely to address the security fatigue problem; sociological approaches such as the slower is faster (SIF) effect and the automaticity of social behaviour principle were suggested. At a more practical level, the results on risk homeostasis in this study offer decision makers and security specialists valuable information and new insights that could be advantageous in a strategic security planning process.

Other contributions include the following:

- The use of a value-focused approach to determine distinctive security dimensions and objectives provides a unique framework to practitioners to determine fundamental objectives and how to achieve them.
- It was shown how a practical security incident (phishing) can create an opportunity for organisational learning in order to improve the educational value of a practical security test. In addition, the practical social engineering test revealed information that was not generally known within the organisation. Empirical evidence was provided to show the serious challenges presented by the privacy paradox phenomenon, regardless of the apparently high levels of security awareness.
- A unique trust survey confirms that human trust, although not the sole determinant, does play a role in the privacy paradox.
- A specially focused investigation into perceptual differences between different groups of people proved to be a prerequisite for a successful information security environment. This investigation has led to a new proposed model for a safe and secure information security environment that is based on information security congruence between people.
- The company under study (where the practical tests and surveys were conducted) benefits from the new knowledge that was generated during the research project. The results therefore contribute and help in guiding the development of a better and more successful information security framework for the organisation.

1.9 Chapter conclusion

Chapter 1 provided an overview of the research project. The problem was contextualised and a problem statement, research objectives, and research paradigm and methodology were presented. This was followed by some ethical considerations as well as the thesis layout and structure. The chapter was concluded with an explanation of the contributions of the study.

References

Albrechtsen, E. 2003. Barriers against productive organisational learning from information security incidents. Paper in the PhD course Organisational Development and ICT, Norwegian University of Science and Technology.

Albrechtsen, E. and Hovden, J. 2009. The information security digital divide between information security managers and users. *Computers and Security*, 28:476-490.

Alhogail, A. 2015. Design and validation of information security culture framework. *Computers in Human Behavior*, 49:567-575.

Alhogail, A. and Mirza, A. 2014. Information security culture: A definition and literature review. World Congress on Computer Applications and Information Systems (WCCAIS). DOI: 10.1109/WCCAIS.2014.6916579.

Allam, S. 2014. A model to improve smartphone information security awareness. Unpublished DPhil thesis. Department of Information Systems, Faculty of Management and Commerce, University of Fort Hare.

Alnatheer, M.A. 2015. Information security culture critical success factors. 12th International Conference on Information Technology: New Generations. DOI: 10.1109/ITNG.2015.124

Bada, M. and Sasse, A. 2014. Cyber security awareness campaigns. Why do they fail to change behavior? Global Cyber Security Capacity Centre: Draft working paper. July 2014.

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.

Business Dictionary. 2015. www.businessdictionary.com

Chandrashekhar, A.M., Gupta, R.K. and Shivaraj, H.P. 2015. Role of information security awareness in success of an organisation. *International Journal of Research (IJR)*, 2(6):15-22.

Collis, J. and Hussey, R. 2014. Business research. A practical guide for undergraduate and postgraduate students. 4th edition, Palgrave Macmillan.

Cox, J.A. 2012. Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28:1849-1858.

Creswell, J.W. 2003. Research design. Qualitative, quantitative, and mixed method approaches. 2nd edition, Sage Publications, Thousand Oaks.

Crossler, R.E. 2010. Protection motivation theory: understanding determinants to backing up personal data. The 43rd Hawai International Conference on System Sciences. DOI: 10.1109/HICSS.2010.306.

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 and Security*, 32:90-101.

D'Arcy, J., Hovav, A. and Galletta, D. 2008. User awareness of security countermeasurers and its impact on information systems misuse: a deterrence approach. *Information Systems Research*. DOI: 10.1287/isre.1070.0160.

Da Veiga, A. 2015. An information security training and awareness approach (ISTAAP) to instill an information security-positive culture. Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015).

Da Veiga, A. and Martins, N. 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security*, 49:162-176.

Dodge, R.C., Carver, C. And Ferguson, A.J. 2007. Phishing for user security awareness. *Computers and Security*, 26:73-80.

Durandt, C. 2015. The productive use of free time: The utilisation of deterministic maintenance opportunity windows due to access capacity in large coupled production lines with finite buffers. PhD dissertation, Faculty of Economic and Management Sciences, Stellenbosch University.

Enrici, I., Ancilli, M. and Lioy, A. 2010. A psychological approach to information technology security. 3rd International Conference on Human System Interaction, HSI2010. DOI: 10.1109/HIS.2010.5514528.

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

Furnell, S. and Clarke, N. 2012. Power to the people? The evolving recognition of human aspects of security. *Computers and Security*, 31:983-988.

Gartner. 2015. Top 10 strategic technology trends for 2015. Available at: www.gartner.com

Glaser, B.G. and Strauss, A.L. 1967. The discovery of grounded theory: strategies for qualitative research, New York.

Gundu, T. and Flowerday, S.V. 2013. Ignorance to awareness: towards an information security awareness process. *South African Institute of Electrical Engineers*, 104(2):69-79.

Hasle, H., Kristiansen, Y., Kintel, K. and Snekkenes, E. 2005. Measuring resistance to social engineering. *In* ISPEC 2005. LNCS, Volume 3439, *eds*. Deng, R.H., Bao, F., Pang, H., Zhou, J., (Heidelberg: Springer). p132-143.

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

Herath, T. and Rao, H.R. 2009b. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2):1546-165.

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

Ifinedo, P. 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence and cognition. *Information and Management*, 51:69-79.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menezer, F. 2007. Social phishing. *Communications of the ACM*, 50(10):94-100.

Jansen, J. 2015. Studying safe online banking behavior: a protection motivation theory approach. Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015).

Jensen, C.D. 2015. Trust is the foundations for computer security. Information Security for South Africa Conference (ISSA 2015).

Kearney, W.D. and Kruger H.A. 2005. The development and application of a model to measure information security awareness. *In* Proceedings of the CACS2005 Oceania Conference. ISBN: 1-86308-124-0. Perth, Western Australia.

Keeney, R.L. 1994. Creativity in decision-making with value-focused thinking. *Sloan Management Review Summer*, 33-41.

Keser, H. and Gulduren, C. 2015. Development of information security awareness scale. *KU Kastamonu Egitim Dergisi*, 23(3):1167-1184.

Kokolakis, S. 2015. Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers and Security*, In Press.

Kruger, H.A. and Kearney, W.D. 2005. Measuring information security awareness: A West Africa gold mining environment case study. Information Security for South Africa Conference (ISSA 2005).

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

Kruger, H.A. and Kearney, W.D. 2008. Consensus ranking – an ICT security awareness case study. *Computers and Security*, 27:254-259.

Kruger, H.A. and Kearney, W.D. 2009. Effective corporate governance – a case study using a value-focused approach, *In* Proceedings of the 21st Conference of the South African Institute for Management Scientists (SAIMS).

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. 2013. Employees' information security awareness and behavior: a literature review. The 46th Hawai International Conference on System Sciences. DOI: 10.1109/HICSS.2013.192.

Oates, B.J. 2006. Researching information systems and computing. Sage Publications, Thousand Oaks.

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. 2010. Human factors and information security: Individual, culture and security environment. Australia Government, Department of Defence. Command Control, Communications and Intelligence Division, Defense Science and Technology Organisation, Edinburgh, Australia.

Pattinson, M.R. and Anderson, G. 2004. Risk homeostasis as a factor of information security. Available at: http://www.igneous.scis.ecu.edu.au.

Rantos, K., Fysarakis, K. and Manifavas, C. 2012. How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A global perspective*, 21:328-345.

Safa, N.S. von Solms, R. and Futcher, L. 2016. Human aspects og information security in organisations. *Computer Fraud & Security*, 15-18.

Saunders, M., Lewis, P. and Thornhill, A. 2003. Research methods for business students. 3rd edition. Prentice Hall.

Shaik, R. and Sasikumar, M. 2015. Trust model for measuring security strength of cloud computing service. *Procedia Computer Science*, 45:380-390.

Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76:146-164.

Siponen, M., Pahnila, S. and Mahmood, A. 2007. Employees' adherence to information security policies: an empirical study. *In* IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, *eds*. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer). p133-144.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. 2014. Variables influencing information security policy compliance. A systematic review of quantitative studies. *Information Management and Computer Security*, 22(1):42-75.

Soomro, Z.A., Shah, M.H. and Ahmed, J. 2016. Information securitry management needs more holistic approach: a literature review. *International Journal of Information Management*, 36:215-225.

Spandonidis, B. 2015. Linking information security awareness to information security management strategy. A study in an IT company. Masters Degree. Linnaeus University, Sweden.

Stewart, A. 2004. On risk: perception and direction. *Computers and Security*, 23:362-270.

Steyn, T., Kruger, H.A. and Drevin, L. 2007. Identity theft – empirical evidence from a phishing exercise. *In* IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, *eds*. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer). p193-203.

Teddlie, C. & Tashakkori, A. 2003. Major issues and controversies in the use of mixed methods in the social and behavioral sciences. *In* Handbook of mixed methods in social & behavioral research, *eds*. Tashakkori, A., Teddlie, C., (Thousand Oaks, CA: Sage). p3-50.

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.

Van Wyk, B. nd. Research design and methods. Post graduate enrolment and throughput. University of the Western Cape.

Wilde, G.J.S. 1994. Target risk. PDE Publications, Toronto, Canada.

Chapter 2

Literature synopsis

2.1 Introduction

A thesis that is presented in article format normally contains a chapter on a literature survey pertaining to the topic of the study. This is a requirement if the literature review for each of the papers (presented as chapters) is insufficient. In this research project, a focused and appropriate literature review and analysis were provided with each paper; in addition, the contextualisation (Chapter 1) was also based on a comprehensive literature research. These literature resources for Chapter 1 and each of the respective papers (Chapters 3-7) are presented in the form of a bibliography as part of the specific chapter. The objective of Chapter 2 is therefore to present only a high-level summary of literature resources used for the various topics in the research project.

2.2 The literature synopsis

A summary of key literature references per topic in the different chapters are presented in Table 2.1. Please note that these are just examples of the literature used and that the full bibliographies are available at the end of each chapter.

Chapter	Main areas in the chapter	Examples of key references
Chapter 1: Contextualisation and background *(Chapter 1 has a bibliography of 61 literature resources.)*	Human aspects of information security	*Frangopoulos, E.D., Eloff, M.M. and Venter, L.M.* 2014. Human aspects of information insurance: A questionnaire-based quantitative approach to assessment. Proceedings of the 8th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014). *Safa, N.S., Von Solms, R. and Fitcher, L.* 2016. Human aspects of information security in organisations. *Computer Fraud & Security*, 15-18.
	Information security policies	*Ifinedo, P*. 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence and cognition. *Information and Management*, 51:69-79. *Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J.* 2014. Variables influencing information security policy compliance: A

		systematic review of quantitative studies. *Information Management and Computer Security*, 22(1):42-75.
	Security awareness and culture	*Alhogail, A. and Mirza, A.* 2014. Information security culture: A definition and literature review. World Congress on Computer Applications and Information Systems (WCCAIS). DOI: 10.1109/WCCAIS.2014.6916579. *Da Veiga, A.* 2015. An information security training and awareness approach (ISTAAP) to instil an information security-positive culture. Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015). *Spandonidis, B.* 2015. Linking information security awareness to information security management strategy: A study in an IT company. Masters Degree. Linnaeus University, Sweden.
	Psychological and sociological models	*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 and Security*, 32:90-101. *Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B.* 2013. Employees' information security awareness and behavior: A literature review. The 46th Hawai International Conference on System Sciences. DOI: 10.1109/HICSS.2013.192. *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.
	Privacy paradox	*Cox, J.A.* 2012. Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28:1849-1858.

		Kokolakis, S. 2015. Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers and Security*, In Press.
	Research paradigm and methodology	*Saunders, M., Lewis, P. and Thornhill, A.* 2003. Research methods for business students. 3rd edition. Prentice Hall.
Chapter 3: A framework for good corporate governance and organisational learning – an empirical study *(Chapter 3 has a bibliography of 30 literature resources.)*	Value-focused approach	*Keeney, R.L.* 1994. Creativity in decision-making with value-focused thinking. *Sloan Management Review Summer*, 33-41.
	Corporate governance	*Australian Securities Exchange (ASX).* 2007. Corporate Governance Principles and Recommendations. 2nd edition. ASX Corporate Governance Council. *AS8015-2005.* 2008. Australian Standard for Corporate Governance of Information and Communication Technology (ICT). Available at http://www.ramin.com.au/it_ governance/as8015.html
Chapter 4: Phishing and organisational learning *(Chapter 4 has a bibliography of 24 literature resources.)*	Phishing	*Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menezer, F.* 2007. Social phishing. *Communications of the ACM*, 50(10):94-100. *Jansson, K. and Von Solms, R.* 2011. Phishing for phishing awareness. *Behaviour & Information Technology*. DOI: 10.1080/0144929X.2011.632650. *Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A. and Pham, T.* 2009. School of Phish: A real-world evaluation of anti-phishing training. Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS).
	Organisational learning	*Argyris, C. and Schon, D.* 1996. Organisational Learning II: Theory, method and practice. Prentice Hall. *Buckler, B.* 1998. Steps towards a learning organisation: Applying academic knowledge to improvement and innovation in business processes.

		The Learning Organisation, 5(1):15-23. *Kennedy, E.* 2008. A critical evaluation of the organisational learning that takes place in a project management environment. Unpublished M-dissertation, North-West University. *Van Niekerk, J. and Von Solms, R.* 2004. Proceedings of the 3rd International Information Security for South Africa Conference (ISSA 2004).
Chapter 5: Considering the influence of human trust in practical social engineering exercises *(Chapter 5 has a bibliography of 29 literature resources.)*	Trust	*Bose, R., Luo, X. and Liu, Y.* 2013. The roles of security and trust: Comparing cloud computing and banking. *Procedia – Social and Behavioral Sciences*, 73:30-34. *Kim, C., Tao, W., Shin, N. and Kim, K.* 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9:84-95. *McCole, P., Ramsey, E. and Williams, J.* 2010. Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, 63:1018-1024.
Chapter 6: Can perceptual differences account for enigmatic information security behaviour in an organisation? *(Chapter 6 has a bibliography of 47 literature resources.)*	Perceptual differences	*Akcam, B.K., Hekim, H. and Guler, A.* 2015. Exploring business student perception of information and technology. *Procedia – Social and Behavioral Sciences*, 195:182-191. *Albrechtsen, E. and Hovden, J.* 2009. The information security digital divide between information security managers and users. *Computers and Security*, 28:476-490. *Posey, C., Roberts, T.L., Lowry, P.B. and Hightower, R.T.* 2014. Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information and Management*, 51:551-567.

	Evaluation of results	*Cohen, J.* 1988. Statistical power analysis for behavioural sciences. 2nd edition. Hillsdale, NJ: Erlbaum. *Ellis, S.M. and Steyn, H.S.* 2003. Practical significance (effect sizes) versus or in combination with statistical significance (p-values). *Management Dynamics*, 12(4):51-52.
Chapter 7: Theorising on risk homeostasis in the context of information security behaviour *(Chapter 7 has a bibliography of 53 literature resources.)*	Risk homeostasis	*Wilde, G.J.S.* 1994. Target risk. PDE Publications, Toronto, Canada. *Wilde, G.J.S.* 1998. Risk homeostasis: An overview. *Injury Prevention*, 4:89-91. *Wilde, G.J.S.* 2001. Target Risk 2. PDE Publications, Toronto, Canada.
	Risk homeostasis in information security	*Pattinson, M.R. and Anderson, G.* 2004. Risk homeostasis as a factor of information security. http://www.igneous.scis.ecu.edu.au. *Stewart, A.* 2004. On risk: Perception and direction. *Computers and Security*, 23:362-270.
	Other suggested frameworks used with risk homeostasis	*Bargh, J.A., Chen, M. and Burrows, L.* 1996. Automaticity of social behavior: Direct effects of trait construct and stereotype activation on action. *Journal of Personality and Social Psychology*, 71(2):230-244. *Gershenson, C. and Helbing, D.* 2015. When slower is faster. *Complexity*, 21(2):9-15.

Table 2.1: Example literature

2.3 Chapter conclusion

This chapter presented a high-level summary of examples of literature resources used in the research project. Complete bibliographies are provided at the end of each chapter.

Chapter 3

A Framework for Good Corporate Governance and Organisational Learning – An Empirical Study

3.1 Introduction

Chapter 3 is presented in the form of a manuscript that was published in *The International Journal of Cyber-Security and Digital Forensics.* The paper was first presented as a peer reviewed conference paper at the 2nd International Conference on Cyber Security, Cyber Peacefare and Digital Forensics (CyberSec2013), Asia Pacific University of Technology and Innovation (APU), Kuala Lumpur, Malaysia, 4-6 March 2013. The title of the conference paper was *Effective corporate governance: Combining an ICT security incident and organisational learning.* The paper was then selected by the conference program committee to be published in the journal mentioned above. The final journal paper (presented here as Chapter 3) was an extended version of the original conference paper.

The paper details the use of a value-focussed approach to construct a framework that can be used to identify fundamental objectives in a good corporate governance model. Some high-level information on a first practical social engineering test is also presented. The paper forms the basis of the study to ensure, and confirm, that risk management and information security do indeed form part of the unique dimensions of a good corporate governance environment.

Figure 3.1 (on the next page) shows how the chapter is linked to the research objectives and research questions. This is then followed by the article as it was published. Guidelines of the journal are presented in Appendix F.

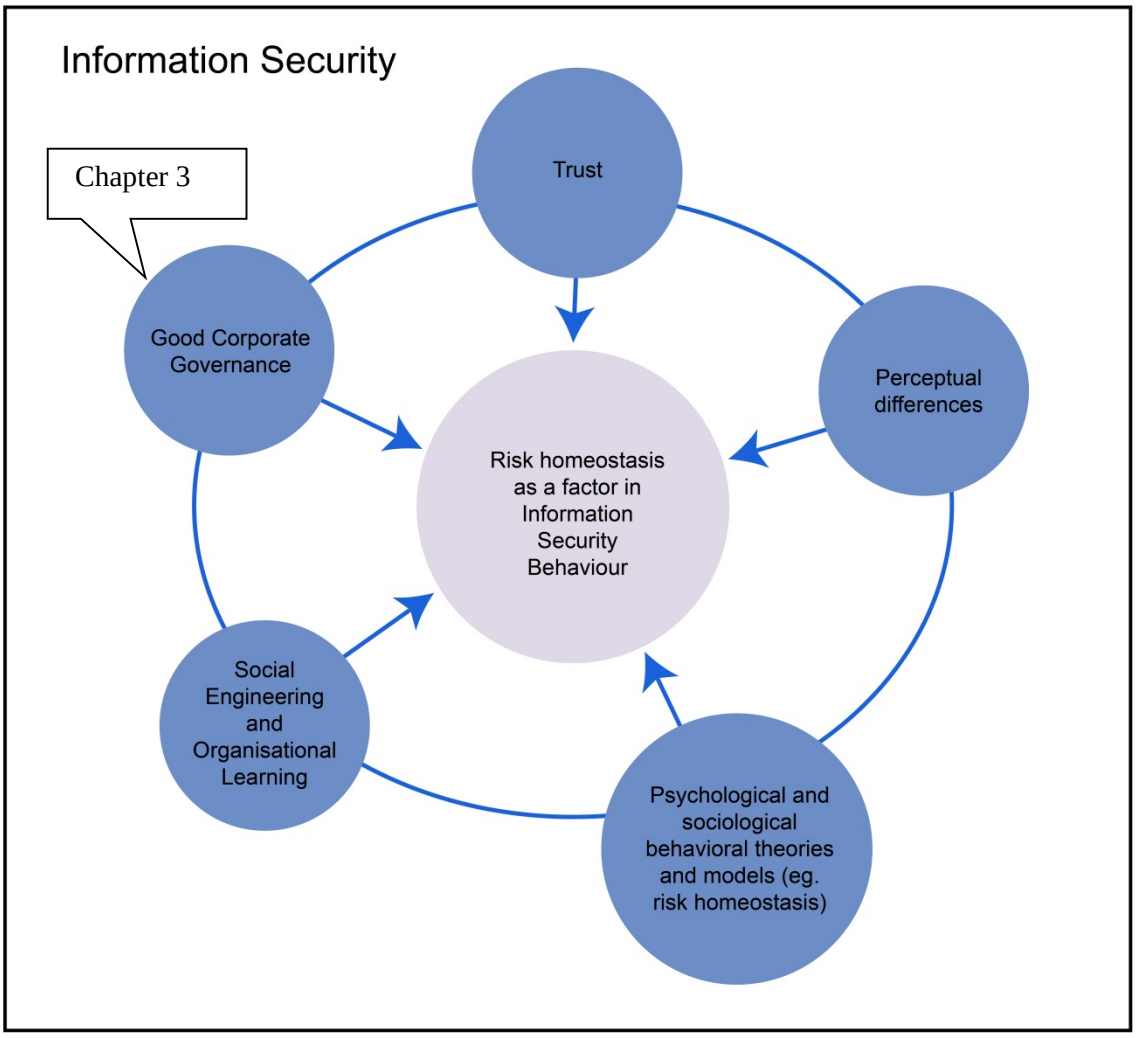


Figure 3.1 – Chapter 3 as part of the research study

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(1): 36-47
The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)

A FRAMEWORK FOR GOOD CORPORATE GOVERNANCE AND ORGANISATIONAL LEARNING – AN EMPIRICAL STUDY

WD Kearney, HA Kruger
School of Computer, Statistical and Mathematical Sciences
North-West University, Private Bag X6001, Potchefstroom, 2520
South Africa
Kearneys@iinet.net.au, Hennie.Kruger@nwu.ac.za,

Abstract. The importance of applying good governance principles has grown over the past decade and many studies have been performed to investigate the role and impact of such principles. One of the difficulties in the governance arena is to provide sufficient empirical evidence that good corporate governance and good governance of information technology is beneficial. This paper describes a framework, based on a value-focused approach, which is used to identify unique dimensions for evaluation in a large organisation. Following the evaluation a practical phishing experiment was used to show how a learning process can be initiated through security incidents and how organisational learning can be used to focus on the improvement of specific governance areas.

Keywords: Corporate governance, Governance of Information Technology, Value-focused approach, Phishing, Social engineering, Security awareness, Organisational learning.

1. INTRODUCTION AND BACKGROUND

It is often stated that information and information technology are key assets in many organisations and that it is used to drive business processes [1]. Information technology has become intrinsic to business operations and inadequate systems can hinder the performance and competitiveness of organisations and expose them to the risk of not complying with legislation [2]. It makes therefore sense to have proper governance principles in place that would apply firstly, to corporate governance and, second, to appropriate information technology governance principles which is a subset of corporate governance.

Corporate governance has become a topic that has been researched increasingly in the last decade [3]. Many definitions for corporate governance exist but in its simplest form it refers to the set of processes, customs, policies, laws and institutions affecting the way a corporation is directed, administered or controlled [4]. There are a number of standards and frameworks that define, describe and recommend the application of good corporate governance, all with the same objective of directing and controlling organisations to conduct business in such a way that it is beneficial to all parties involved. A number of common elements that underlie good corporate governance can be found within these frameworks and standards. Examples of such standards are the King III report [5], the Guidelines on Corporate Governance published by the Organisation for Economic Co-operation and Development (OECD) [6] and the Corporate Governance Principles and Recommendations issued by the Australian Securities Exchange (ASX) Corporate Governance Council [7].

There is a general lack of sufficient empirical evidence that good corporate governance pays. The core of this problem lies in the question on what and how to measure the success or impact of applying good corporate governance principles. A number of research studies to address these questions have been completed and some of the studies include the following. Bhagat and Bolton [8] performed a comprehensive study to analyse the relation between corporate governance and performance while Kelton and Yang [9] studied the impact of corporate governance on Internet financial reporting. Other researchers, who have studied the topic, or parts of it, include Plant [10] and Abdo and Fischer [11].

To address the importance of good corporate governance principles and how it may be

evaluated, this paper reports on a project that was initiated at a large geographically dispersed utility to investigate the feasibility of developing a framework to identify key dimensions that are specific to the company. The technique used to identify the dimensions was based on a value-focused approach [12] which allows for participation from stakeholders and helping to align dimensions in accordance with stakeholders' values. As corporate governance for information technology forms an integral part of corporate governance, it was decided to focus on the identification of key dimensions within the corporate governance arena which will then also cover information technology governance. The organisation in question is a large multi-billion dollar entity with over 3500 IT users and supply essential services to over 2 million customers.

In an effort to also respond to those dimensions that are perceived to be on an inadequate level, one of the identified dimensions *Risk Management* was chosen for further analysis. The objective was to show how a security incident such as a phishing scam may lead to organisational learning and ultimately lower some of the risks associated with the *Risk Management* dimension. This evaluation phase is important as it is imperative to ensure that there are proper security metrics and methodologies in place which will eventually lead to the achievement of specific security control objectives [13]. It is also important to try and quantify the measures for information security [14]. The choice of the *Risk Management* dimension can further be justified from the literature. Tamjidyamcholo and Al-Dabbagh [15] argue that the core of information security lies in risk management. According to them there is also a lack of details in the literature on how to reduce risk, especially in instances where uncertainty plays a role.

Van Niekerk and Von Solms [16] stated that organisational learning theories deal with the idea of how organisations learn and adapting their behaviour. One of the definitions for organisational learning is formulated as follows. Organisational learning occurs when individuals within an organisation experience a problematic situation and enquire into it on the organisational behalf [17]. The two main types of learning that generally occur are called single-loop and double-loop learning. Single-loop learning occurs when errors are detected and corrected and organisations continue with the present status quo without modifying present policies and goals while double-loop learning challenges, and possibly makes changes to the status quo and the existing assumptions and conditions [18]. Examples of researchers who performed studies related to information technology and organisational learning include Ahmat *et al* [19] and Van Niekerk and Von Solms [16].

In order to create an opportunity for organisational learning a practical phishing exercise was conducted. The basic idea of phishing is when someone attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity [20]. The use of practical tests seems to be a popular and effective way of making people aware of the dangers of phishing. Examples of such studies include Dodge *et al* [21] who performed a practical phishing experiment involving students from the United States Military Academy, Jagatic *et al* [20] performed a study at the Indiana University, Steyn *et al* [22] conducted a practical experiment in South Africa and Hasle *et al* [23] a study in Norway.

The remainder of this paper is organised as follows. Section 2 describes the methodology used for the different phases of the exercise while Section 3 presents the results. Section 4 concludes the paper with some general comments.

2. METHODOLOGY

The study comprises of three main steps. First, a value-focused approach was followed to identify the different dimensions of corporate governance; secondly, a survey was conducted to evaluate the identified dimensions; and finally, a practical phishing exercise was conducted to show how organisational learning can take place from security incidents which may improve specific corporate governance dimensions.

2.1 Value-focused Approach

Value-focused thinking is a three step decision technique suggested by Keeney [12]. The approach is concerned with what is important and how to achieve it [24]. The first step involves in-depth interviews with stakeholders with the objective of eliciting values that these persons or groups of persons might have within the decision context. The result is then a list of individual wishes or values. In step two, the values are converted into a common format which is termed an objective. According to Keeney [12] an objective is characterised by an object and a direction of preference. In the third and last step a means-ends network of objectives is established. Objectives are first classified as either a fundamental or means objective and then interrelationships and possible cause-effect relationships are generated. To classify an objective as a fundamental or means objective, Keeney suggested the use of a "why is this important" test. Each objective is tested against this question and if the answer suggests another objective, then it is classified as a means objective. Fundamental objectives are essential reasons for the problem and are not used to achieve any other objectives. The complete process and steps are schematically summarised in figure 1.

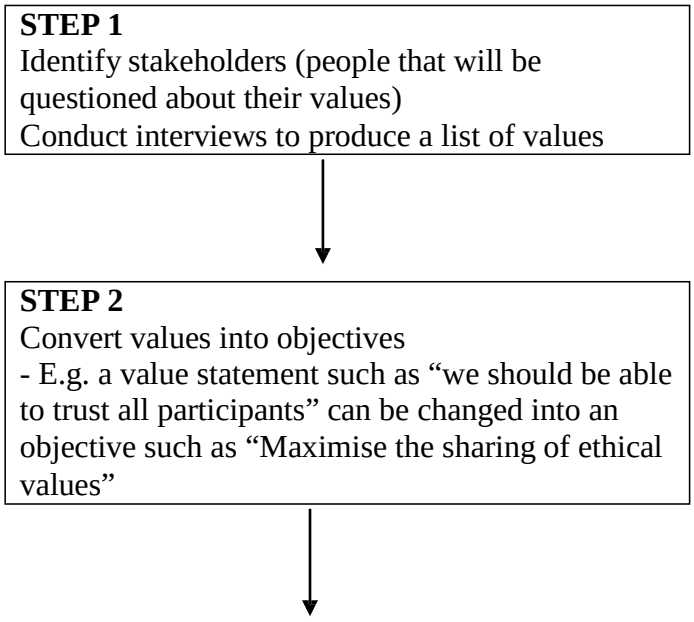


Figure 1 – Value-focused thinking process

To ensure that meaningful interviews (step 1) are conducted and that the wishes, concerns, problems and values of stakeholders are identified, a discussion document was prepared that was used during the interviews. The document contained four broad and open questions that was compiled according to the techniques for the identification of objectives suggested by Keeney. The four questions, used as discussion points, were the following.

1. What would you regard as important aspects in good corporate governance?

The purpose of this question was to encourage stakeholders to discuss their goals and to determine strategic and generic objectives. Examples of some of the answers received include building trust with partners, risks that are well managed, proper structures and systems in place etc.

2. What would you do or implement to ensure that the application of corporate governance principles is effective?

The second discussion point assisted mainly with the development of a wish list and the identification of alternatives. The wish list included answers such as proper contracts and documentation, monitoring systems, capacity to respond to changes etc.

3. What are your current concerns regarding the effective application of good corporate governance principles?

It is often useful to identify shortcomings and problems when trying to determine and describe objectives. The goal of this discussion point was to

assist with this identification, for example, a concern such as "a mismatch between our requirements and what our business partners can provide" may indicate that appropriate structures are essential to ensure that business objectives are achieved.

4. If you have to evaluate the effectiveness of the application of corporate governance principles, how would you do it and how would you know that it is acceptable?

The aim of this point was to try and quantify objectives. Answers ranged from the use of audit reports to measuring against contractual obligations to monitoring financial indicators.

Some researchers prefer to make use of questionnaires to gather information but in this study it was decided to follow a similar interview process as the one used by Dhillon and Torkzadeh [25] and Sheng, *et al* [24] who evaluated the strategic implications of mobile technology using a value-focused approach. Seven senior staff members (ranging from managers to directors) were interviewed using the four discussion points as a basis. This sample size was determined by a "saturation point" which is a standard stopping rule for qualitative research. Glaser and Strauss [26] used the term "theoretical saturation" which means that no additional data is found by the researcher for a specific category in a study. It is off course true that one would never know if the next interviewee would be able to provide new information (which is also true in the case of questionnaires). Statistically speaking it might also be argued that the sample size is not sufficient. It was however decided to keep to the generally accepted qualitative procedure utilizing the saturation point stopping rule. The interviews lasted for approximately 30-60 minutes and were recorded together with notes taken during the interviews.

2.2 Survey To Evaluate Dimensions

Following the identification of the different dimensions, a survey was conducted to determine the level of compliance. A questionnaire, based on the different means objectives, was developed to obtain respondents' views. A total of 20 questions were formulated in the form of statements that had to be evaluated on a scale of 1 to 10. Some of the statements were formulated in a subjective manner to gauge perceptions while others were more of an objective nature to determine whether certain matters have been implemented or exist.

One of the main objectives identified (see section 3.1 for details) was *Risk Management*. Figure 2 presents two example questions in the form of statements for this objective. The first question is an example of an objective question to determine if something has been implemented while the second question has a subjective nature intended to measure a perception.

The application of the questionnaire was structured in such a way that a number of opportunities to benefit from the process were possible, for example measuring and reporting in a drilled down fashion, the use of importance weights, sensitivity analysis etc. Questionnaire results were processed in a spreadsheet application and output was presented in the form of various graphs (see section 3.2) and tables describing the different evaluations.

1. The company has a fully effective documented risk register for its operations and projects
2. The company has effectively manage risks that may have an impact on its objectives and operations

Figure 2 – Example survey questions

2.3 The Phishing Exercise

The successful implementation of an e-mail phishing exercise is dependent on how well certain issues, associated with the exercise, are considered. In this study general as well as specific considerations had to be taken into account. The general considerations are concerned with those issues that may have an impact on the exercise as a whole and include a range of issues such as the determination and definition of an objective; getting ethical clearance and top management

approval; the timing of the exercise; maintaining the privacy of respondents; the selection of a random and representative sample of respondents; measurements to ensure that no information was disclosed prior to the exercise; and, a debriefing exercise following the test.

The specific considerations deal with aspects specific to the enterprise where the study was conducted. Some of the aspects included no reference to any specific IT, security or internal audit staff as this may compromise the trust between users and staff. Steps also had to be taken to ensure that the enterprise's anti-phishing tools and spam filters do not identify the message as spam or a phishing scam, and the Service Centre had to be provided with a predetermined response should there be any queries from users. Provision was also made for respondents who reply directly to the phishing e-mail. Some of the technical considerations include the deletion of duplicate records (if a user responds more than once) and also a check to see whether the correct usernames were supplied (password were requested but not recorded). The key issue was the construction of an appropriate e-mail message. The message had to be concise, credible and at the same time be enticing in order for participants to react.

To ensure that the phishing e-mail message complies with all the necessary requirements, it was decided to make use of certain emotional exploits [27]. The emotional exploits include legitimacy (when a user is made to believe that the source of the e-mail message is legitimate), authority (people tend to comply with instructions or requests issued by someone with authority), scarcity (when users believe that the time to react is limited) and conformity (users who believe that other fellow-employees have already reacted to a request are inclined to also comply with the request).

Figure 3 shows how the e-mail was constructed and the clues provided to alert users that the message was likely not to be legitimate. The real name of the organisation has been changed in figure 3.

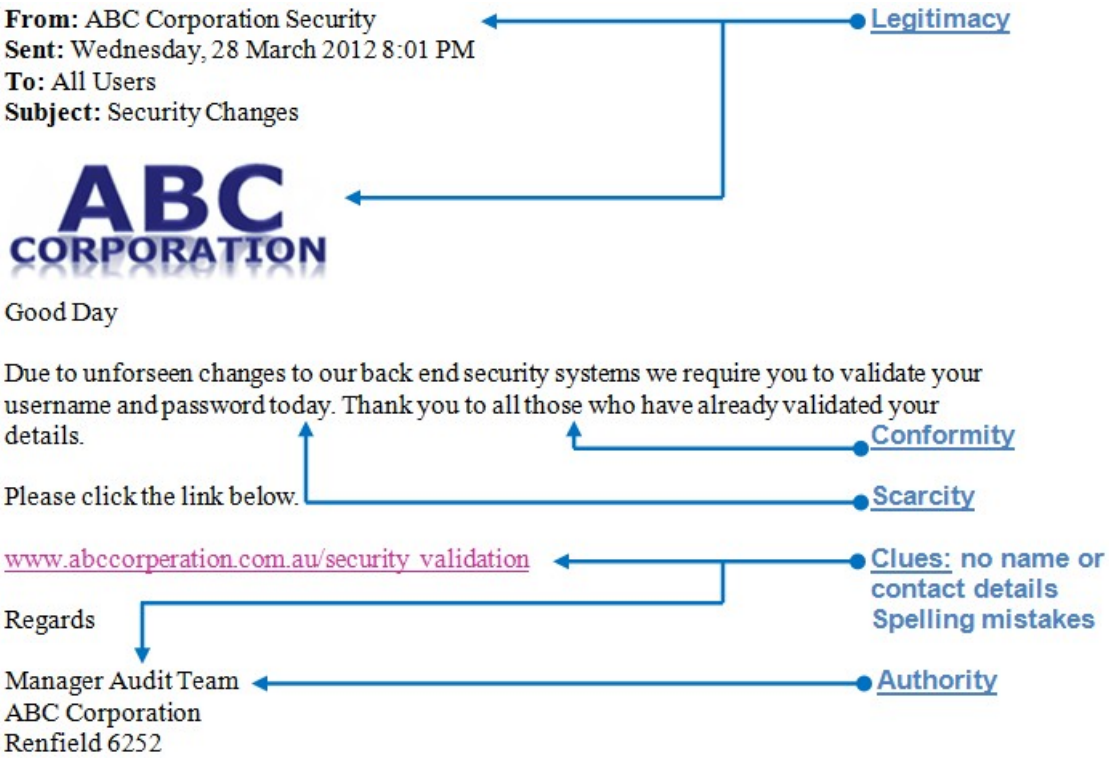


Figure 3 – Phishing e-mail message

The e-mail message (figure 3) was first sent to a small group of 10 employees to test whether all technical aspects are functioning correctly and also to get feedback on possible improvements. After

some minor changes were made it was decided to go ahead and implement the phishing test.

The phishing e-mail message was sent to all employees at 8:00pm on a weekday night. The organisation is a 24-hour operation with activities taking place on a continuous basis. This was done to ensure that night workers are included in the test and also to guarantee that day workers receive the message first thing in the morning. As soon as the message was sent out, security personnel were involved and concern was expressed regarding the possibility of an external attack aimed at disrupting essential services. Due to this and the reaction of senior managers, it was decided at 8:30am the next morning to remove the phishing message and to officially end the test. The reasons for withdrawing the phishing e-mail relatively early the next morning were firstly, to prevent large-scale disruptions and secondly, because enough data has been recorded at that stage to draw meaningful conclusions. The data and the experience were sufficient and interesting results were obtained.

3. RESULTS

This section presents the results for the value-focused process, the survey to evaluate the identified dimensions and the phishing exercise used to demonstrate how organisational learning can take place to address the *Risk Management* dimension.

3.1 Results Of The Value-focused Process

Following the value-focused thinking approach as described in section 2.1, a network of objectives was constructed which is presented in figure 4 (on the next page). On the left hand side (in figure 4) are the means objectives that show the concerns, wishes and values of interviewees while the right hand side shows the fundamental objectives.

The fundamental and means objectives on which the means-ends network is based are listed in tables 1 and 2. Table 1 shows the fundamental objectives and the factors describing them while table 2 shows an extract of the aspects that influence some of the means objectives according to the interviewees. A detailed description of these results can also be found in [28].

Table 1 - Fundamental Objectives

1. **Appropriate Board and Management structures are in place**
   - An appropriate alliance structure is in place
   - All arrangements are formalized
2. **Maximize the use of appropriate business practices and ethics**
   - Build trust with partners; have trusted people; openness
3. **Maximize performance management**
   - Strategic risk
   - Project outcomes must be good
4. **Maximize disclosure and transparency**
   - Continuous improvement; standardized frameworks
5. **Maximize risk management**
   - Robust risk management principles
6. **Appropriate legal, regulatory and social environment exists**
   - Regular reviews
   - Policies and procedures to manage compliance

Table 2 - Means Objectives

1. **Maximize understanding of roles, right and obligations**
   - Protect the interest of the organization; define what needs to be achieved
   - Roles and responsibilities must be understood
2. **The most appropriate structure is used to achieve objectives**
   - Number of parties involved should be appropriate; appropriate resources
   - Structure must be accepted and operates well; value for money

   .
   .
18. **Maximize use of appropriate policies and procedures to manage compliance**
    - Systems and frameworks in place; monitoring – internally e.g. internal audit department
    - Measure against objectives
19. **Maximize internal audit process**
    - Internal mechanisms such as quality control, compliance verification etc.
    - Formal internal audit department exists; regular audit reports

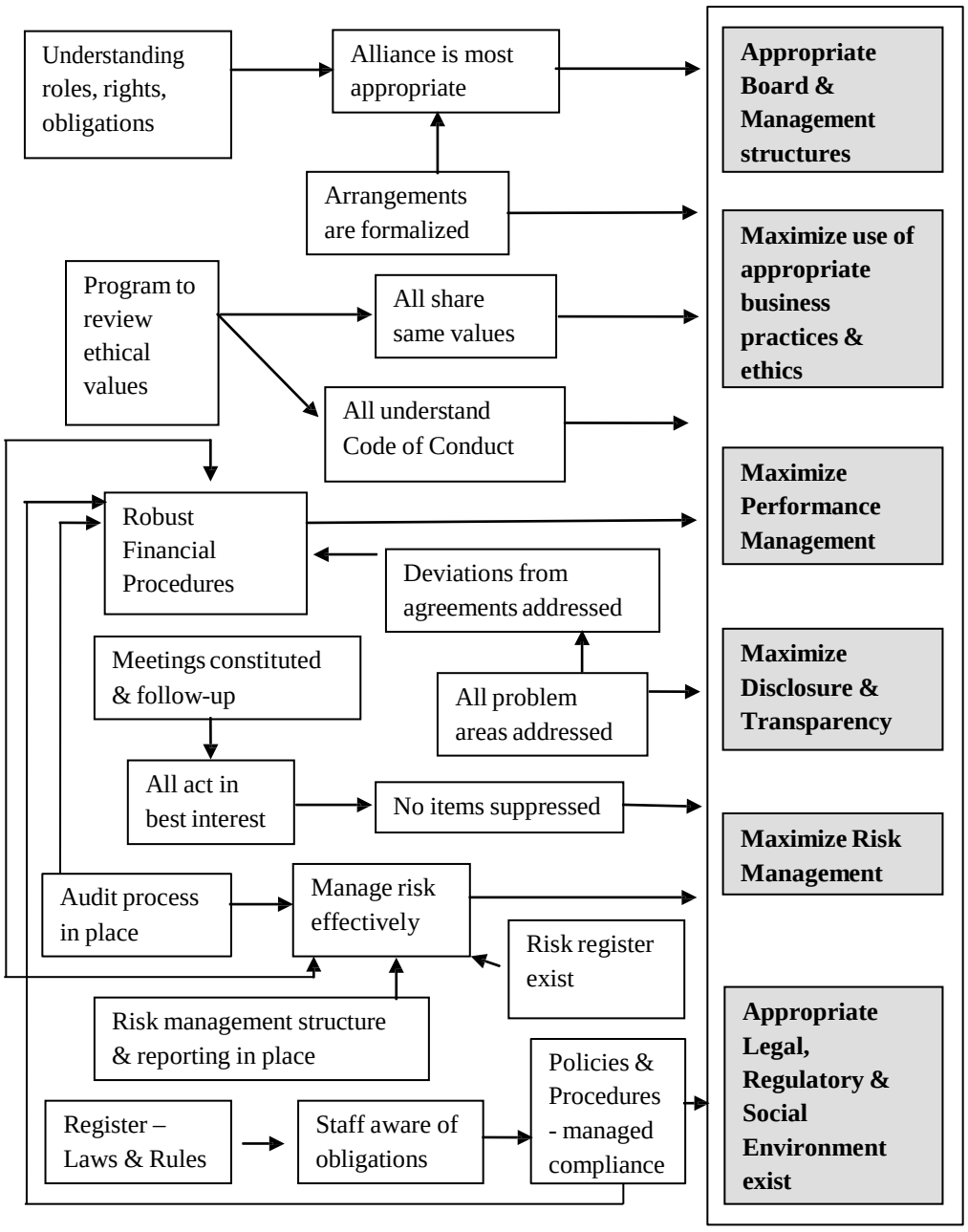


Figure 4 – Means-ends objectives for corporate governance

An analysis of the different means and fundamental objectives resulted in the six different dimensions as indicated in table 1 and figure 4. These six dimensions are:

- Appropriate board and management structures;
- Maximize the use of appropriate business practices and ethics;
- Maximize performance management;
- Maximize disclosure and transparency;
- Maximize risk management; and
- Appropriate legal, regulatory and social environment exist.

To verify whether the six fundamental objectives (or dimensions) identified are in line with generally accepted corporate governance principles, it was decided to compare them to two sets of published principles namely the Corporate

Governance Principles and Recommendations issued by the Australian Securities Exchange (ASX) Corporate Governance Council [7], and the AS8015-2005: Australian Standard for Corporate Governance of Information and Communication Technology [29].

The ASX Corporate Governance Council listed eight corporate governance principles as being necessary to ensure good corporate governance in enterprises while the AS8015 standard provides six principles for good governance of ICT. These principles are briefly presented in table 3 along with an indication of how the identified fundamental objectives may be linked to them.

Table 3 – Corporate Governance and ICT Principles

ASX Principles [7]	**Corresponding fundamental objectives identified with value-focused assessment**	**AS8015 Principles for ICT Governance [29]**
1. Lay solid foundations for management and oversight (refers to roles and responsibilities of the board and management)	Appropriate board and management structures are in place	Establish clearly understood responsibilities Plan ICT to best support the organisation
2. Structure the board to add value (refers to composition, size and commitment)	No specific fundamental objective can be mapped to this principle, but it is partially addressed by *Appropriate board and management structures are in place*	
3. Promote ethical and responsible decision making	Maximise the use of appropriate business practices and ethics	Ensure ICT respects human factors
4. Safeguard integrity and financial reporting	Maximise performance management	Acquire ICT validly Ensure that ICT performs well whenever required
5. Make timely and balanced disclosure	Maximise disclosure and transparency	Acquire ICT validly Ensure ICT conforms with formal rules
6. Respect the rights of shareholders	No specific fundamental objective can be mapped to this principle, but it is partially addressed by *Maximise the use of appropriate business practices and ethics*	Ensure ICT respects human factors
7. Recognise and manage risk	Maximise risk management	Plan ICT to best support the organisation Ensure that ICT performs well whenever required
8. Remunerate fairly and responsibly	No specific fundamental objective can be mapped to this principle	
Appropriate legal, regulatory and social environment exists. There is no specific principle where this fundamental objective can be linked to. It does however cover certain aspects under the principle *Promote ethical and responsible decision making*.		

It is clear from table 3 that the value-focused assessment produced fundamental objectives that are in line with accepted corporate governance principles. Only one of the principles (Remunerate fairly and responsibly) was not directly covered by the identified objectives while there was also only one fundamental objective that could not directly be linked to any of the eight principles (Appropriate legal, regulatory and social environment exists). This objective, however, covers certain aspects in some of the other principles.

3.2 Results Of The Survey

A total of 31 staff members were identified as respondents to evaluate the identified dimensions. This choice of participants was based on their level of seniority, their knowledge of corporate governance principles, and a request from senior management to include them in the exercise. Figure 5 shows a graph with the overall evaluation of the six dimensions. A formal 5-level scale (not presented here) was constructed to interpret the results on the graph. The scale ranges from no evidence that governance principles are applied at the lower end, to significant investment in time and resources to apply governance principles at the other end.

Applying the scale and from figure 5 it can be seen that the two principles *Disclosure and Transparency* and *Performance Management* are, on average, currently performing satisfactorily as evaluated by the participants. The remaining four governance principles were all, on average, evaluated as principles that are applied to a certain degree but with some room for improvement. The *Risk Management* dimension was chosen for further investigation to see if a practical security incident can initiate an organisational learning process that can contribute to the risk management process.

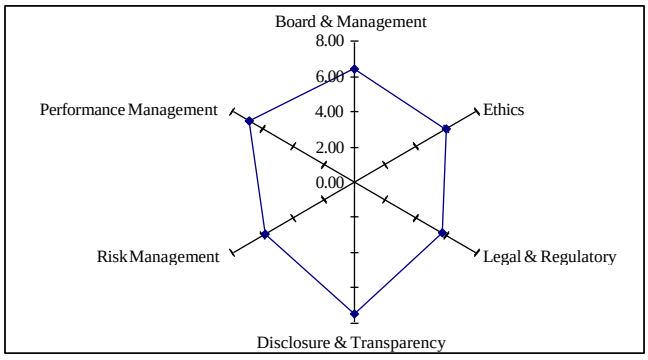


Figure 5 – Overall evaluation of principles

3.3 Organisational Learning Results

The data recorded from the phishing exercise include the employee name, department where the person is working and the username. Passwords were also requested but not recorded due to privacy considerations. As part of the exercise, passwords were validated but only the result was recorded in a simple yes/no format. Appropriate safeguards to ensure privacy were put in place. The recorded employee names were purely recorded for statistical purposes and nowhere during reporting were specific names linked to responses.

During the test 280 users responded to the phishing message of whom 231 (83%) entered their usernames and passwords on the webpage. Although there were approximately 1700 active users logged on during the test, it would be incorrect to assume that all of those who did not respond acted in a positive way. Reasons for this may be the fact that many people do not respond immediately to e-mail messages, some users may have left their workstations logged on during the night while not there, some users may have been engaged in other tasks and simply did not check their mail inboxes, etc. A much more significant analysis was to link the 280 users who responded, to an information security course that all staff members are required to complete and which would have provided them with basic security information on how to react to possible phishing scams. An unexpected 69% of those users who entered their passwords did complete the security training in the past. This also implies that almost one third (31%) never completed the security training course. These basic results indicate that there are at least two points of concern. Firstly, the high number of users who responded in a negative way despite their security training and secondly, the relatively high number of users that never completed the information security course.

An analysis of responses (percentages) per experience (years of service) category for those who entered their usernames and passwords shows that those employees with less experience at the organisation - and therefore less exposure to its security practices and policies - are more inclined to give away personal details. More than a third (35%) of those who entered their usernames and passwords have less than 5 years experience with more than half (52%) less than 10 years. This analysis is shown graphically in figure 6.

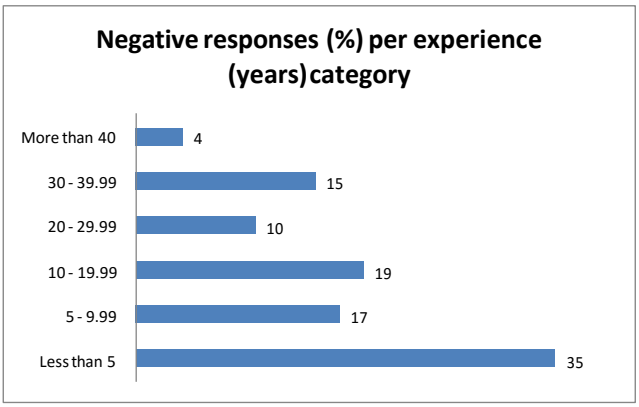


Figure 6 – Responses per experience category

Apart from these results the focus was more directed at possible organisational learning opportunities that may contribute to the Risk Management corporate governance principle. As explained earlier, organisational learning involves the adjustment of actions based on an experience. These adjustments, or learning, can then be categorised as single or double-loop learning. The results from this study have shown that the phishing experiment offers the ideal opportunity for learning and that both single and double-loop learning has taken place.

Single-loop learning took place in the form of small changes in making staff aware of the risks and consequences of phishing scams. Instructions concerning basic acceptable behaviour related to suspicious e-mail messages were issued in the form of e-mail messages and the company's weekly in-house bulletin.

In addition, a corporate blog was employed to assist in making staff aware of risks involved in social engineering activities. There has been a high growth in the use of corporate blogs over the last few years and at the corporation where the testing was done, this is no different. The CEO makes use of a blog to communicate a variety of messages into the organisation. Whilst email communication is more direct, the blog is often seen to offer a more open and personable medium of communication. These corporate blogging initiatives are interactive and cheap to deploy which does make them a very attractive form of communication.

In ongoing discussions regarding the learning from the exercise, the CEO has indicated that this medium will be used to educate and make staff members aware of the dangers of "phishing" and other social engineering scenarios. As the initial email phishing exercise created a level of angst amongst certain elements within the organisation, care will need to be taken on the content and timing of the message. The level of interaction and any feedback received will be monitored and evaluated. This evaluation, which may eventually become a double-loop learning activity, will form part of the broader study and is not a part of this paper.

The single-loop learning activities mentioned above did not change the status quo of any process but were quick and effective corrective measures to address a specific problem area. There were, however, other issues that needed a more comprehensive investigation that may lead to a change in policies and procedures. These double-loop learning issues include the following.

– All staff members are required to complete an information security course which will equip them with basic security knowledge for different security situations including phishing scams. An analysis of the phishing results showed that not all staff has completed the course. More importantly, a relatively large number of those who have completed the course had given their passwords away. An assessment of the course content and possible controls to ensure that everybody completes the course is planned. This may lead to a change in the current security policy on issues pertaining to basic security training.

– Another issue, planned for the future, which was highlighted during the phishing exercise relates to the gap between the different security views and expectations of managers and users. This gap is sometimes referred to as the information security digital divide between managers and users [30] and may lead to unrealistic security assumptions and management strategies that are not aligned with the dynamics of the user environment.

Basic problems were immediately corrected through an easy and uncomplicated single-loop learning approach while double-loop learning issues provided an opportunity for the organisation to adapt and adjust some of their information strategies. To adapt and improve information security strategies implies a definite contribution to the important corporate governance principle concerned with risk management and it therefore seems permissible to draw the conclusion that the practical security exercise has created opportunities for organisational learning which in turn will contribute to the management of risk in general.

4. CONCLUSION

Interest in corporate and information technology governance has grown tremendously in the past decade. It has become increasingly important to ensure that businesses align their information technology leadership, direction and strategies with the rest of their business objectives. One of the challenges in the field of corporate governance is to provide empirical evidence that the application of good corporate governance is beneficial. This paper reported on the development and application of a process to evaluate good corporate governance principles. A value-focused approach was followed to determine important factors specific to the company reviewed. This resulted in six different factors that were in line with those suggested in the literature on corporate governance and governance for information technology. The framework was tested and results have shown that certain areas, e.g. risk management, in the company under review, can be improved. A successful phishing exercise was then conducted to show how a security incident can create opportunities for organisational learning which will benefit the risk management dimension of information technology governance.

REFERENCES

1. Von Solms, R., Von Solms, S.H.: Information security governance: Due care. Computers and Security 25, pp. 494--497 (2006).
2. ISO/IEC standard for corporate governance of information technology). http://www.iso.org/iso/ (2008).
3. Gillan, S.L.: Recent developments in Corporate Governance: An overview. Journal of Corporate Finance 12, pp. 381--402 (2006).
4. Wikipedia. http://en.wikipedia.org/wiki/Corporate-Governance (2008).
5. King III Report on Corporate Governance. The Institute of Directors. http://www.iodsa.co.za (2009).
6. Organisation for Economic Co-operation and Development. OECD Guidelines on Corporate Governance of State-owned Enterprises (2005).
7. Australian Securities Exchange (ASX). Corporate governance principles and recommendations. 2nd edition. ASX Corporate Governance Council (2007).
8. Bhagat, S., Bolton, B.: Corporate governance and firm performance. Journal of Computer Finance 14, pp. 257--273 (2008).
9. Kelton, A.S, Yang, Y.: The impact of corporate governance on Internet financial reporting. Journal of Accounting and Public Policy 27, pp. 62--87 (2008).
10. Plant, K.: Towards the development of a framework for ethics audits: an internal auditing perspective. SA Journal of Accountability and Auditing research 8, pp. 15--26 (2008).
11. Abdo, A., Fisher, G.: The impact of reported corporate governance disclosure on financial performance of companies listed on the JSE. Investment Analysts Journal 66, pp. 43--56 (2007).
12. Keeney, R.L.: Creativity in decision-making with value-focused thinking. Sloan Management Review Summer, pp. 33--41 (1994).
13. Azuwa, M.P., Ahmad, R., Sahib, S., Shamsuddin, S.: Technical security metrics in compliance with ISO/IEC 27001 Standard. International journal of Cyber-Security and Digital Forensics (IJCSDF). The Society of Digital Information and Wireless Communications 1(4), pp. 280-288 (2012).
14. Jouini, M., Aissa, A.B., Rabai, L.B.A., Mili, A.: Towards quantitative measures of information security: A cloud computing case study. International journal of Cyber-Security and Digital Forensics (IJCSDF). The Society of Digital Information and Wireless Communications 1(3), pp. 248-262 (2012).
15. Tamjidyamcholo, A., Al-Dabbagh, R.D.: Genetic algorithm approach for risk reduction of information security. International journal of Cyber-Security and Digital Forensics (IJCSDF). The Society of Digital Information and Wireless Communications 1(1), pp. 59-66 (2012).
16. Van Niekerk, J., Von Solms, R.: Organisational learning models for information security. http://icsa.cs.up.za/issa/2004/Proceedings/Full/043.pdf (2004).
17. Argyris, C., Schon, D.: Organisational learning II: Theory, method and practice. Prentice Hall (1996).
18. Kennedy, E.: A critical evaluation of the organisational learning that takes place in a project management

environment. Unpublished M-dissertation, North-West University (2008).
19. Ahmad, A., Hadgkiss, J., Ruighaver, A.B.: Incident response teams – challenges in supporting the organisational security function. Computers and Security 31, pp. 643--652 (2012).
20. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menezer, F.: Social phishing. Communications of the ACM 50(10), pp. 94--100 (2007).
21. Dodge, R.C., Carver, C., Ferguson, A.J.: Phishing for user security awareness. Computers and Security 26, pp. 73--80 (2007).
22. Steyn, T., Kruger, H.A., Drevin, L.: Identity theft – empirical evidence from a phishing exercise. New approaches for Security, Privacy and Trust in complex environments, IFIP International Federation for Information Processing 232, pp. 193--203 (2007).
23. Hasle, H., Kristiansen, Y., Kintel, K., Snekkenes, E.: Measuring resistance to social engineering. In: Proc. 2005 ISPEC05 first international conference on information security practice and experience, pp. 132--143 (2005).
24. Sheng, H., Fui-Hoon, F., Siau, K.: Strategic implications of mobile technology: A case study using Value-Focused thinking. Journal of Strategic Information Systems 14, pp. 269--290 (2005).
25. Dhillon, G., Torkzadeh, G.: Value-focused assessment of information system security in organisations. In: Proc. 2001, The 22nd international conference on information systems, pp. 561--565 (2001).
26. Glaser, B.G., Strauss, A.L.: The discovery of grounded theory: strategies for qualitative research, New York (1967).
27. Jansson, K.: A model for cultivating resistance to social engineering attacks. Unpublished M-dissertation, Nelson Mandela Metropolitan University (2011).
28. Kruger, H.A., Kearney, W.D.: Effective corporate governance: A case study using a value-focused approach, In: Proc. 2009 SAIMS 21st Conference of the South African Institute for Management Scientists, on CD (2009).
29. AS8015-2005 – Australian Standard for Corporate Governance of Information and Communication Technology (ICT). http://www.ramin.com.au/it-governance/as8015.html (2008).
30. Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Computers and Security 28, pp. 476--490 (2009).

Chapter 4
Phishing and Organisational Learning

4.1 Introduction

Chapter 4 is presented in the form of a manuscript that was published in *Security and Privacy Protection in Information Processing Systems.* L.J. Janczewski, H.B. Wolfe, and S. Shenoi (Eds.): SEC 2013, IFIP AICT 405, pp. 379-390, 2013 (Springer).

This paper shows how a practical social engineering experiment can create opportunities for organisational learning. The paper also provides empirical evidence that highlights security information behaviour challenges such as the privacy paradox despite high security awareness levels.

Figure 4.1 (on the next page) shows how the chapter is linked to the research objectives and research questions. This is then followed by the article as it was published. Guidelines of the journal are presented in Appendix G.

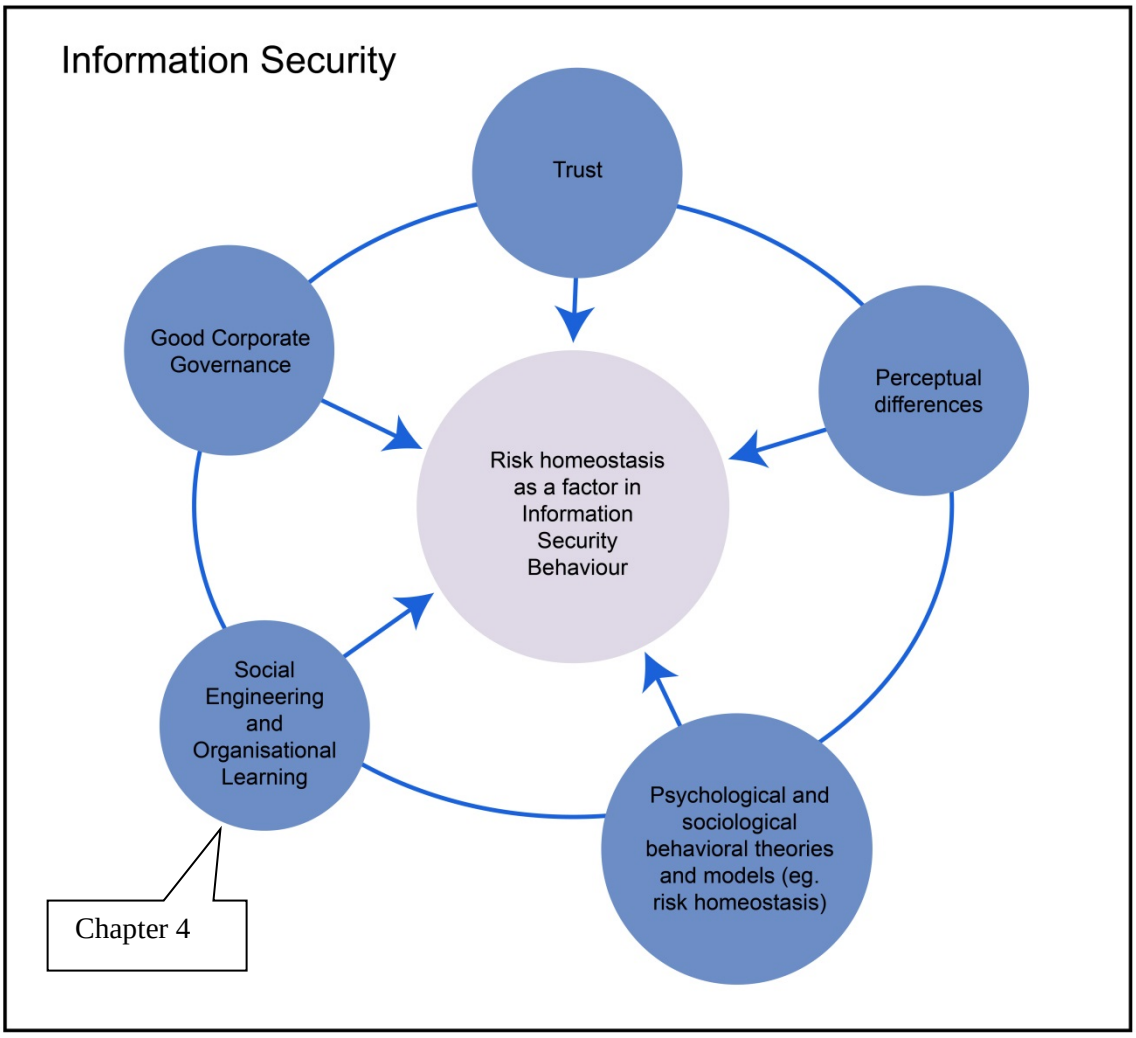


Figure 4.1 – Chapter 4 as part of the research study

Phishing and Organisational Learning

Wayne D. Kearney and Hennie A. Kruger

School of Computer, Statistical and Mathematical Sciences,
North-West University, Private Bag X6001, Potchefstroom, 2520
South Africa
Kearneys@iinet.net.au, Hennie.Kruger@nwu.ac.za

Abstract. The importance of addressing the human aspect in information security has grown over the past few years. One of the most frequent techniques used to obtain private or confidential information from humans is phishing. One way to combat these phishing scams is to have proper security awareness programs in place. In order to enhance the awareness and educational value of information security awareness programs, it is suggested that an organisational learning model, characterised by so called single-loop and double-loop learning, be considered. This paper describes a practical phishing experiment that was conducted at a large organisation and shows how a learning process was initiated and how security incidents such as phishing can be used successfully for both single and double-loop learning.

Keywords: Phishing, Social engineering, Information security awareness, Organisational learning.

1 Introduction

Traditionally the mitigation of information security risks was addressed using a variety of technical controls. It is however widely accepted and recognised that technology on its own cannot deliver complete solutions to the security problem and that the human aspect of security should receive more attention [1], [2], [3]. One way of addressing the human side of security is to focus on awareness and educational activities [4] making use of some form of an awareness program.

An information security awareness program normally focuses on a number of issues related to the correct security behaviour of users. In some instances it may also concentrate on one area such as social engineering which is one of the most serious threats to information security as criminals keep on focussing on deceptive techniques to attack computer users and organisations [5]. Phishing, which is one of the social engineering techniques, occurs when people are manipulated by deception into giving out information [6] and is one of the major threats to modern organisations and information technology users in general. It requires an ongoing awareness not to become a victim of a phishing scam and various researchers have completed studies related to phishing experiments and awareness levels of users [5], [7], [8].

A popular technique to improve user awareness pertaining to phishing scams is to conduct unannounced phishing tests in order to evaluate users' propensity to respond

L.J. Janczewski, H. Wolf, and S. Shenoi (Eds.): SEC 2013, IFIP AICT 405, pp. 379–390, 2013.

to an attack [5], [9]. Albrechtsen [10] contend that these type of incidents and experiments present great opportunities to learn and improve information security. To ensure that learning does take place Van Niekerk and Von Solms [3] suggested that an organisational learning model be used.

This paper describes a practical phishing exercise that was conducted in industry and shows how organisational learning took place as a result. The remainder of the paper is organised as follows. Section 2 presents the background to the study as well as appropriate references to related work. In section 3 the methodology used is discussed while section 4 details the results. Concluding remarks are presented in section 5.

2 Background and Related Work

Organisational learning theories deal with the idea of how organizations learn and adapting its behaviour [3]. This concept has been subjected to a wide and growing variety of researchers and a number of definitions have been suggested in the literature [11], [12]. Despite all these definitions the concept of organizational learning is by no means an unambiguous concept, as no one irrefutable definition has emerged in literature [13]. Organisational learning originated from the work by Argyris and Schon during the 1970s and one of the definitions suggested by them will be assumed in this study. The definition is formulated as follows. Organisational learning occurs when individuals within an organisation experience a problematic situation and enquire into it on the organisational behalf [14].

In an effort to enhance organisational learning, Buckler [15] proposed that an actual learning process, as depicted in figure 1, occurs in organisations. Buckler then argues that individuals will move through the different learning stages driven by their inherent individual motivations to learn. Associated with these motivational forces, there will be certain barriers to the learning process, and where the motivational restraining (barrier) forces are matched, learning will not take place. In order for organisational learning to result in performance improvement, the enactment stage (see figure 1) of the learning

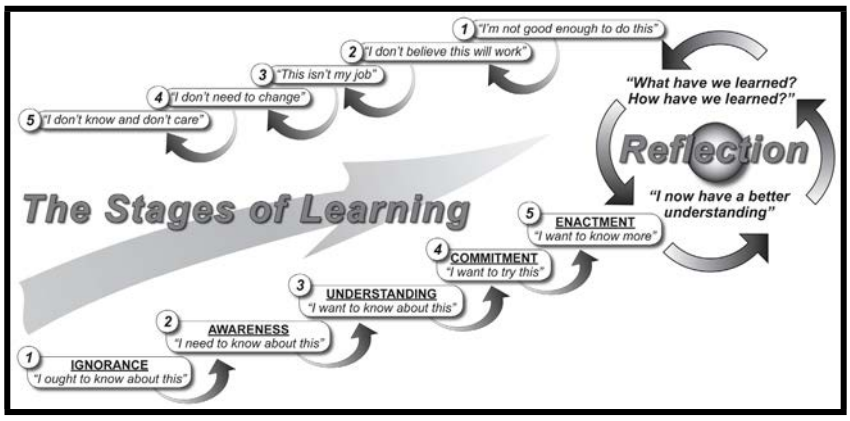


Fig. 1. The learning process (adapted from [15])

process needs to be achieved – this will imply behavioural change which is a requirement for successful organisational learning. To assess the effectiveness of the behavioural changes, the reflection stage should be entered.

There are various applications of learning processes but in general three types of learning can be categorised. These three types are summarized by Kennedy [13] as follows.

- Single-loop learning, which occurs when errors are detected and corrected and organisations continue with the present status quo without modifying present policies and goals. In essence, single-loop learning focuses on improving the status quo through small incremental changes in how organisations functions. An example in the area of information security could be a case of unauthorized access by a user to privileged data. A single-loop response would be to simply deny future access to this specific user. The status quo is maintained and present policies and/or goals are not modified.
- Double-loop learning challenges, and possibly makes changes to the status quo and the existing assumptions and conditions. It means that the organisation questions and modifies its existing norms, policies, procedures and objectives and it can lead to transformational change that radically alters the status quo. In the information security example mentioned, a double-loop response may be to investigate the circumstances and reasons for the unauthorized access. Double-loop learning may then occur when a decision is taken to improve (change) the process of allocating access rights in order to minimize future unauthorized access risks.
- Deutero learning involves focusing on the learning process itself. This type of learning seeks to improve how organisations perform single and double-loop learning. It can be described as "learning how to learn" and it occurs when organisations learn how to perform both single and double-loop learning.

Due to the focus on long term goals and the more complex nature of double-loop learning, most companies focus only on single-loop learning [16]. According to Van Niekerk and Von Solms [3] this is also true in the information security discipline. They pointed out that generative, or double-loop learning, emphasizes continuous experimentation and feedback.

Although there are a large number of studies on organisational learning, there are not particularly many studies that relate organisational learning to information security. Even so, the studies that have been conducted in this area prove that information security is an important area that offered ample opportunities, linked to organisational learning, that can make a significant contribution to organisations and their performance. Examples of studies where organisational learning and information security were explored include the following.

Van Niekerk and Von Solms [3] investigated, amongst other models, the use of an organisational learning model for information security education. Their aim was to ensure that adequate attention is given to behavioural theories in information security education programs. Albrechtsen [10] conducted a comprehensive study into the barriers that exist and that prohibit productive organisational learning from

information security incidents while Ahmat *et al* [16] suggested that the practice of incident response may lead to organisational learning. They proposed a double-loop learning model for security incident learning to address potential systemic corrective action. An interesting and authoritative study was conducted by Pfleeger and Caputo [2] where it was argued that blending behavioural sciences and cyber security may lead to the mitigation of cyber security risks. Although organisational learning was not specifically mentioned, the study strongly supports the idea that behavioural sciences (of which organisational learning is at least a sub-section) is relevant to information security in general. To further motivate this idea, Thomson and Van Niekerk [4] also contend that employee apathy towards information security can be addressed through the use of existing theory from the social sciences.

There are also a number of studies where the focus is not on information security per se but rather on how information technology in general relates to organisational learning. These studies usually concentrate on computer systems necessary to facilitate organisational learning and knowledge transfer [17], [18].

In the context of this paper, where it is claimed that a phishing exercise may lead to organisational learning, the next few paragraphs will briefly refer to the phishing concept and examples of studies related to it.

The basic idea of phishing is when someone attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity [8]. A more formal definition can be obtained from the Oxford English Dictionary [19] where phishing is defined as *the fraudulent practice of sending e-mails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.*

Phishing attacks are on the increase and successful attacks may have devastating effects on both enterprises and individuals. The Symantec Intelligence Report [20] of June 2012 reported that one out of every 170.9 e-mails sent during the month of June 2012, in South Africa, was a phishing scam. In the Netherlands the figure for June 2012 was one out of every 54.4 e-mails. Considering the billions of e-mail messages that are transmitted worldwide during a specific month, it becomes clear to what extend phishing attacks form part of the day to day electronic communication activities. With this in mind it becomes more and more important to implement the right and effective countermeasures to mitigate or prevent phishing attacks. One way of dealing with this growing number of phishing incidents is to implement security awareness and training programs where users are made aware of phishing scams. The use of practical tests seems to be a popular and effective way of making people aware of the dangers of phishing and some examples of the work conducted by other researchers in this area will be highlighted below.

Pattison *et al* [21] investigated the behaviour response of computer users when receiving either phishing e-mails or genuine e-mails. The study was conducted as a scenario-based role-play experiment where participants had to indicate what the appropriate response would be on certain e-mail messages. The study found that participants who were informed, prior to the experiment, that they are part of a phishing exercise performed better in handling phishing e-mail messages.

Simulated phishing attacks together with embedded training were used by Jansson and Von Solms [5] in an effort to cultivate users' resistance towards phishing attacks, while Kumaraguru *et al* [7] also conducted a study on anti-phishing training to proof that user training should be used in conjunction with technological solutions for security problems. Other studies include Dodge *et al* [9] who performed a practical phishing experiment involving students from the United States Military Academy, Jagatic *et al* [8] performed a study at the Indiana University, Steyn *et al* [22] conducted a practical experiment in South Africa and Hasle *et al* [23] a study in Norway.

It is interesting to note that all the practical phishing experiments referred to so far, were conducted using students as participants. Although these studies produced many advantages and insights, it is doubted whether the results can be generalised and extrapolated to industry enterprises.

Consistent with the research projects mentioned above, this study also performs a practical phishing experiment but uses an industry enterprise for research purposes instead of students in a university environment. In addition, the exercise is aimed at creating a climate for organisational learning. To ensure that the exercise is not a once-off event, the objective is to initiate a learning process and to show how security incidents such as phishing can and should be used for single and double-loop learning in an organisation.

The study was conducted at a large geographically dispersed utility. The organisation in question is a large multi-billion dollar entity with over 3500 IT users and they supply essential services to over 2 million customers. The organisation has an information security course that is mandatory for all employees and partners who have access to the IT infrastructure. The objective of the course is to make IT users aware of their responsibilities with regards to protecting the organisations' information and information systems from unauthorised access, loss or disclosure. Whilst the information security course is deemed mandatory, the records could not support this assertion as many staff was found not to have completed the course or no records could be found of their attendance.

3 Methodology

The successful implementation of an e-mail phishing exercise is dependent on how well certain issues, associated with the exercise, are considered. Jansson and Von Solms [5] categorised these issues into principles to be considered *before designing* the exercise, *before conducting* the exercise, *during* the exercise, and *after* the exercise while Dodge *et al* [9] simply refer to them as general and specific considerations. In this study considerations are also presented as general and specific considerations. The general considerations are concerned with those issues that may have an impact on the exercise as a whole while the specific considerations deal with aspects specific to the enterprise where the study was conducted.

General Considerations

The first and most important general consideration is the determination and definition of an objective. There should be a clearly defined goal and in this study the goal was

simply stated as the evaluation of security awareness associated with phishing and the creation of an opportunity for organisational learning to take place. The next consideration is critical for success i.e. to get ethical clearance and top management approval. This was achieved by conducting personal meetings with the CEO, the CFO and the IT manager where the purpose, actual steps and possible outcomes were explained. A formal project proposal detailing aspects such as the basic process, different phases, measures of success and possible risks, was also submitted for approval to management.

Other general considerations which were appropriately addressed included the timing of the exercise; maintaining the privacy of respondents; the selection of a random and representative sample of respondents; measurements to ensure that no information was disclosed prior to the exercise; and, a debriefing exercise following the test.

Specific Considerations

The central issue among the specific considerations was the construction of an appropriate e-mail message. The message had to be concise, credible and at the same time be enticing in order for participants to react.

To ensure that the phishing e-mail message complies with all the necessary requirements, it was decided to make use of aspects that may trigger certain emotions from participants. Jansson [6] presents a list of a large number of techniques that are based on negative, positive and neutral emotional exploits. For the construction of the e-mail message the following emotional exploits were used.

Legitimacy – when a user is made to believe that the source of the e-mail message is legitimate.

Authority – people tend to comply with instructions or requests issued by someone with authority.

Scarcity – when users believe that the time to react is limited.

Conformity – users who believe that other fellow-employees have already reacted to a request are inclined to also comply with the request.

Apart from these four techniques which were explicitly built into the e-mail message (see figure 2), three other important emotional exploits were also implicitly included. They were *urgency* (making users believe it is an emergency), *carelessness* (clicking on a link) and *diffusion of responsibility* (users believe that someone else is responsible for security). Users were asked to click on the link in the message which would then take them to another webpage where their usernames and passwords were requested. Figure 2 also indicates how the e-mail was constructed to provide clues to alert users that the message was likely not to be legitimate. The real name of the organisation has been changed in figure 2.

There were a number of other specific issues that also needed clarification before the actual exercise could take place i.e. it was important not to refer to any specific IT, security or internal audit staff as this may compromise the trust between users and

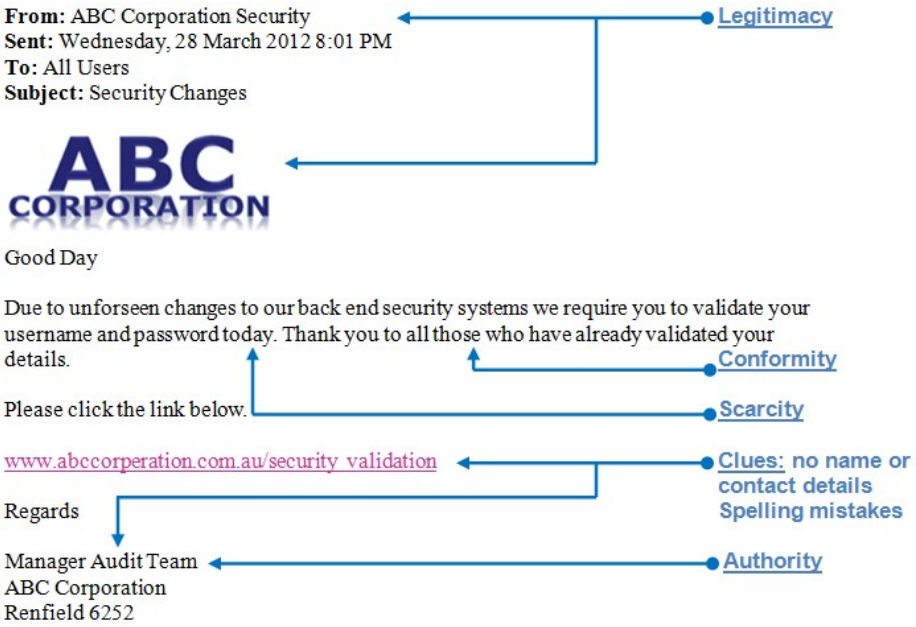


Fig. 2. Phishing e-mail message

staff. Steps also had to be taken to ensure that the enterprise's anti-phishing tools and spam filters do not identify the message as spam or a phishing scam, and Helpdesk had to be provided with a predetermined response should there be any queries from users. Provision was also made for respondents who reply directly to the phishing e-mail. Some of the technical considerations include the deletion of duplicate records (if a user responds more than once) and also a check to see whether the correct usernames were supplied (password were requested but not recorded).

The e-mail message (figure 2) was first sent to a small group of 10 employees. The objective was to test whether all technical aspects are functioning correctly and also to get feedback on possible improvements. After some minor changes were made, following the small pilot study, it was decided to go ahead and implement the phishing test.

The phishing e-mail message was sent to all employees at 8:00pm on a weekday night. The organisation is a 24-hour operation with activities taking place on a continuous basis. Statistics of user logs showed that there are on average about 1700 active IT users signed on during any night and to ensure that the night workers are included in the test, the 8:00pm sending time was chosen. This sending time would also guarantee that day workers should have the phishing e-mail in their inboxes first thing in the morning. The idea was to get users to respond early before they can discuss it with fellow employees.

A number of senior managers found the phishing e-mail very annoying and some of them sent out general e-mail messages to object to the phishing message (and the test). The security personnel were also involved and concern was expressed regarding

the possibility of an external attack aimed at disrupting essential services. Due to this, it was decided at 8:30am the next morning to remove the phishing message and to officially end the test. The reasons for withdrawing the phishing e-mail relatively early the next morning were firstly, to prevent large-scale disruptions and secondly, because enough data has been recorded at that stage to draw meaningful conclusions. The data and the experience were sufficient and interesting results, presented in the next section, were obtained.

4 Results

The data recorded from the phishing awareness exercise include the employee name, department where the person is working and the username. Passwords were also requested but not recorded due to privacy considerations. As part of the exercise, passwords were validated but only the result was recorded in a simple yes/no format. Appropriate safeguards to ensure privacy were put in place. The recorded employee names were purely recorded for statistical purposes and nowhere during reporting were specific names linked to responses. The reason for recording usernames was to perform a validation test to ensure that users do enter valid usernames (and by implication valid passwords). All duplicate records (users who entered their details more than once) and records with invalid usernames were removed from the final data set.

The main result, before any further analyses were performed, was the number of negative responses received. A negative response is a response where a user provided his or her username and password. During the test 280 users responded to the phishing message of whom 231 (83%) entered their usernames and passwords on the webpage. Of the 231 users, 23 (10%) entered their valid details more than once. Although there were approximately 1700 active users logged on during the test, it would be incorrect to assume that all of those who did not respond acted in a positive way. Reasons for this may be the fact that many people do not respond immediately to e-mail messages, some users may have left their workstations logged on during the night while not there, some users may have been engaged in other tasks and simply did not check their mail inboxes, etc. A much more significant analysis was to link the 280 users who responded, to the information security course that all staff members are required to complete and which would have provided them with basic security information on how to react to possible phishing scams. Figures 3(a) and (b) show the results graphically. Figure 3(a) shows that an unexpected 69% of those users who entered their passwords did complete the security training in the past. Figure 3(b) shows the training details of those who responded without entering their usernames and passwords. These results indicate that there are at least two points of concern. Firstly, the high number of users who responded in a negative way despite their security training and secondly, the relatively high number of users that never completed the information security course.

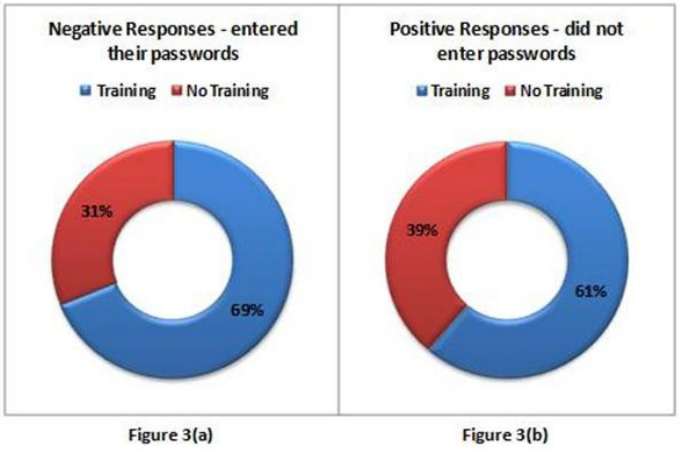


Fig. 3. Responses related to training completed

Figure 4 shows an analysis of responses (percentages) per experience category for those who entered their usernames and passwords. Experience in this case refers to the number of years a person is employed at the organisation. From figure 4 it can be seen that those employees with less experience at the organisation (and therefore less exposure to its security practices and policies) are more inclined to give away personal details. More than a third (35%) of those who entered their usernames and passwords have less than 5 years experience with more than half (52%) less than 10 years.

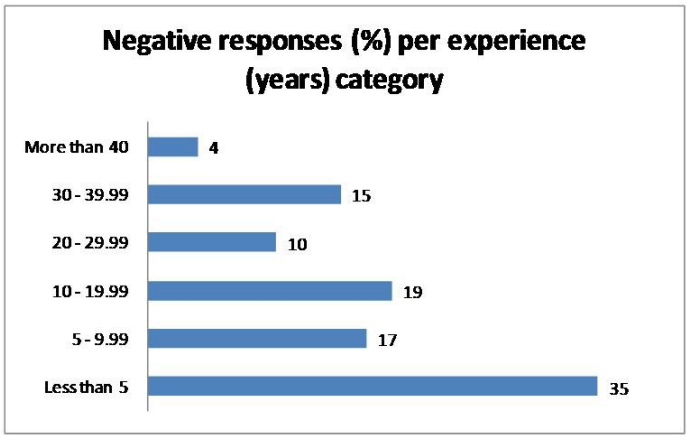


Fig. 4. Responses per experience category

The data that was captured during the exercise makes it possible to perform a number of analyses, e.g. responses per department, gender, age group etc. These types of analyses were not done in this study as the focus was more directed at possible organisational learning opportunities.

As explained earlier, organisational learning involves the adjustment of actions based on an experience. These adjustments, or learning, can then be categorised as single or double-loop learning. The results from this study have shown that the phishing experiment offers the ideal opportunity for learning and that both single and double-loop learning has taken place.

Single-loop learning took place in the form of small changes in making staff aware of the risks and consequences of phishing scams. Instructions concerning basic acceptable behaviour related to suspicious e-mail messages were also issued. Specific actions that can be attributed to single-loop learning include the following.

- The first day, following the phishing exercise, the Manager Risk and Assurance sent out an e-mail message to all staff informing them about the exercise and, more importantly, making them aware of the risks and giving them basic instructions on how to react to these type of e-mails (e.g. to report it to the Service Centre).
- The company's weekly in-house bulletin was used to reinforce the security awareness message and to instruct staff to complete the company's computer based information security course. This was done for two consecutive months following the phishing exercise.

The single-loop learning examples mentioned here did not change the status quo of any process but were quick and effective corrective measures to address a specific problem area. There were, however, other issues that needed a more comprehensive investigation that may lead to a change in policies and procedures. These double-loop learning issues include the following.

- All staff members are required to complete an information security course which will equip them with basic security knowledge for different security situations including phishing scams. An analysis of the phishing results showed that not all staff has completed the course. More importantly, a relatively large number of those who have completed the course had given their passwords away. An assessment of the course content and possible controls to ensure that everybody completes the course is planned. This may lead to a change in the current security policy on issues pertaining to basic security training.
- Another issue, planned for the future, which was highlighted during the phishing exercise relates to the gap between the different security views and expectations of managers and users. This gap is sometimes referred to as the information security digital divide between managers and users [24] and may lead to unrealistic security assumptions and management strategies that are not aligned with the dynamics of the user environment.

If one considers the results of the phishing exercise it seems permissible to draw the conclusion that the exercise has created opportunities for organisational learning. Basic problems were immediately corrected through an easy and uncomplicated single-loop learning approach while double-loop learning issues provided an opportunity for the organisation to adapt and adjust some of their information strategies.

5 Conclusions

Modern businesses are characterised by the increasing reliance on information assets. The protection of these assets depends to a large extend on the employees and users and it is not surprisingly that criminals tend to focus their attacks on humans. Phishing has become one of the most frequently used techniques to obtain personal or private information and to combat it, proper security awareness programs should be in place. To ensure that a security awareness activity does not become a once-off event, organisations may want to consider the use of various organisational learning models to enhance the awareness and educational value of such programs.

In this paper a successful practical phishing exercise was conducted at a large organisation. The aim was not only to record the number of users who are willing to give away personal information, but also to create an opportunity for organisational learning in order to improve the educational value of the phishing experiment. The results have shown that employees are prone to phishing attacks, but more importantly, the phishing exercise created an excellent opportunity for both single and double-loop learning activities. A single-loop learning approach was followed to immediately correct certain shortcomings without changing the status quo, while double-loop learning provided the opportunity to revisit and adapt some of the longer term information security strategies.

One security experiment linked successfully to organisational learning does not necessarily prove that all security exercises will lead to organisational learning. The exercise did, however, provide an insight into exciting possibilities to increase the value of security awareness exercises and that it may ultimately lead to the completion of the learning process described in section 2 of the paper.

References

1. Furnell, S., Clarke, N.: Power to the People? The Evolving Recognition of Human Aspects of Security. Computers and Security 31, 983–988 (2012)
2. Pfleeger, S.L., Caputo, D.D.: Leverage Behavioral Science to Mitigate Cyber Security Risk. Computers and Security 31, 597–611 (2012)
3. van Niekerk, J., von Solms, R.: Organisational Learning Models for Information Security (2004), http://icsa.cs.up.za/issa/2004/Proceedings/Full/043.pdf
4. Thomson, K., van Niekerk, J.: Combating Information Security Apathy be Encouraging Prosocial Organisational Behaviour. Information Management & Computer Security 20, 39–46 (2012)
5. Jansson, K., von Solms, R.: Phishing for Phishing Awareness. Behaviour & Information Technology (2011), doi:10.1080/0144929X.2011.632650
6. Jansson, K.: A Model for Cultivating Resistance to Social Engineering Attacks, Unpublished M-dissertation, Nelson Mandela Metropolitan University (2011)
7. Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A., Pham, T.: School of Phish: A Real-World Evaluation of Anti-Phishing Training. In: Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS), pp. 3:1–3:12 (2009)
8. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menezer, F.: Social Phishing. Communications of the ACM 50(10), 94–100 (2007)

9. Dodge, R.C., Carver, C., Ferguson, A.J.: Phishing for User Security Awareness. Computers and Security 26, 73–80 (2007)
10. Albrechtsen, E.: Barriers against Productive Organisational Learning from Information Security Incidents. Paper in the PhD course Organisational Development and ICT, Norwegian University of Science and Technology (2003)
11. Schermerhorn, J.R., Osborn, R.N., Uhl-Bien, M., Hunt, J.G.: Organisational Behavior, 12th edn. John Wiley & Sons, Inc., NJ (2012)
12. Lopez, S.P., Peon, J.M.M., Ordas, C.J.V.: Organisational Learning as a Determining Factor in Business Performance. The Learning Organisation 12(3), 227–245 (2005)
13. Kennedy, E.: A Critical Evaluation of the Organisational Learning that takes place in a Project Management Environment. Unpublished M-dissertation, North-West University (2008)
14. Argyris, C., Schon, D.: Organisational Learning II: Theory, Method and Practice. Prentice Hall (1996)
15. Buckler, B.: Practical Steps towards a Learning Organisation: Applying Academic Knowledge to Improvement and Innovation in Business Processes. The Learning Organisation 5(1), 15–23 (1998)
16. Ahmad, A., Hadgkiss, J., Ruighaver, A.B.: Incident Response Teams – Challenges in Supporting the Organisational Security Function. Computers and Security 31, 643–652 (2012)
17. Kane, G.C., Alavi, M.: Information Technology and Organisational Learning: Investigation of Exploration and Exploitation Processes. Organization Science 18(5), 796–812 (2007)
18. Chou, S.: Computer Systems to Facilitating Organizational Learning: IT and Organizational Context. Expert Systems with Applications (24), 273–280 (2003)
19. Oxford Dictionary (November 2012), http://oxforddictionaries.com/definition/english/phishing
20. Symantec Intelligence Report (June 2012), http://www.symantec.com/content/en/us/enterprise/other_resources/b_intelligence_report_06_2012.en-us.pdf
21. Pattinson, M., Jerram, C., Parsons, K., McCormac, A., Butavicius, M.: Why do some People Manage Phishing E-mails Better than Others? Information Management and Computer Security 20(1), 18–28 (2012)
22. Steyn, T., Kruger, H.A., Drevin, L.: Identity Theft – Empirical Evidence from a Phishing Exercise. In: Venter, H., Elofif, M., Labuschagne, L., Elofif, J., von Solms, R. (eds.) New Approaches for Security, Privacy and Trust in Complex Environments. IFIP, vol. 232, pp. 193–203. Springer, Boston (2007)
23. Hasle, H., Kristiansen, Y., Kintel, K., Snekkenes, E.: Measuring Resistance to Social Engineering. In: Deng, R.H., Bao, F., Pang, H., Zhou, J. (eds.) ISPEC 2005. LNCS, vol. 3439, pp. 132–143. Springer, Heidelberg (2005)
24. Albrechtsen, E., Hovden, J.: The Information Security Digital Divide between Information Security Managers and Users. Computers and Security (28), 476–490 (2009)

Chapter 5

Considering the influence of human trust in practical social engineering exercises.

5.1 Introduction

Chapter 5 is presented in the form of a peer reviewed conference manuscript that was published in the 13th International Information Security South Africa Conference (ISSA). Johannesburg, 13-14 August 2014. ISBN: 978-1-4799-3383-9. IEEE Catalogue Number: CFP1466I-CDR.

This paper describes a specific trust survey linked to the practical social engineering tests. The results confirm that human trust plays a role in information security behaviour and it also provides an early indication that risk homeostasis should be considered as a factor in information security.

Figure 5.1 (on the next page) shows how the chapter is linked to the research objectives and research questions. This is then followed by the article as it was published. Guidelines of the journal are presented in Appendix H.

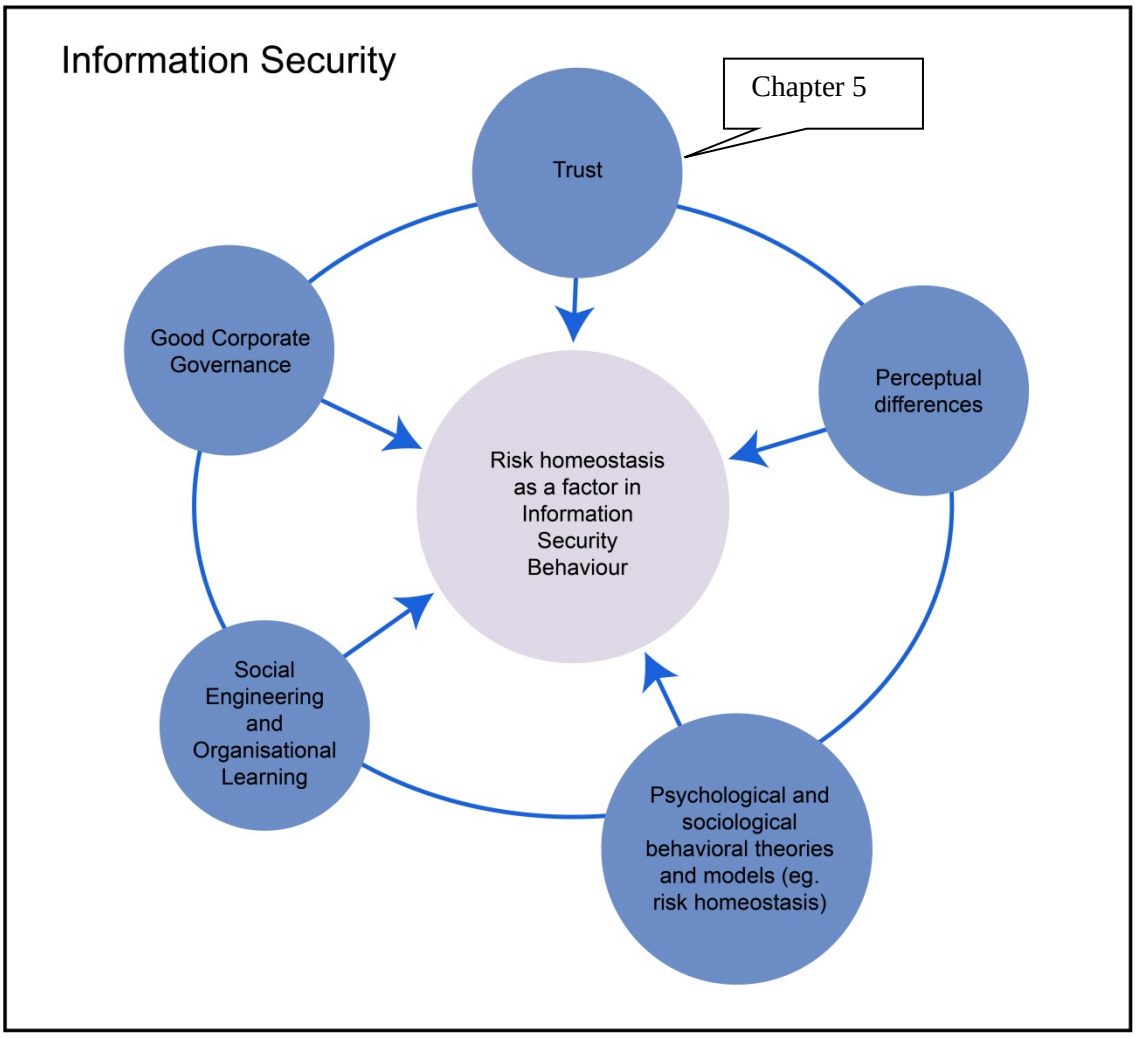


Figure 5.1 – Chapter 5 as part of the research study

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

Considering the influence of human trust in practical social engineering exercises

WD Kearney
School of Computer, Statistical and Mathematical Sciences
North-West University
Potchefstroom, South Africa
Kearneys@iinet.net.au

HA Kruger
School of Computer, Statistical and Mathematical Sciences
North-West University
Potchefstroom, South Africa
Hennie.Kruger@nwu.ac.za

Abstract— **There are numerous technical advances in the field of information security. However, the application of information security technologies alone is often not sufficient to address security issues. Human factors play an increasing role in securing computer assets and are often detrimental to the security of an organisation. One of the salient aspects of security, which is linked to humans, is trust. It is safe to assume that trust will play an important role in any information security environment and may influence security behaviour significantly. In this paper the results of a practical phishing exercise and a trust survey are considered. The research project is part of a larger project and the phishing exercise is a follow-up to an earlier first practical phishing test. Results of the phishing test are compared with the first exercise. In addition, the newly obtained trust information from the survey is also incorporated into the report in order to try and explain security behaviour. The research was performed at a large organisation. Results indicate that although there is a general high level of trust in the organisation's ability to provide safe and secure information systems, a large number of staff was still victim to a simple phishing exercise. A possible explanation, which opens up further avenues for research, is offered.**

Keywords – Information security; Social engineering; Phishing;Trust

I. INTRODUCTION

Information security professionals know that users are often the weakest link in the information security chain. The famous hacker Kevin Mitnick had much success using social engineering – tricking people to give away sensitive data such as passwords [1]. There is a body of literature that shows technical controls work more effectively than the ability to manage the human aspects of information security. However, an important distinction that needs to be made is that technology is not the only answer in addressing information security risks, with attitudes and user perceptions playing an important part [2], [3].

More and more people are coming to realise that security failures are often due to issues other than the lack of suitable technical protection mechanisms. Some aspects are shown in the rapidly growing field of research in "Economics of Security" [4]. As part of this field, Moore and Anderson [5] describe active research with breaches of personal information and behavioural analysis.

The importance of addressing the human aspect in information security has grown over the past few years. One of the most frequent used techniques used to obtain private or confidential information from humans is phishing. Phishing is a kind of embezzlement that uses social engineering in order to obtain personal information from its victims, aiming to cause losses [6]. The Oxford English Dictionary [7] formally defines phishing as the fraudulent practice of sending e-mails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.

The Symantec Internet Security Threat Report [8] of April 2013 reported that e-mail phishing rates are down from one in 299 emails in 2011 to one in 414 in 2012. This does not, however, imply that the risk of being deceived has been reduced. The reason for this slight decrease is attributed to a shift in activity from email to social networks. Considering the billions of e-mail messages that are transmitted annually worldwide, it is clear that phishing attacks still form a considerable part of the day to day electronic communication activities and even with the slight decrease reported by Symantec, successful attacks may have a devastating effect on both enterprises and individuals. With this in mind it is safe to assume that technical as well as human controls become increasingly more important to mitigate or prevent phishing attacks.

It is also safe to assume that trust will play a significant role in any information security environment as good security will probably improve trust. Users' perceived security and perceived trust are closely related and it is therefore appropriate to consider human trust perceptions when dealing with social engineering and security awareness in general. There are many similar definitions of trust, the Macquarie Online Dictionary [9] describes trust as "on whom or that on which one relies" whilst another online dictionary definition states it as "a confidence that something is safe, reliable, or effective" [10]. The key words revolve around confidence and reliability. If one is confident that something is safe, reliable and effective, there would be a higher level of trust in that matter. Trust in this case refers to the human nature and not

the computational notion of trust. It also refers, in this paper, to the sense of security or comfort a user has in the corporate environment, i.e. the level of confidence the user has in using the various systems.

This paper describes a practical social engineering experiment that was performed at a large organisation as a follow-up exercise to a previous practical exercise [11]. Apart from a mere comparison with previous results, a trust survey was also conducted to determine if trust has any influence in users' behaviour. The remainder of the paper is organised as follows. Section II presents, as background, a few examples of related research and also gives a very brief summary of the previous social engineering exercise. The methodology followed in this study is outlined in section III while section IV presents the results and a discussion of the current exercise. The paper is then concluded with general concluding remarks in section V.

II. Background and Related Work

A popular and effective way of addressing the human side of security is to focus on some form of an information security awareness program. Such a program can then concentrate on specific areas such as social engineering in general or phishing in particular. This is usually also an opportunity to emphasize the role of trust in an information security setup. There exist a large body of literature on these topics and the next few paragraphs will present some examples of such studies.

The acknowledgement that security breaches can be attributed to the behavior of computer users has led to a number of studies that were directed to users. Parsons *et al* [12] have developed a questionnaire to determine employee awareness by focusing on human aspects, while Crossler *et al* [13] highlighted directions for behavioral research in information security. Other examples of recent studies in this area can be found in [14] and [15].

Research studies on phishing, especially simulated attacks as reported on in this paper, were detailed in the first study of which this one is a follow-up and can be found in [11]. More recent examples can also be found in [6] and [16].

The possible role of trust forms an integral part of this paper and is consistent with other studies in this area. It is not unusual to find studies where trust is assessed in different systems or environments. Examples include trust in e-health systems [17], cloud computing [18], online purchasing [19] and e-payment systems [20].

As part of an ongoing study in understanding the management of information security risks, a first practical phishing exercise was conducted at a large geographically dispersed utility in 2012 and reported on in [11]. The organisation where the test was conducted is a large multi-billion dollar entity with over 3500 IT users and they supply essential services to over 2 million customers. During this first test, 280 users responded to a phishing message of whom 231 (83%) entered their usernames and passwords on a webpage. Of the 231 users, 23 (10%) entered their valid details more than once. A number of practical learning objectives were identified from the results of the first exercise. As part of this study, a follow-up practical test was undertaken together with a survey of users and management to assess their level of trust in the organisation's information systems.

III. Methodology

The methodology followed in this study comprised of two main steps. First, a questionnaire based survey was conducted to a broad spectrum of personnel to determine if any had been victims of a cybercrime, and also to establish whether those users had a level of trust in the corporation's ICT systems and infrastructure. This was then followed up by a practical e-mail based phishing exercise. The results of the phishing exercise were then evaluated and comparisons made to the original exercise [11] to determine if any change in behaviour had occurred or if any meaningful insights could be gained.

A. Trust survey

To gauge levels of trust and determine whether staff had been a victim of cybercrime before, a questionnaire was developed. The questionnaire consisted of 20 questions that were constructed based on management input and certain literature resources. The questions were specific to the organisation where the study was conducted and was tested with a small number of employees in a pilot run.

A sample of 40 users was used in the survey and included executive members, management and staff over a broad spectrum of the business. An appropriate sample size was difficult to determine as there were a myriad of factors that had to be taken into account, e.g. the sensitivity of the subject limited the sample size in this specific case. It was therefore decided to determine the sample size through a "saturation point" which is a standard stopping rule for research of this nature. Glaser and Strauss [21] used the term "theoretical saturation" which means that no additional data is found by the researcher for a specific category in a study. A disadvantage of this technique is of course that one would never know if new information can be obtained by questioning or interviewing an additional staff member. The same is however true for a statistically determined sample size. To ensure an appropriate response and to comply with the requirements of a saturation point stopping rule, the questionnaires were completed on an interview basis. An additional advantage of this approach was that the questions can be explained to respondents and in doing so ensure that all respondents understand the questions in the same manner. This hopefully increased the integrity of responses received.

Some of the questions had to be answered simply by indicating a yes or no. The objective of these questions was to establish a baseline e.g. whether users had been victims of cybercrime in the past 12 months. The majority of the questions had to be answered on a 5-point Likert scale and was aimed at assessing trust levels e.g. "*To what extend do you believe the Corporation provides a safe and trustworthy environment?*" There were also a few questions designed to deal primarily with the users' perception of whether they thought they had enough insight to both understand and manage their information risks. An example of such a question, which also had to be answered on a 5-point scale, is

the following. *"Do you have enough knowledge or information to manage your information risks?"* Interesting results were obtained from this first part of the study and will be presented in the section IV.

B. Phishing exercise

The practical phishing exercise implemented the same general and specific considerations used in the first exercise as discussed in detail in [11] except for a small change in the actual wording of the message. The structure and format of the e-mail was substantially similar but the message, whilst still relying on an explicit emotional exploit of scarcity, was modified to say: *"With our new password complexity rules, we require you to validate your username and password. If you act today, you will be in the draw to win a prize"*. One of the reasons for doing this was that the Symantec Internet Security Threat Report [8] stated that there is an increase of phishing scams that utilise fake websites and offer non-existent prizes.

This modification strengthened the legitimacy emotional exploit as the organisation where the exercise was conducted had recently modified their password complexity rules and length of password expiry as part of their ongoing information security risk management processes. This had been communicated throughout the organisation by poster, e-mail and articles in the in-house online magazine. The use of a prize was an added incentive.

To be able to perform a valid comparative analysis, the actual phishing exercise was conducted in the same manner as the first one and the same parameters were used. These parameters include sending out the message to all employees at 8:30 pm on a weekday night (the organisation is a 24-hour operation with activities taking place on a continuous basis). The reasons for this were the same as with the first exercise - to ensure that night workers are included in the test and to guarantee that day workers receive the message first thing in the morning. Following some concerns expressed with the first exercise, certain enhanced control measures were implemented, including ensuring the appropriate security personnel were notified. This follow-up actual test was allowed to run for an extended time. The extra time has provided further data for analysis which may provide further insight into the management of this important risk aspect. However, for the data analysis, only the dataset for the 12 hour test interval (the same as for the first exercise) were used.

Apart from the above specific issues, all general considerations to ensure the success of the project were also addressed, e.g. the obtaining of clearance and permission from the Chief Executive Officer to conduct the exercise, maintaining privacy of respondents etc.

IV. Results and Discussion

This section presents the results of the trust survey, the phishing exercise and comparative results with the initial first phishing experiment conducted in [11]. A possible explanation, especially with reference to the trust aspect, will also be presented.

A. Results of the trust survey

The overall result of the trust survey was clearly that there is a high level of trust amongst employees in the ability of the Corporation to provide a safe, secure and trustworthy environment. The following three questions are examples of evidence of this high level of trust that exist (all three were answered on a 5-point scale).

Q1: Do you think the Corporation protects and secures email communications and related data adequately? All respondents reacted by indicating that they believe that protection is adequate (either a 1 or a 2 on the 5-point scale – a 3 and higher indicates that they doubt the issue). This question is specifically significant to the email phishing exercise that was also conducted.

Q2: Do you feel confident enough in the corporate systems to do your online banking? The result was exactly the same as for the first question – all respondents feel confident to do online banking using corporate systems. This clearly implies a high level of trust in the corporate systems.

Q3: To what extent do you think the Corporate provides a secure or trustworthy IT environment? More than half, 57% rated it as a 1 (very secure) with 37% rated it as 2 (somewhat secure). Only 5% rated it as 3 (neutral) and no respondents rated it as 4 (not very secure) or 5 (very insecure). Figure 1 shows the results for this question graphically.

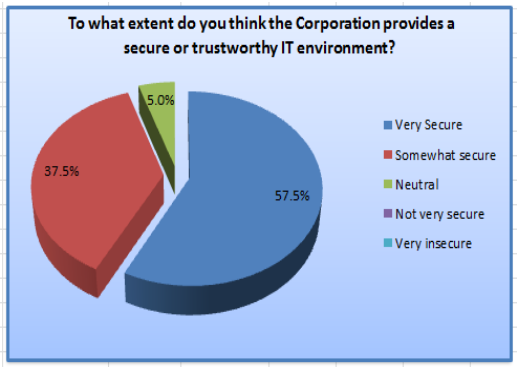


Figure 1. Secure and trustworthy environment

Another relevant question, mentioned in the methodology section, was *"Do you have enough knowledge or information to manage your information security risks?* The answers were somewhat illuminating in that only a small percentage of respondents believed they did not have enough information. Figure 2 graphically shows that over half were either somewhat (47.5%) or completely (12.5%) confident that they had enough knowledge to manage risks. The work of Schneier [22] shows that, on average, approximately 62% of employees have limited knowledge of information security risks whereas for this study 60% showed a positive slant – another indication of the high level of trust of employees in the Corporation and in their own security risk management capabilities.

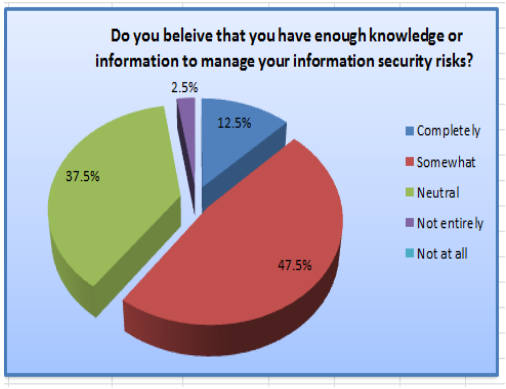


Figure 2. Knowledge to manage information risks

A final, interesting, remark on the trust survey is that more than half (55%) of the respondents had been a victim of any form of cybercrime in the past 12 months. This is notably higher than the reported 46% of computer user adults who had fallen victim of cybercrime in the last year [23].

B. Results of the phishing exercise

The same data as in the first test were recorded. This included user identification, section or department where the person works and time of access. Passwords were requested and were also validated through a technical process. To protect users' privacy, no passwords were recorded – only a simple yes or no was recorded depending on whether a valid password was entered or not. To ensure an acceptable level of data integrity, all duplicate records (users who entered their details more than once) and records with invalid usernames were removed from the final data set.

During the measured 12 hour time period of the test, 490 users responded to the phishing message of whom 312 (64%) entered their correct usernames and passwords on the webpage. A further 25 (5%) entered incorrect passwords and 154 (31%) users accessed the website but did not enter any credentials. A significant and somewhat disappointing statistic was the 48 users who accessed the website and who were repeat offenders in that they had entered their password correctly in the previous test. A total of 30 (63%) of these repeat offenders had entered their correct passwords again in the current exercise. Table 1 gives an overview of the statistics of users during the phishing exercise.

TABLE I. USER STATISTICS DURING THE PHISHING EXERCISE

Total employees	3500
Total number of users logged on for test	1400
Number of users who responded to the phishing message	490
Number of users who responded and who entered their passwords	312
Number of repeat offenders (first and current test)	48

It should be noted that although there were approximately 1400 active users logged on during the test, it would be incorrect to assume that all of those who did not respond recognised the phishing scam. There are certain reasons why many users did not respond to the phishing e-mail message. Some of the reasons include the fact that many people do not respond immediately to e-mail messages, others may have recognised the email for what it was and immediately deleted it, some users may have been engaged in other tasks and simply did not check their mail inboxes, etc.

One of the significant statistics computed during the first test was the number of users who entered their correct passwords and who has also completed a security training course. The objective of this security training course is to provide users with a basic level of security awareness so that they would be able to identify threats such as phishing scams. During the first test [11], 69% of the users who entered their correct passwords have also completed the security training. In this current test, the figure is very high at 92%.

The comparative results between the first test in [11] and this current follow-up test are summarised in table 2.

TABLE II. COMPARATIVE RESULTS OF THE TWO PHISHING EXERCISES

	First test [11]	Current follow-up test
Nr of responses	280	490
Nr of users who entered their user id's and passwords correctly	231 (83%)	312 (64%)
Nr of users who entered their passwords correctly and who previously completed security training	159 (69%)	288 (92%)

It is clear from table 2 that the results are quite unexpected and maybe somewhat disappointing. More people responded to the phishing e-mail message than in the initial exercise. Although there was a decrease in the percentage of users who entered their passwords, the physical number of users who did this increased by 81. The percentage number of users who completed the security training course and still gave away their passwords has also increased from 69% to 92%. This is an indication that the same concerns raised in the first exercise, still exist. These concerns are firstly, the high number of users who responded in a negative way despite their security training and secondly, the fact that there are still a number of users that never completed the compulsory information security course.

The results were also used to try and establish whether there is a link between experience (years of service) and being a victim of the phishing scam. In the first study it was found

that more than a third (35%) of those who entered their usernames and passwords has less than 5 years of experience and more than half (52%) had less than 10 years of experience. This was an indication that younger people (with less experience) are more prone to these types of security attacks. The results in this study confirmed this idea with just more than 50% of users who gave away their passwords having less than 5 years of experience, and a further more than 16% with less than 10 but more than 5 years of experience. These results are consistent with other research studies which focused on the same issues. Sheng *et al* [24], for example, used an online survey to try and determine who fell for phishing attacks. Their report shows that people aged 18-25 are more likely to be victims of a phishing scam when compared to the general population. Figure 3 shows an analysis of responses per experience category for this current study.

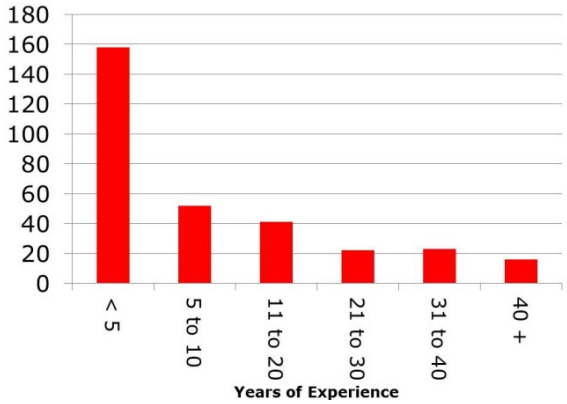


Figure 3. Responses per experience category

To summarize the results so far, it is clear that there is a high level of trust amongst users in their organisation's ability to provide a safe and secure information environment. Users also feel that they have on average enough skills and information to manage information security risks. However, a look at the results of the practical phishing test shows that a number of users became victims to the scam. It also appears as if they did not learn much from the previous test. The question now arises why this apparent contradiction in results? The next section will offer brief ideas or possible explanations for this situation.

C. *Possible explanations*

It seems like an anomaly when staff in an organisation fell, in large numbers, victim to a phishing scam while there is such a high level of trust in the organisation's information security environment. In addition, staff has indicated that they have sufficient knowledge to manage information security risks. The question arises why then do so many of them give away their passwords on web pages when asked for it?

The answer probably lies in the fact that information security is highly dependent on human factors. Aspects such as cognitive abilities, personal traits, perception of risk etc., plays a significant role and are most likely to impact security behavior. This case study has shown that the overwhelming majority of respondents have a positive perception of their own and their organisation's ability to protect them against security incidents such as phishing. High levels of trust seem to lead to carelessness where people are more easily tricked into security scams. It almost seems as if the level of trust impacts the level of risk behavior. This may be explained as follows.

Peltzman [25] put forward the concept of risk compensation in the safety arena to explain driver behaviour in adjusting individuals' levels of risk. Drivers would take more chances if they felt they were in a safer environment. Wilde [26] used this approach to develop the risk homeostasis theory. Risk homeostasis is based on the concept that people have a perceived or expected level of tolerable risk [27]. If there is a change in this level of risk they may compensate for it by changing their behaviour. For example, if the level of risk experienced by someone is low in comparison to the expected level of risk, he/she might engage in actions that will increase their exposure to risk. Conversely, if the level of experienced risk is higher than is acceptable, he/she may make an attempt to exercise greater caution.

This relates to information security in the sense that employees may become less vigilant or more careless when they know that good and adequate controls are implemented. E.g. users may become more easily victims of social engineering techniques such as phishing because they know (or perceive that) their organisation has the necessary controls (e.g. spam filters) in place? According to Pattinson and Anderson [27] there is not much doubt that risk homeostasis probably applies in many information security scenarios. They stated that risk homeostasis is after all a management theory and information security is all about managing risks. A similar link can be found in the medical field where some people believe that vaccinating young women against the human papillomavirus (HPV) will increase risky sexual behaviour [28] or in studies of sexual risk compensation such as in [29].

The trust survey conducted in this research has shown that users have a high level of trust in the Corporation's systems – at the same time a considerable number of employees fell victim to the phishing experiment. This seems to be in line with the above explanation of risk homeostasis. The level of risk experienced by users are low (results from the trust survey that indicates a high level of trust); users then compensate for this low risk by changing their behavior (taking more risks) and in so doing become phishing scam victims.

This paper forms part of a larger research project and in a next step of this larger project the role of risk homeostasis will be explored in more detail and reported on. It is hoped that the above theory on risk homeostasis will then be proved with more concrete examples and arguments.

V. CONCLUSION

With the acknowledgement that human factors play a significant role in the protection of information and information assets, the task of safeguarding these assets has

become more complex. To provide for risk perceptions, different attitudes and different levels of security knowledge is not an easy task. Criminals know that and focus their attacks on humans. A popular way of doing this is through social engineering attacks, more specifically phishing.

This paper forms part of a larger and ongoing project to investigate issues surrounding social engineering. In the first part of the project a practical phishing test was conducted at a large organisation. The results of this exercise were reported in [11]. In this current phase (this paper) a follow-up phishing test was performed at the same organisation. In addition, a trust survey was conducted to establish whether levels of trust may or may not play a role in being caught in a phishing scam. Interesting results were obtained. There was no real improvement in the number of people caught in the phishing scam; however, the trust survey revealed that respondents have a high level of trust in their own risk management abilities as well as in the ability of the organisation to provide them with a safe and secure information systems environment. No crystal clear explanation for this exist and the conclusion was that it is probably a case of risk homeostasis where users adjust their behavior (taking risks) to compensate for perceived low levels of existing risk (as indicated by the high level of trust).

There is already progress made with an ongoing research and investigation project that explores the risk homeostasis concept and applicability further. This is in an effort to gain more insight into the risk and security behaviour of people, especially in social engineering attacks.

REFERENCES

[1] K. Mitnick, The art of deception: Contolling the human element of security. Wiley, New York, 2002.

[2] S. Furnell and N. Clark, "Power to the people? The evolving recognition of human aspects of security," Computers and Security, 31, pp. 983-988, 2012.

[3] S. L. Pfleeger and D. D. Caputo, "Leverage behavioral science to mitigate cyber security risk," Computers and Security, 31, pp. 597-611, 2012.

[4] R. Anderson, "Economics and security resource," http://www.cl.cam.ac.uk/~rja14/econsec.html, Acessed: March 2014.

[5] T, Moore and R. Anderson, "Economics and internet security: A survey of recent analytical, empirical and behavioral research in internet security," in The Oxford handbook of the digital economy, M. Peitz and J. Waldfogel, Eds. Oxford University Press, 2011.

[6] C. K. Olivo, A. O. Santin and L. S. Oliveira, "Obtaining the threat model for e-mail phishing," Applied soft computing, 13, pp. 4841-4848, 2013.

[7] Oxford Dictionary, http://oxforddictionaries.com/definition/english/phishing, Accessed: February 2014.

[8] Internet Threat Security Report. Symantec Corporation, vol. 18, April 2013.

[9] Macquarie Dictionary, http://www.macquariedictionary.com.au, Accessed: February 2014.

[10] Macmillan online dictionary, http://www.macmillandictionary.com/dictionary/british/trust_23, Accessed: February 2014.

[11] W. D. Kearney and H. A. Kruger, "Phishing and organisational learning," in SEC2013, IFIP AICT 405, L. J. Janczewski, H. Wolf and S. Shenoi, Eds., pp. 379-390, 2013.

[12] K. Parsons, A. McCormac, M. Butavicus, M. Pattinson and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," Computers and Security, in press, 2014.

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

[14] T. Sommestad, J. Hallberg, K. Lundholm and J. Bengtsson, "Variables influencing information security policy compliance. A systematic review of quantitative studies," Information Management and Computer Security, vol. 22(1), pp. 42-75, 2014.

[15] K. Rantos, K. Fysarakis and C. Manifavas, "How effective is your security awareness program? An evaluation methodology," Information Security Journal: A global perspective, 21, pp. 328-345, 2012.

[16] S. Furnell, "Still on the hook: The persistent problem of phishing," Computer Fraud and Security, pp. 7-12, October 2013.

[17] S. Bahtiyar and M. U. Caglayan, "Trust assessment of security for e-health systems," Electronic Commerce Research and Applications, in press, 2013.

[18] R. Bose, X. Luo and Y. Liu, "The roles of security and trust: Comparing cloud computing and banking," Procedia – Social and Behavioral Sciences, 73, pp. 30-34, 2013.

[19] P. McCole, E. Ramsey and J. Williams, "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns," Journal of Business Research, 63, pp. 1018-1024, 2010.

[20] C. Kim, W. Tao, N. Shin and K. Kim, "An empirical study of customers' perceptions of security and trust in e-payment systems," Electronic Commerce Research and Applications, 9, pp. 84-95, 2010.

[21] B. G. Glaser, and A. L. Strauss, The discovery of grounded theory: strategies for qualitative research. New York, 1967.

[22] B. Schneier, "Insider threat statistics," http://www.schneier.com/blog/archives/2005/12/insider_threat.html, Accessed: March 2014.

[23] Symantec, "2012 Norton Cybercrime Report," http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf Accessed: March 2014.

[24] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor and J. Downs, "Who fallsfor phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," Proceedings of the 28th International Conference on Human Factors in Computing Systems, pp. 373-382, 2010.

[25] S. Peltzman, "The effects of automobile safety regulation," Journal of Political Economy, vol. 83(4), pp. 677-726, August 1975.

[26] G. J. S. Wilde, Target risk. PDE Publications, Toronto, Canada, 1994

[27] M. R. Pattinson and G. Anderson, "Risk homeostasis as a factor of information security," http://www.igneous.scis.ecu.edu.au, Accessed January 2014.

[28] N. T. Brewer, L. C. Cuite, J. E. Herrington and N. D. Weinstein, "Risk compensation and vaccination: Can getting vaccinated cause people to engage in risky behaviours?," Annals of Behavioural Medicine, vol. 34(1), pp. 95-98, 2007.

[29] S. D. Pinkerton, "Sexual risk compensation and HIV/STD transmission: Empirical evidence and theoretical considerations," Risk Analysis, vol. 21(4), pp. 727-736, 2001.

Chapter 6

Can perceptual differences account for enigmatic information security behaviour in an organisation?

6.1 Introduction

Chapter 6 is presented in the form of a journal article that was published in *Computers & Security* (2016).

As part of the efforts to explain contradictory information security behaviour, this article describes a special focused survey on perceptual differences between different groups of people in an organisation. The results indicate that perceptual congruence is a pre-requisite for a successful information security environment. The paper then finally proposes a new model for a safe and secure information environment.

Figure 6.1 (on the next page) shows how the chapter is linked to the research objectives and research questions. This is then followed by the article as it was published. Guidelines of the journal are presented in Appendix I.

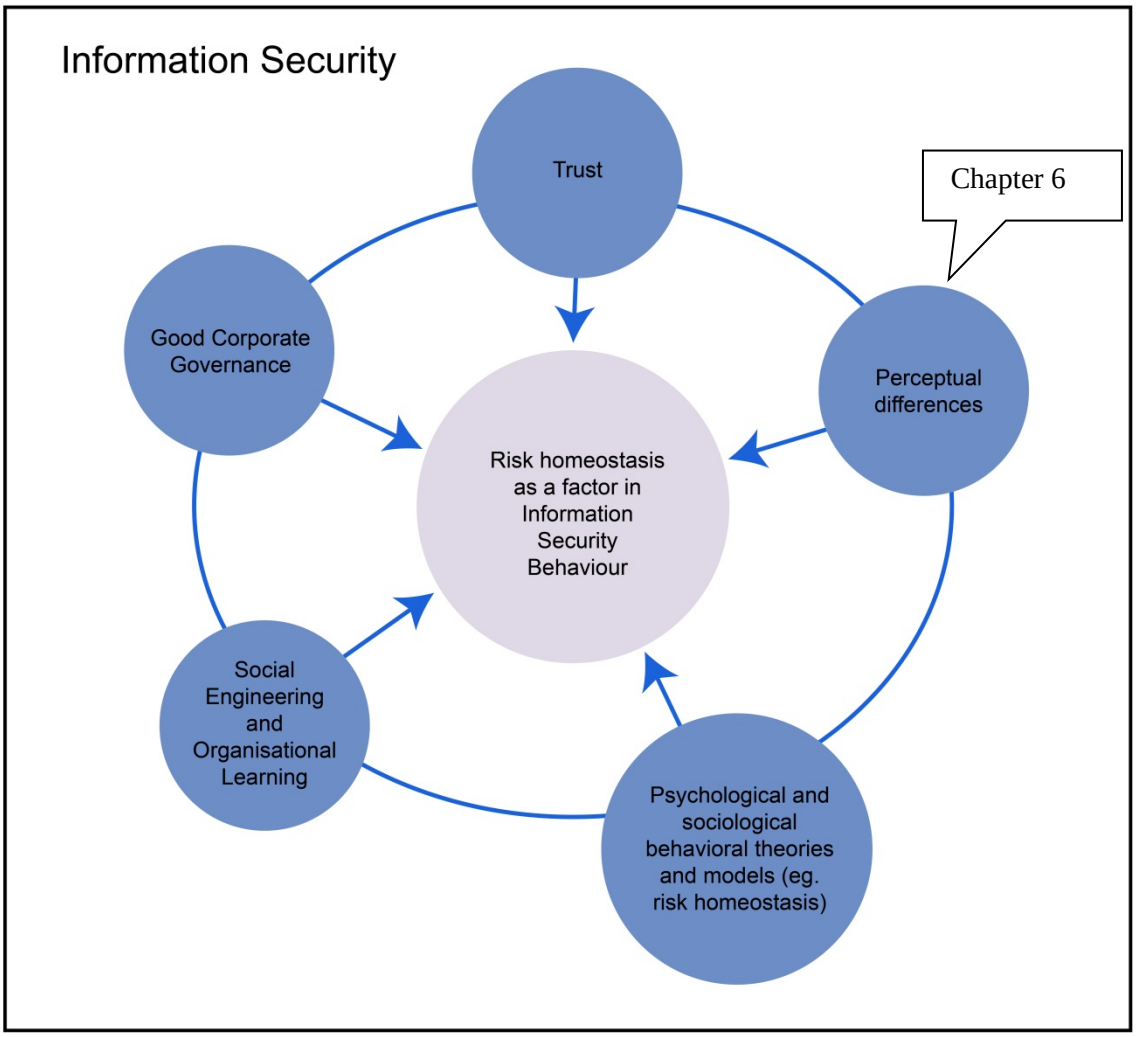


Figure 6.1 – Chapter 6 as part of the research study

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Can perceptual differences account for enigmatic information security behaviour in an organisation?

W.D. Kearney, H.A. Kruger *

School of Computer, Statistical and Mathematical Sciences, North-West University, Potchefstroom, South Africa

ARTICLE INFO

Article history:
Received 13 February 2016
Received in revised form 28 April 2016
Accepted 27 May 2016
Available online 31 May 2016

Keywords:
Information security awareness
Phishing
Social engineering
Information security behaviour
Trust
Perceptual differences

ABSTRACT

Information security in organisations is often threatened by risky behaviour of users. Despite information security awareness and training programmes, the human aspect of information security remains a critical and challenging component of a safe and secure information environment, and users reveal personal and confidential information regularly when asked for it. In an effort to explain and understand this so-called privacy paradox, this paper investigates aspects of trust and perceptual differences, based on empirical research. Two preceding social engineering exercises form the basis of the research project and are also presented as background information. Following the empirical work, a safe and secure information model is proposed. It is then argued that perceptual alignment of different organisational groups is a critical and prerequisite requirement to reach information security congruence between groups of people. In the context of the proposed model, the perceptual differences also offer some explanation as to why users with high levels of security awareness as well as high levels of trust in own and organisational capabilities so often fall victim to social engineering scams. The empirical work was performed at a large utility company and results are presented together with appropriate discussions.

1. Introduction

Information security has become one of the most critical and important areas of interest in modern-day business. It is unlikely that information security specialists will not acknowledge the importance of the human factor in information security. This acknowledgement has led, and still leads, to a large number of different studies on how to understand and manage the various human aspects such as knowledge, attitude and behaviour in information security.

A number of researchers and practitioners argue that the solution to the general information security problem lies in the existence and quality of an information security policy. Sommestad et al. (2014), for example, have identified variables that may influence compliance with information security policies, whereas Ifinedo (2014) has studied information systems security policy compliance, taking the effects of socialisation, influence and cognition into account. It is interesting to note that a wide variety of studies exists in this context; in some cases, human characteristics that may seem to be rather unusual are linked to the compliance or non-compliance of information security policies. Kelecha and Belanger (2013) have illustrated this by investigating religiosity as a possible role player in the intention to comply with an information security policy. Other instances of studies in the area of information security policies can be found in Bulgurcu et al. (2010) and Whitman and Mattord (2003). Information security awareness

* *Corresponding author.*
E-mail addresses: Kearneys@iinet.net.au (W.D. Kearney), Hennie.Kruger@nwu.ac.za (H.A. Kruger).
http://dx.doi.org/10.1016/j.cose.2016.05.006

is an area that is often associated with information security policies and a large number of studies are regularly conducted in an effort to address the awareness and human factor in information security. These studies are normally focused on how to raise information security awareness levels (Alnatheer, 2015; Da Veiga, 2015; Safa et al., 2015), how to measure these levels (Chandrashekhar et al., 2015; Keser and Gulduren, 2015; Parsons et al., 2014), and the monitoring and management of security awareness levels (Rantos et al., 2012; Spandonidis, 2015).

There is also a significant number of security specialists who contend that the problem should be addressed by creating (and maintaining) a suitable security culture in an enterprise. A large body of knowledge on security culture exists and examples of the existing literature include the work of Da Veiga and Martins (2015), who focus on an information security culture assessment process to improve an information security culture, specifically in financial institutions. In a study by Alhogail (2015), the design and validation of an information security culture framework is described. This framework incorporates the domains of preparedness, responsibility, management and society and regulations, and should be useful to organisations who want to develop an effective information security culture. Critical success factors for an information security culture can be found in Alnatheer (2015), whereas Alhogail and Mirza (2014) provide an overview of the different information security culture definitions as well as a review of literature sources that deal with information security culture studies. Closely related to security culture studies is the trend to borrow from the social sciences and to use psychological, sociological and other models in the endeavour to gain more insight into the complexities of human behaviour in information security. Studies using this type of approach can be found in Enrici et al. (2010), Lafrance (2004) and Tsohou et al. (2015).

The abovementioned models and approaches are not solely capable of explaining human activities when it comes to information security – other issues and factors may also play an important role. One such an important aspect is trust, which may be considered as a "soft" security property (Jensen, 2015) that interacts with other perceptual, attitudinal and behavioural factors. The importance of trust as a key element in information security has resulted in many research studies (Martin et al., 2015; Miltgen and Smith, 2015). It is also not unusual to find examples of studies where trust is evaluated in a specific information area. Examples include studies of trust in Internet of Things (Sicari et al., 2015), trust in cloud computing (Shaik and Sasikumar, 2015) and trust in e-payment systems (Kim et al., 2010).

Despite all these and other studies, the concept of a "privacy paradox" still exists. The privacy paradox refers to individuals with an apparently high level of security awareness who place a high premium on their privacy, but are easily persuaded to reveal their personal or other confidential information. The reader is referred to the studies by Hull (2015), who discusses the problem from a more philosophical viewpoint, and Kokolakis (2015), who presents the results of a review of research literature on the privacy paradox. A further complicating factor is that organisations do not really collect or have data available on the impact of IT and information security. This means that perceptions play a key role when decisions pertaining to information security have to be made. Not only do these differences occur in perceptions amongst various industry types, but there may also be perceptual differences between staff and management in the same organisation. Tallon (2014), for example, points out that there is a lack of consensus amongst executives' perceptions of IT impact and value. Albrechtsen and Hovden (2009) go even further by referring to a digital divide between information security managers and users when it comes to information security practices. The study by Martin et al. (2015) provides further proof of the importance of expectations in information security. The authors examined the expectations of IT professionals towards online privacy and concluded that expectations often go unsatisfied – a finding that, according to the authors, builds further understanding of expectations and associated behaviours.

It is interesting to note Kokolakis's suggestion (2015) that future studies regarding the privacy paradox should report evidence that is based on actual behaviour. In line with this suggestion and with the brief introductory comments in mind, this study investigates aspects of trust and perceptual differences that are based on empirical research. The empirical research was done in Australia at a large utility company that is a capital-intensive and customer-focused entity with over 2 million customers. To put the size of the company into perspective, one can only mention that during the last financial year, it had over 750 million AU$ in capital works and over 850 million AU$ in direct operating expenditure. There are over 3500 IT users, and with regard to its external IT presence, the company recorded 1.4 million visitors to its website and answers over 800,000 telephone calls from customers annually. The work that was performed includes two practical social engineering exercises that formed part of the regular control testing at the organisation in question, a survey to determine the role of trust in these security breaches, as well as a follow-up survey to determine the perceptual differences (if any) between management and users. The first practical social engineering experiment was reported in Kearney and Kruger (2013), whereas the results of the second experiment and the trust survey were detailed in Kearney and Kruger (2014). These first three studies and the results that were obtained constitute the first part of a larger research project that has ultimately led to the exercise on perceptual differences. It is therefore important to refer to these studies as part of the larger study; they will thus be presented briefly as background information. The focus of this paper is to report on the methodology and results of the perception survey.

The remainder of the paper is organised as follows: The next section will provide the background information on the two social engineering experiments and the trust survey. These studies led to the investigation of possible perceptual differences that will be described in the third section. The paper is then concluded with some general remarks.

2. Background

A popular and frequently used technique to study human behaviour in information security is the use of practical experiments that are associated with social engineering and, more specifically, with phishing (Jansson and Von Solms, 2013; Kumaraguru et al., 2009; Pattinson et al., 2012). Owing to its

nature, phishing exercises also appear to be a natural starting point for the investigation of the privacy paradox. As part of a larger study to try and understand information security behaviour of users and the management of security risks, two practical phishing exercises were conducted. These experiments took place at the large utility company that has been described in the introduction. The results of these phishing experiments led to a follow-up study in trust, as well as another study on possible perceptual differences between management and users. In this section, the two phishing exercises and the trust survey are summarised as background information. More detailed feedback on these projects can be found in Kearney and Kruger (2013, 2014).

2.1. *The phishing exercises*

Phishing can formally be defined as "the fraudulent practice of sending e-mails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online" (Oxford Dictionary, 2013). Jagatic et al. (2007) explain "phishing" simply as an attempt to acquire sensitive information from a victim fraudulently by impersonating a trustworthy entity. The practical phishing exercises that were conducted in this research project are in line with the definitions and explanations of the phishing concept and the methodology that was followed can be summarised as follows:

Both experiments made use of an e-mail message in which users were asked to click on a link that took them to a webpage where their usernames and passwords were requested. The e-mail messages were carefully constructed to trigger certain emotions that were designed to elicit a response. This entices users to react. These emotional exploits include legitimacy (the source of the message is legitimate), authority (the message has been issued by someone with authority), scarcity (time to react is limited), and conformity (the belief that others have already completed the request). In both cases, the message was chosen to reflect a real current situation in the organisation. The message in the first experiment reads as follows:

> Due to unforeseen changes to our back-end security systems, we require you to validate your username and password today. Thank you to all of you who have already validated your details.

The message of the follow-up phishing experiment was worded as follows:

> With our new password complexity rules, we require you to validate your username and password. If you act today, you will be in the draw to win a prize.

Each message has two additional clues to alert users that it may be fake messages. The first clue is an obvious spelling mistake (of the organisation's name) in the link on which users were asked to click. The other clue is the fact that no name or contact details are provided at the end of the message – the messages are simply signed by "Manager Audit Team", followed by the organisation's name.

All the normal planning activities, for example, objective setting, risk analysis, contingency and backup preparation, staff communication, timing and maintaining privacy, were completed. In addition, ethical clearance and top management approval were obtained. This was achieved by conducting personal meetings with the CEO, the CFO and the IT Manager where the purpose, actual steps and possible outcomes of tests and surveys were explained. Written clearance and consent was then given by the CEO. Following a small pilot study to test the technical aspects and obtain feedback on the planned tests, the first message was sent out to all employees. The message was available for 12 hours before it was withdrawn.

Data that were recorded during the phishing exercises included the employee's name and the name of the department in which the user works. This information was used purely for statistical reasons and specific names were never linked to responses in any form of report. Usernames were also recorded (as part of the actual phishing exercise) and were used to validate users' input. The most important function of the test was to see if users would reveal their passwords. As soon as users entered their passwords, the password was validated and then a single *Yes* (valid username and password) or *No* (invalid password for the given username) was recorded. Actual passwords were never recorded.

The results of the first phishing exercise indicated that 280 users responded to the e-mail message, with 231 (83%) who entered (gave away) their correct usernames and passwords. Further analysis showed that 159 (69%) of the 231 who gave away their personal details had already completed the company's in-house security training course that taught them how to recognise and react to possible phishing scams. This result seems to be consistent with the privacy paradox: the workers had reasonably high security awareness and training, but still revealed personal details on request. Another result showed that users with less years of work experience with the company were more inclined to give away personal details. This finding is consistent with the results of other similar studies (see Sheng et al., 2010). One explanation for this may be that employees with less years of working experience have also less exposure to the organisation's security practices and policies.

The second and follow-up phishing exercise was conducted after a period of time; the goal was to perform some form of comparative analysis in an attempt to determine whether user behaviour had changed positively since the first test. Except for the phishing message that was different from the one in the first test, all other conditions and data-recording activities were exactly the same as in the initial exercise.

The results of the second test were unexpected and rather disappointing. Although a lower percentage of users entered their valid usernames and passwords, the actual number increased from 231 users to 312 users (the total number of users who responded to the message increased from 280 in the first test to 490 in the second test). To add to this, the number of users who previously completed the security training and who gave away their correct usernames and passwords also increased from 159 to 288. A final disappointing (but significant) result was that there were 48 users who were repeat offenders; they revealed their passwords in both the first and second tests. There were no significant changes in new staff intakes or staff leaving during the interval between the tests that could

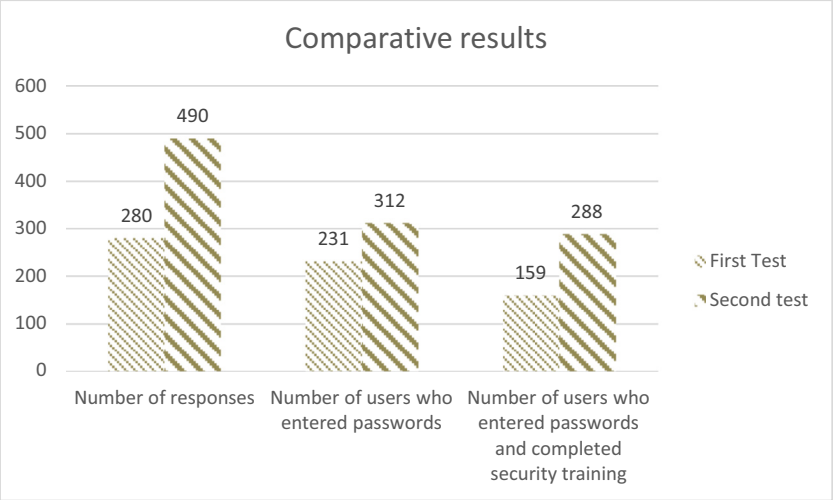


Fig. 1 – Comparative results of the two phishing exercises.

have influenced the results. The comparative results of the two phishing tests are graphically displayed in Fig. 1.

The correlation between years of work experience and the revealing of personal information was confirmed during the second test. Just over 50% of users who entered valid passwords had less than five years of experience within the company.

The results of the two practical phishing tests show that, despite the controls and mechanisms in place, a number of users still became victims. The results of the second test also indicate that perhaps users did not learn much from the first test. This raises the question of why so many users give away their passwords when asked for it – sometimes even more than once. It is probably safe to assume that one of the determinants of good security and a stable security environment is trust. To determine whether trust has an influence on users' security behaviour, and in an effort to try and explain the surprising results of the phishing tests, a trust survey was conducted in the company.

2.2. *The trust survey*

The role of trust in an information security setup is important and, as indicated in the introduction, a considerable body of knowledge exists on this topic. In an effort to understand and formulate a possible explanation for the observed paradoxical security behaviour, a trust survey was conducted in the company under study.

The concept of trust is defined in different, but mostly similar, ways. One such definition from an online dictionary defines trust as "a confidence that something is safe, reliable or effective" (Macmillan Online Dictionary, 2015). In the context of this study and consistent with the dictionary's definition, it is assumed that if one were confident that something was safe, reliable or effective, there would be a higher level of trust in that matter. Furthermore, in this study, the notion of trust is focused on human nature and not necessarily on any technical or computational notion of trust.

The methodology that was followed for the trust survey can be summarised as follows: A company-specific questionnaire, consisting of 20 questions, was developed, based on management input and literature resources. Forty users, representing the whole spectrum of staff and ranging from executive members to ordinary workers, were selected to participate in the survey as a sample. The sample size was based on a "saturation point", meaning that no additional information was obtained by interviewing additional respondents. Although the majority of the questions had to be evaluated on a 5-point Likert scale, it was decided to conduct the survey on an interview basis, using the questions as entry points. This had the added advantage of ensuring that all respondents understood the questions in the same way. The majority of the questions were aimed at assessing the users' trust levels; however, a few questions were designed to deal with users' perceptions of their own abilities when it comes to understanding and managing their information risks. An example of such a question is "Do you have enough knowledge or information to manage your information risks?" Two examples of questions aimed at assessing trust levels are "Do you feel confident enough in the organisation's systems to do your online banking?" and "Do you think the organisation protects and secures e-mail communications and related data adequately?"

The overall results of the trust survey have shown that, amongst employees, there is a significant high level of trust in the ability of the organisation to provide a safe, secure and trustworthy environment. The responses to the questions that aimed to determine trust levels were, without exception, all positive. In addition to this high level of trust, most respondents were also confident that they had sufficient knowledge and information to manage information security risks.

The apparent intertwining paradoxical results from the two phishing tests and the trust survey expand the initial question of "Why do so many users give away their passwords when asked for them?" to "To what extent do the high levels of trust in user's own and their organisation's ability to protect them against security threats contribute to the privacy paradox of giving away personal information when asked for it?" Answering this question is not straightforward and the answer is probably strongly linked to the human aspect of information security. There is a myriad of human factors that have been

identified as contributors to practical information security as well as to issues such as awareness, attitude, behaviour and culture (see for example Parsons et al., 2010). In addition to this, other aspects such as cognitive and culture biases, personal traits and perception of risk may also play an important role in influencing information security compliance (Tsohou et al., 2015). Of these aspects, perception of risk may be one of the pertinent issues that need further investigation. Perceptual differences or a gap between different security views and expectations of managers and users will no doubt have an influence on security practices. The next section will report on work that was performed to investigate whether there are any perceptual differences amongst employees in the same company in which the phishing tests and trust survey were conducted.

3. Perceptual differences

3.1. *Introduction to the perceptual differences study*

In the past, it has often been accepted that technical security measurements are sufficient to protect information assets but security solutions based on technical aspects are however insufficient to protect organisations (Montesdioca and Macada, 2015) and many security threats can be attributed to the behaviour of computer users (Parsons et al., 2014). Besides the large number of human aspects that may impact information security, researchers and decision-makers realise increasingly that the way in which users perceive various aspects related to security plays a crucial role – this potential problem is further aggravated when there is a difference in perceptions amongst different groups of people in an organisation. Furnell and Thomson (2009) argue that the degree to which users deem (perceive) information security as important will influence their compliance with security measures. The issue of perceptual differences is an important determinant of an effective and stable information security environment and a substantial number of studies in this area exist in the literature. Examples may be found in the works of Akcam et al. (2015), Albrechtsen and Hovden (2009), Huang et al. (2011), Martin et al. (2015), Posey et al. (2014), Tallon (2014) and Tsohou et al. (2015). Perceptual differences are also important in the context of social engineering and the associated behaviour of users. Flores et al. (2015), for example, found that psychological and personal factors will influence a user's behaviour in a phishing scam, whereas Nohlberg et al. (2008) emphasised that a victim's perspective tend to impact the readiness of an organisation to deal with social engineering attacks.

The two phishing tests and the trust survey that have been detailed in the previous section have each provided a certain degree of insight into the security problems and behaviour in the organisation under study. However, they have also confirmed that absolute explanations and solutions cannot be arrived at by looking at results in isolation. For example, the privacy paradox is still not addressed adequately. As an extension of these three exercises and in an effort to gain further understanding of security behaviour, a further experiment was conducted. This experiment aimed at evaluating the possible different perceptions of different groups of people to determine whether such perceptual differences can explain some of the intricacies of security behaviour.

3.2. *Methodological approach*

To evaluate perceptual differences, it was decided to make use of a measuring process that would be based on a questionnaire that had to be completed during a structured, one-on-one interview. Substantial thought, debate and reflection went into the development of the measuring instrument. Care was taken not to present merely a tick list to respondents and then draw conclusions on a simple count of positive or negative responses. A literature search for studies that deal specifically with perceptual differences in information security was conducted and some of these resources have been mentioned in Section 3.1. In addition to the literature resources, an intensive consultation process with the top management of the company under study was undertaken. The purpose of this consultation process was first to ensure that management requirements would be addressed and second to gauge management's view on possible eligible participants in the exercise. The influence that management had on the selection of participants was limited to guidance on a stratification process to ensure that participants are representative of the different departments. This was based on a random selection from an organisation chart. No one was instructed by management to take part in the study and eligible participants were free to refuse the request from the researchers to take part in the study. Interaction with management also facilitates the development of an instrument that is focused on the specific organisation and ensures that it can be linked to the preceding phishing and trust surveys. An additional advantage of involving top management was that management supported and approved of the research study – a crucial requirement for conducting a successful survey.

In line with management recommendations and consistent with similar studies that had been reported in the literature, it was decided to involve 60 people in the survey. This group was divided into three separate groups of 20 each, representing Management, IT Staff and Users; the purpose was to determine whether there were any perceptual differences between the three groups in terms of information security. The decision to involve 60 people was deemed adequate and in line with similar studies: Akcam et al. (2015) used 53 respondents in their study; Posey et al. (2014) used 33 respondents (22 users and 11 information security professionals); Huang et al. (2011) involved 64 participants in their study; and Albrechtsen and Hovden (2009) interviewed 11 information security managers and 18 users in their digital divide project. However, to perform a specific risk perception comparison, Albrechtsen and Hovden used 151 users and 87 information security managers for comparison purposes. The three groups that were used in this study are summarised in Appendix A by their designations, gender, age and years of service within the company.

The final questionnaire contains 11 questions. Some of the questions comprise the ranking of items (e.g. "Rank the top 5 vulnerabilities or threats in order of severity") or simply require a Yes/No response (e.g. "Is information security considered a problem to be resolved with technology?"), whereas other questions could be regarded as open questions where respondents

Interview protocol

The high-level interview framework that was used during interviews with participants is summarised as follows:

1. Explain to the participant that he/she was selected to take part in a research project on information security and that the selection was influenced by senior management. However, the only influence by senior management was guidance on a stratification process to obtain a representative sample of people.
2. Explain the goal of the research – to gauge perceptions on information security that may ultimately help explain the privacy paradox. Furthermore, explain that the purpose of the research project is also to evaluate perceptions of respondents to determine if a form of digital divide exists at the organisation. The project forms part of a broader project that investigates possible theories that can be used to explain why social engineering experiments have such levels of success.
3. Explain that the interview will last approximately 30 minutes and consists of a questionnaire containing 11 questions. There are no right or wrong answers and participants may ask for explanations/clarifications at any time.
4. Explain that participation is voluntary and that all responses will be held in strict confidentiality. No reference will be made to any person and results will only be reviewed by the researchers. The persons may also exclude themselves at any time without being penalised.
5. Obtain explicit and informed consent from the participant. Ensure that the consent form is signed.
6. Go through and complete the questionnaire, explaining or answering any questions that the participant may have.
7. Express your thankfulness to and appreciation for the respondent and emphasise that without his/her contribution, the research project cannot be successful. Ensure that the respondent understands that his/her responses will help guide the development of a better and more successful information security framework for the organisation.

Fig. 2 – Interview protocol.

are required to give their own view or opinion (e.g. "Who is responsible for information security in the company?").

As mentioned earlier, it was decided that the questionnaire would be completed on an interview basis in order to ensure an appropriate response. A one-on-one interview, taking approximately 30–40 minutes, was conducted with each of the 60 participants and the same interviewer was used in every interview. All interviewees were guaranteed confidentiality and they gave consent to the interview and to complete the questionnaire. Interviews were not audio recorded, as problems and questions were dealt with during the interview and results of any questions or problems were reflected in the responses of participants. The interview protocol that was followed is briefly summarised in Fig. 2. In a similar fashion as the trust survey that was also conducted on an interview basis, it was found that respondents tend to be more open and provide more honest answers during a personal interview.

The results of the survey are presented in the next section, followed by a discussion of the observed responses.

3.3. *Results of the perceptual differences evaluation*

The results for the three groups of respondents revealed both consistencies and inconsistencies. Basic statistical tests were performed to ensure that the results reported make sense, are valid and were evaluated using acceptable techniques. These tests include analysis of variance tests and tests for statistical significance. A discussion of every question in the questionnaire would be too long; only a few selected questions and their results will be dealt with in this section. These results will hopefully be adequate to illustrate the main findings and results. Where appropriate, the associated statistical techniques that have been used to interpret results will be briefly explained.

The first question deals with respondents' views on how well the organisation manages information technology risks. Participants had to record their opinion on a 5-point Likert scale with Excellent at the top end of the scale and Poor at the bottom end. A basic one-way analysis of variance (ANOVA) test was performed and showed that there were no statistical differences between the three groups. Management, IT Staff and Users were in agreement that the information technology risks at the organisation are well managed. This seems to be consistent with the general high level of trust that had been recorded in the earlier trust survey. It should be noted that social desirability (responding in a socially accepted way) is a recognised problem in research where questionnaires are used and it may have an impact on results (Frangopoulos et al., 2014). In an effort to mitigate the impact of social desirability in this study, participants were given the assurance that results will be confidential and no names will be revealed to management. Confidentiality and the importance of open and honest responses were also emphasised during the interviews with respondents.

Closely linked to the question on how well information technology risks are managed were two other questions that provided further insight into perceptions. These two questions (that were evaluated without any statistical tests) were "Who is responsible for information security in the organisation?" and "Is information security a problem that can be resolved with technology?" The objective of the first question was to determine whether there was consensus that *everybody* in the organisation is responsible for information security. The aim of the second question was to establish whether everybody agreed that technology on its own is not an adequate solution for the information security problem. The results in terms of responsibility indicate that 60% of both Users and IT Staff believed that information security should be the responsibility of everybody. Only 40% of management agreed

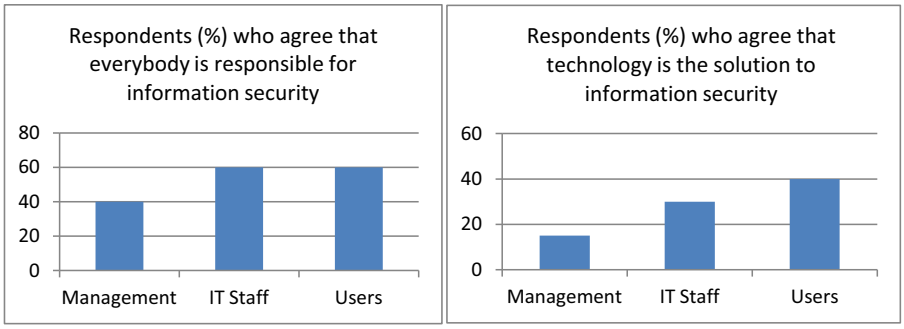


Fig. 3 – Results of two perceptual questions.

with this. Just over a quarter (28%) of all respondents believed that information security is the responsibility of the IT department; this is in line with the second question, where one third of all the respondents indicated that technology (by implication the IT department) is the solution for information security. The breakdown of the technology solution question shows that 40% of the users, 30% of IT Staff and 15% of management were of the opinion that technology on its own is the solution to the information security problem. The results of the two questions are graphically displayed in Fig. 3.

The following results show the perceptions of the three groups pertaining to control measures, importance of risks and threats, and the severity of threats. The results were analysed by using a basic protocol to test for significant differences in perceptions.

A popular way of testing for statistical significance is the use of p-values. However, p-values tend to vary with the size of the data set that is used and are normally more appropriate when random samples are taken (Ellis and Steyn, 2003). For this study, it was decided to make use of the Cohen's d-value (also known as an effect size) to test for significant differences (Cohen, 1988; Ellis and Steyn, 2003). An effect size is defined as a standardised difference between the means of two populations and gives the importance of the effect in practice. Mathematically, the effect size can be expressed as $(|\bar{x}_1 - \bar{x}_2|)/s_{max}$, where $|\bar{x}_1 - \bar{x}_2|$ is the absolute difference between the two mean values and s_{max} is the maximum of s_1 and s_2 (the sample standard deviations). According to Cohen (1988), the following may serve as a guideline for the interpretation of the d-value: If d = 0.2, the effect is small; if d = 0.5, there is a medium effect; and if d = 0.8, there is a large effect. The Cohen's value was used to test whether there are significant differences between the perceptions of the three combinations of IT Staff and Management, IT Staff and Users, and Management and Users.

Considering the type of control measures that had been implemented by the organisation to manage information security risks, there was a clear agreement that the six most important measures are Firewalls, Intrusion Detection, Antivirus Software, Password Complexity Rules, Policies and Procedures, and Monitoring. With the exception of two measures, Intrusion Detection and Policies and Procedures, they all received more or less the same number of votes from each of the three groups of participants. Intrusion detection received far more votes from Management as from the other two groups, whereas Policies and Procedures received significantly more votes from the IT Staff group. As for the perceptual differences in some of the remaining control measures, Table 1 provides a summary of the d-values that indicate the differences between the three groups.

From the d-values that are reported in Table 1, notable effect sizes (differences in perceptions) can be seen. For example, there is a medium effect (or medium perceptual difference) between IT Staff and Users with respect to Latest software and updates (d = 0.45). For this same control measure, there is a large perceptual difference (d = 0.73) between Management and Users. In the context of the two phishing tests with their associated somewhat poor results, it is significant that there are perceptual differences listed in Table 1 that may be directly related to a phishing scam, for example, Policies and Procedures, Well-trained staff, Security awareness training and Incident management.

Information technology risks, threats and vulnerabilities, and how they are managed are crucial in any information security framework. Views and opinions of all employees, including management, should therefore be aligned to manage and deal with security threats properly. To determine whether there exists any possible perceptual difference between the three groups, two specific questions that dealt exclusively with

Table 1 – Effect size (d-values) for control measures.

Control measure	Effect size (d-values)		
	IT staff with management	IT staff with users	Management with users
Latest software and updates	0.06	0.45	0.73
Well-trained staff	0.01	0.63	0.82
Policies and Procedures	0.50	0.11	0.40
Security awareness training	0.38	0.09	0.79
Incident management	0.50	0.57	0.09
Physical security	0.15	0.53	0.40

Table 2 – Effect size (d-values) for severity of risks.

Threats or vulnerabilities	Effect size (d-values)		
	IT staff with management	IT staff with users	Management with users
Human error	0.55	0.52	0.02
Virus/Malware	0.55	0.14	0.38
Complacency	0.39	0.44	0.77
Misuse of information	0.15	0.39	0.49
Hacking	0.62	0.27	0.28

cyber threats and risks were included in the questionnaire. The first question presents a list of 14 threats and vulnerabilities that respondents had to rank on a 5-point Likert scale with the following scale ratings: 1 – no risk; 2 – little risk; 3 – moderate risk; 4 – high risk; and 5 – very high risk. The second question requires of participants to rank their top five threats or vulnerabilities in order of severity, with a ranking of 1 being the most severe and 5 the least severe. The 14 threats or vulnerabilities that were used in these two questions were taken from Albrechtsen and Hovden (2009), as their list was deemed to be complete and also covers the risks areas applicable to the organisation under study. Appendix B contains a list of the threats and vulnerabilities that were used. An advantage of using threats and vulnerabilities from an existing study is that it facilitates some form of comparison of results between the two studies. The results of both questions were analysed once again by using Cohen's d-value to determine the extent of differences in perceptions between the three groups.

The results of the first question were encouraging and show that, with the exception of two of the threats or vulnerabilities, all three groups were in agreement with the risks that are posed to the organisation. The two exceptions were Complacency and Social Engineering, where a medium effect size (medium difference in perceptions) was recorded between IT Staff and Management with d-values of 0.44 and 0.42, respectively. These two threats were also amongst those reported by Albrechtsen and Hovden (2009) as areas with different perceptual views from Managers and Users. It should also be noted that the two threats and vulnerabilities are directly linked to security breaches such as phishing scams and the perceptual differences may have played some role in the poor phishing results that have been described earlier.

With regard to the second question (ranking of threats or vulnerabilities according to severity), a few differences in perceptions emerged. Table 2 lists the d-values of the threats, where clear differences between the three groups were observed.

It is interesting to note from Table 2 that there were perceptual differences between the IT Staff and both Management and Users. This may be attributed to the availability and access that IT Staff have to the latest industry details and statistics on issues such as human errors, viruses and hacking. Even in cases where these statistics show a positive trend, perceptual differences may still occur; for example, due to positive statistics (e.g. a reduced number in security incidents), IT Staff may view a specific threat or vulnerability as acceptable, whereas Management and Users may still see it as a high-risk threat. It can further be seen from Table 2 that there were also perceptual differences between Management and Users. These differences seem to occur with threats and vulnerabilities that are strongly linked to users and that may be viewed as strategic issues by management (e.g. Complacency of users and Misuse of information). Considering the two earlier phishing exercises, the results listed in Table 2 once again appear to have a possible link with the phishing results. Comparing the results in Table 2 with the results of the Albrechtsen and Hovden (2009) study, a few similarities are noted, especially with threats and vulnerabilities such as Complacency (Carelessness in the Albrechtsen and Hovden study), Social engineering and Hacking, where strong agreements were recorded. It should be noted, however, that although the similarities between the two studies may present (or possibly confirm) evidence of potential perceptual differences, the results do not, and should not, fully agree. Reasons for this are that Albrechtsen and Hovden used a bigger sample size; they used p-values to identify significant differences (as opposed to effect sizes that were used in this study); they compared two groups with each other (whereas three groups were used in this study); and their study was performed across different organisations (this study was specific to one organisation).

An important related topic that did not form part of this paper is the issue of group dynamics which suggests that work performance (and possibly perceptions) may be dependent on group behaviour in terms of work related preferences and tendencies (Barabanov and Kowalski, 2010).

Further conclusions from the results and how they may possibly be linked to the preceding phishing tests and the trust survey are presented in the next section.

3.4. *Discussion of results*

In the context of this study and the specific organisation in which the empirical experiments were conducted, a safe and secure information environment may be represented by the high-level model that is depicted in Fig. 4. Three major organisational groupings form the backbone of the model, namely a Management and Strategic component; a Technology component; and a Proficient Workforce (Users) component. The first component may be defined by aspects such as legal requirements, policies and procedures, and ethical issues, whereas the second component is a function of technological availability, client needs, business needs et cetera. The last component is a function of human factors and capabilities such as knowledge, attitude and behaviour. The safe and secure information environment in the context of this study refers to an environment where users have the freedom to pursue their daily activities while being protected from information security incidents as far as reasonably practical.

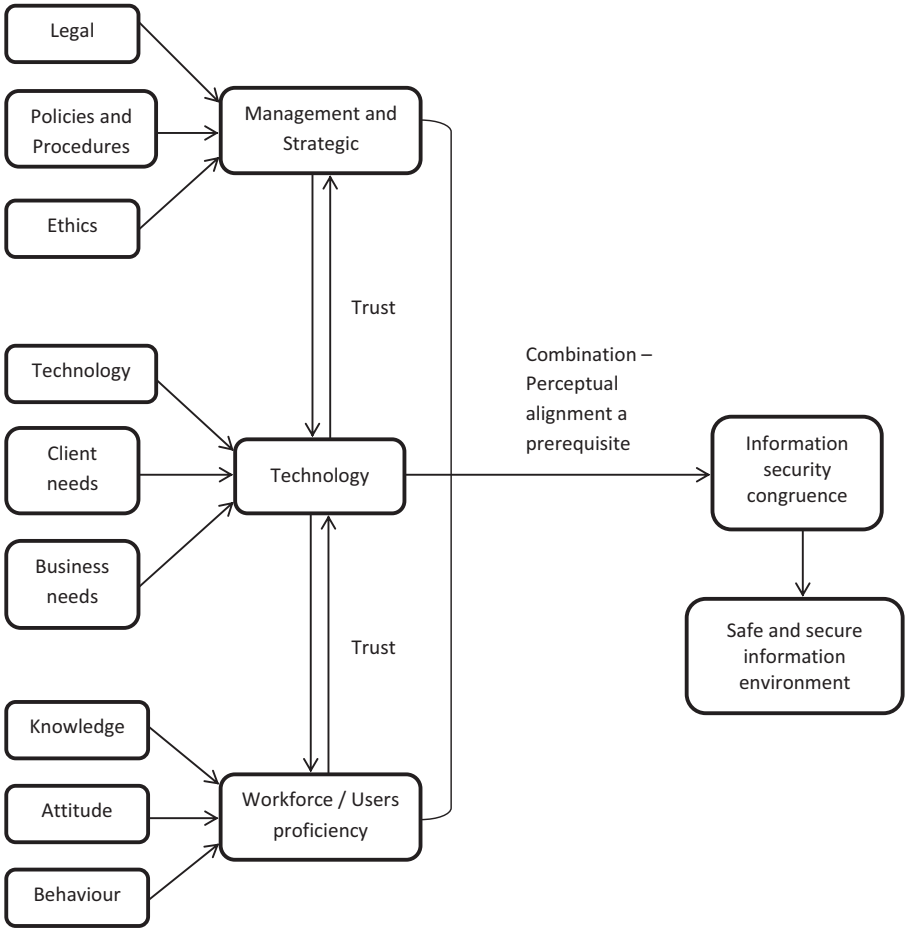


Fig. 4 – Safe and secure information environment model.

The three main organisational groupings are interdependent and interact with each other. This interaction is governed by a large number of factors of which trust is deemed as one of the more significant determinants. To reach a point where an acceptable state of information security will prevail, the three groupings have to be combined. A crucial requirement for a successful combination is that the perceptions and views of the three groups should be aligned – without such an alignment the combination will remain a theoretical goal. The result of the perceptual alignment and a combination of the major organisational groupings will be a form of information security congruence that will ultimately lead to the desired safe and secure information environment. The success of the safe and secure environment can then be tested (or monitored) by measuring certain outcomes. An example of such an outcome would be the level of security breaches (e.g. the phishing exercise that has been described earlier). Another example is the monitoring of the perceptual alignment in order to ensure the successful combination of the organisational groups.

The results of the three preceding empirical phishing and trust surveys that have been described in Section 2 show that a high number of employees are willing to reveal personal details when asked for it. This revealing of private information happens even when they have a high level of trust in their own and the company's ability to protect them. In terms of the safe and secure model in Fig. 4, the empirical experiments involved all three major organisational groups. If the frequency of occurrence of security breaches is accepted as one of the outcomes of a safe and secure information environment, it seems fair to conclude that there may still be certain shortcomings in the organisation's information security setup. The trust levels of staff do not provide sufficient explanations for the phishing results and, according to the model, further investigation concerning the combination of the three groupings into a congruent information security framework needs to be done. The results of the perceptual differences may offer some further explanations.

As reported in the results section (Section 3.3), there are certain differences in view as far as some of the basic principles are concerned; there is not a 100% consensus that everybody is responsible for information security or that technology on its own is not a sufficient solution for the information security problem (see also Fig. 3). Users or employees who do not agree with this may develop the attitude that somebody else will prevent problems and that if problems do occur, somebody else will report them – an almost "don't care" attitude that makes one an easy victim of a phishing scam.

The differences in perceptions pertaining to control measures, risks and severity of risks are in many cases consistent (there is agreement between the groups), with only a few inconsistencies on a medium impact level that have been reported. However, it is significant that the inconsistencies could all be related to social engineering and its associated scams.

It can be accepted that, due to the nature of a specific job designation or the information that is available to specific positions, there may be certain differences in views. Despite this, users are normally the first line of defence in protecting the company against certain threats (e.g. social engineering) and should be kept up to date with organisational viewpoints on information security and related incidents. As already explained, the problem is further complicated when users have a high belief (trust) in their own and the company's abilities – the combined effect of this high level of trust and perceptual differences may lead to the privacy paradox.

Based on the results that have been presented in Section 3.3 and the safe and secure model in Fig. 4, it appears that the differences in perceptions of the three major groupings (supported by the findings of the phishing results in Section 2) do play a role in the privacy paradox. These differences impede the successful combination of the organisation's major groupings, which makes the achievement of acceptable information security congruence difficult, if not impossible.

The problem may be addressed by performing a number of different management tasks of which a few will be highlighted here. First, the well-known problem of managing expectations should receive continuous attention. Expectations, perceptions, priorities, et cetera should be identified and gaps should be eliminated. Such elimination will lead to a better and, eventually, strong alignment of views between the different groups of organisation structures. One way to identify and manage expectations and perceptions is to implement a measuring instrument such as the one described in this paper or suggested by other researchers such as Albrechtsen and Hovden (2009). Another important and well-known factor that is closely related to the management of expectations is communication. Perceptions are not formed on experiences only but also on what is communicated. Feedback and relevant security information will influence perceptions and if current security practices, threats, risks, statistics, et cetera are not communicated or announced in a responsible and appropriate manner (e.g. an information security policy), employees may believe that all information security issues are taken care of and that all is well.

Second, focused and well-designed security awareness programmes remain a necessity. The company in which this study was performed has an extensive and well-designed information security training programme in place, yet many employees still fall victim to the phishing scam. It should be accepted that there is normally a dissipation of information security knowledge over a period of time and that an ongoing information security awareness or training programme is necessary to counter any possibly outdated knowledge. Ongoing information security awareness and training programmes should, of course, be balanced with situations where users are so inundated with security information that it may become difficult to perform their daily tasks. Users being security fatigued and other associated problems are not part of the scope of this paper and will be touched upon in a follow-up paper.

Third, the frequency of testing certain outcomes should be increased. As stated earlier, measuring these outcomes is a good indication of how well different groups have combined to reach information security congruence and, ultimately, a safe and secure information environment. This paper has described two examples of such outcomes (phishing and perceptual differences) and how they can be monitored. Employing these monitoring instruments to specific outcomes is also important in the context of validating or falsification of the proposed safe and secure environment model. Favourable results, for example, from a phishing test or a perceptual differences survey may indicate that the model and its proposed elements comply with a required positive situation (a valid model) while negative results will signify the presence of dysfunctional elements (an unsuccessful model). There are many other examples of outcomes that can be monitored and a successful monitoring framework can easily be put together by an internal audit or risk assurance department.

The focus of this paper was on specific issues in a framework for a safe and secure information environment. There are other factors that will, no doubt, also play a role in the successful combination of organisational structures. However, focusing on perceptual differences as a starting point proved to be a worthwhile exercise, as other factors may assume and rely on the fact that all stakeholders share the same views pertaining to information security.

4. Conclusion

Information security in general, particularly the human aspects thereof, is a well-researched subject. Despite this, there remain certain problems where people with an apparently high level of information security awareness still take unnecessary and ill-considered risks. One example is the so-called privacy paradox, where users are willing to give away confidential information despite their high levels of security awareness – some researchers also refer to this as the knowing-doing gap (Cox, 2012). In an effort to address some of the uncertainties that are associated with the human aspects of information security, a long-term research project was initiated to investigate some of the security issues. Over a period of time, two practical phishing experiments (a trust survey and a perceptual survey) were conducted at a large utility company. This paper reports the results of these empirical exercises. As explained in the introduction, the two phishing experiments and the trust survey had already been reported on in detail and were presented in this paper in a summarised form to contextualise the research project. The main focus of this paper is to report on the perceptual gaps between groups of people in the organisation, and how it may help to explain and understand the privacy paradox as observed from the phishing exercises.

A safe and secure information security model was proposed. The model consists of three organisational groupings (Management, Technology and Users) that have to be combined to reach a state of information security congruence. Perceptual alignment between the three groups proved to be a crucial prerequisite for a successful combination; without this alignment, the ultimate goal of a safe and secure information environment will be difficult to reach and will probably remain a theoretical aim. The results of this study have indicated that there exists a certain degree of perceptual difference between the three organisational groups in the company where the study was conducted. These perceptual differences (in the context of the proposed safe and secure model) help in explaining and understanding the disappointing results of the

phishing tests in an environment with sufficient security awareness and training programmes, as well as a high level of trust in own and organisational capabilities.

Owing to the presence of a strong and significant human element, information security is a complex phenomenon and investigating only one factor, namely perceptual differences, will not offer complete solutions to information security behaviour problems that are characterised by the privacy paradox or the knowing-doing gap. Difference in opinion is, however, a logical starting point for information security problems, as management decisions and actions often assume that everybody shares the same viewpoint. The aim of the greater research project is to continue investigating factors that may influence the formation of a safe and secure information environment. The project will be concluded with a follow-up paper that will theorise on other human aspects such as risk homeostasis and users who suffer from security fatigue.

Appendices

Appendix A. Participants characteristics

Management				IT Staff				Users			
Designation	Gender	Years	Age	Designation	Gender	Years	Age	Designation	Gender	Years	Age
1. Compliance Manager	m	8	43	1. Service Manager	m	10	40	1. Admin Officer	f	5	36
2. Finance Manager	m	35	56	2. IT Project Manager	f	12	35	2. Risk Consultant	m	1	32
3. CEO	f	10	56	3. IT Co-ordinator	m	13	61	3. Risk Systems Analyst	m	8	35
4. Security Manager	m	10	54	4. Manager Information Services	m	12	49	4. Compliance Co-ordinator	f	7	56
5. Manager Technology & Energy Management	m	32	53	5. Process Manager	m	1	37	5. Change Manager	f	3	40
6. Operational Risk Manager	f	4	40	6. IT Sourcing Manager	m	21	67	6. Auditor	m	27	53
7. Manager Operations	m	24	42	7. Information Services Assurance	m	29	49	7. Insurance Manager	m	35	53
8. Business Manager	m	14	44	8. Business Analyst	m	6	43	8. Reporting Analyst	m	3	34
9. Manager Water Policy	f	18	52	9. Business Analyst	m	37	56	9. Operations Co-ordinator	m	41	57
10. Manager Procurement	m	40	63	10. Systems Team Leader	m	12	38	10. Pricing Analyst	f	4	30
11. Manager Infrastructure	m	16	45	11. Account Executive	m	7	46	11. Executive Support	f	4	34
12. Risk Manager	f	8	49	12. Senior Spatial Analyst	m	7	31	12. Freedom of Information Co-ordinator	f	2	29
13. Manager Review & Audit	m	18	55	13. Sourcing Consultant	m	17	61	13. Business Administrator	f	30	46
14. COO	m	44	64	14. Business Analyst	m	9	32	14. Personal Assistant	f	4	37
15 Manager Environment	f	19	45	15. Security Co-ordinator	m	9	31	15. Planning Analyst	m	5	42
16. GM Business Services	m	11	53	16. Team Leader	m	15	41	16. Superannuation Officer	m	2	46
17. CFO	m	8	54	17. Security Team	m	2	24	17. Land Services	f	8	46
18. Manager Legal Services	m	17	52	18. Systems Engineer	m	3	28	18. Support Officer	f	2	52
19. Head of HR	f	2	59	19. Customer Support	m	9	44	19. Financial Graduate	f	3	28
20. Manager Pricing	f	1	57	20. Security Consultant	m	3	44	20. Compliance Analyst	f	8	39
Averages		16.95	51.8			11.70	42.85			10.10	41.25
All 60 participants Average Age: 45.30 Average Years: 12.92 Number of males: 40 Number of females: 20											

Appendix B. List of vulnerabilities or threats that were used in the perceptions survey

The list was taken from Albrechtsen and Hovden (2009), with minor changes to the wording of some items on the list. The intent and meaning of the different threats were explained and contextualised during the interviews.

Vulnerabilities and threats

1. Human error
2. Virus and malware infection
3. Complacency
4. Misuse of information
5. Loss of information
6. Inappropriate use of e-mail
7. Software vulnerability
8. Improper use of Internet
9. Excessive private use
10. Social engineering
11. Spam
12. Hacking
13. Theft
14. Illegal use

REFERENCES

Akcam BK, Hekim H, Guler A. Exploring business student perception of information and technology. Procedia Soc Behav Sci 2015;195:182–91.

Albrechtsen E, Hovden J. The information security digital divide between information security managers and users. Comput Secur 2009;28:476–90.
Alhogail A. Design and validation of information security culture framework. Comput Human Behav 2015;49:567–75.
Alhogail A, Mirza A. Information security culture: a definition and literature review. In: World congress on computer applications and information systems (WCCAIS); 2014;doi:10.1109/WCCAIS.2014.6916579.
Alnatheer MA. Information security culture critical success factors. In: 12th international conference on information technology: new generations; 2015;doi:10.1109/ITNG.2015.124.
Barabanov R, Kowalski S. Group dynamics in a security risk management team context: a teaching case study. In: Security and privacy-silver linings in the cloud. Heidelberg: Springer; 2010. p. 31–42.
Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 2010;34(3):523–48.
Chandrashekhar AM, Gupta RK, Shivaraj HP. Role of information security awareness in success of an organisation. Int J Res 2015;2(6):15–22.
Cohen J. Statistical power analysis for behavioural sciences. 2nd ed. Hillsdale (NJ): Erlbaum; 1988.
Cox J. Information systems user security: a structured model of the knowing-doing gap. Comput Human Behav 2012;28:1849–58.
Da Veiga A. An information security training and awareness approach (ISTAAP) to instill an information security-positive culture. In: Proceedings of the ninth international symposium on human aspects of information security and assurance (HAISA 2015); 2015.
Da Veiga A, Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput Secur 2015;49:162–76.
Ellis SM, Steyn HS. Practical significance (effect sizes) versus or in combination with statistical significance (p-values). Manag Dynam 2003;12(4):51–2.
Enrici I, Ancilli M, Lioy A. A psychological approach to information technology security. In: 3rd international conference on human system interaction, HSI2010; 2010;doi:10.1109/HIS.2010.5514528.
Flores WR, Holm H, Nohlberg M, Ekstedt M. Investigating personal determinants of phishing and the effect of national culture. Inf Comput Secur 2015;23(2):178–99.
Frangopoulos ED, Eloff MM, Venter LM. Human aspects of information insurance: a questionnaire-based quantitative approach to assessment. In: Proceedings of the 8th international symposium on human aspects of information security & assurance (HAISA 2014); 2014.
Furnell S, Thomson KL. From culture to disobedience: recognising the varying user acceptance of IT security. Comput Fraud Secur 2009;2:5–10.
Huang DL, Rau PLP, Salvendy G, Gao F, Zhou J. Factors affecting perception of information security and their impacts on IT adoption and security practices. Int J Hum Comput Stud 2011;69:870–83.
Hull G. Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. Ethics Inf Technol 2015;17(2):89–101.
Ifinedo P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence and cognition. Inf Manag 2014;51:69–79.
Jagatic TN, Johnson NA, Jakobsson M, Menezer F. Social phishing. Commun ACM 2007;50(10):94–100.
Jansson K, Von Solms R. Phishing for phishing awareness. Behav Inf Technol 2013;32(6):584–93.
Jensen CD. Trust is the foundations for computer security. In: 14th international information security for South Africa conference (ISSA 2015); 2015.
Kearney WD, Kruger HA. Janczewski LJ, Wolf H, Shenoi S, editors. Phishing and organizational learning in SEC2013, IFIP AICT 405. 2013. p. 379–90.
Kearney WD, Kruger HA. Considering the influence of human trust in practical social engineering. Johannesburg: Information Security for South Africa (ISSA); 2014. p. 1–6 doi:10.1109/ISSA.2014.6950509.
Kelecha BB, Belanger F. Religiosity and information security policy compliance, <http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations>; 2013 [accessed 03.12.15].
Keser H, Gulduren C. Development of information security awareness scale. KU Kastamonu Egitim Dergisi 2015;23(3):1167–84.
Kim C, Tao W, Shin N, Kim KS. An empirical study of customers' perceptions of security and trust in e-payment systems. Electron Commer Res Appl 2010;9:84–95.
Kokolakis S. Privacy attitudes and privacy behavior: a review of current research on the privacy paradox phenomenon. Comput Secur 2015;doi:10.1016/j.cose.2015.07.002 (in press).
Kumaraguru P, Cranshaw J, Acquisti A, Cranor L, Hong J, Blair BA, et al. School of phis: a real-world evaluation of anti-phishing training. In: Proceedings of the 5th symposium on usable privacy and security (SOUPS); 2009. p. 3.1–3.12.
Lafrance Y. Psychology: a precious security tool. SANS Institute InfoSec Reading Room; 2004.
Macmillan Online Dictionary. <http://www.macmillandictionary.com/dictionary/british/trust_23>; 2015 [accessed 20.10.15].
Martin N, Rice J, Martin R. Expectations of privacy and trust: examining the views of IT professionals. Behav Inf Technol 2015;doi:10.1080/0144929X.2015.1066444 [accessed 10.06.15].
Miltgen CL, Smith HJ. Exploring information privacy regulation, risks, trust, and behavior. Inf Manag 2015;52:741–59.
Montesdioca GPZ, Macada ACG. Measuring users satisfaction with information security practices. Comput Secur 2015;48:267–80.
Nohlberg M, Kowalski S, Huber M. Measuring readiness for automated social engineering. In: Proceedings of the 7th annual security conference, Las Vegas, USA; 2008.
Oxford Dictionary. <http://oxforddictionaries.com/definition/english/phishing>; 2013 [accessed 20.10.15].
Parsons K, McCormac A, Butavicius M, Ferguson L. Human factors and information security: individual, culture and security environment. Edinburgh, Australia: Australia Government, Department of Defence. Command Control, Communications and Intelligence Division, Defense Science and Technology Organisation; 2010.
Parsons K, McCormac A, Butavicius M, Pattison M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur 2014;42:165–76.
Pattinson M, Jerram C, Parsons K, McCormac A, Butavicius M. Why do some people manage phishing e-mails better than others? Inf Manag Comput Secur 2012;20(1):18–28.
Posey C, Roberts TL, Lowry PB, Hightower RT. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Inf Manag 2014;51:551–67.
Rantos K, Fysarakis K, Manifavas C. How effective is your security awareness program? An evaluation methodology. Inf Secur J 2012;21:328–45.
Safa NS, Sookhak M, Von Solms R, Furnell S, Ghani NA, Herawan T. Information security conscious care behavior formation in organisations. Comput Secur 2015;53:65–78.

Shaik R, Sasikumar M. Trust model for measuring security strength of cloud computing service. Procedia Comput Sci 2015;45:380–90.
Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the 28th international conference on human factors in computing systems; 2010. p. 373–82.
Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: the road ahead. Comput Netw 2015;76:146–64.
Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance. A systematic review of quantitative studies. Inf Manag Comput Secur 2014;22(1):42–75.
Spandonidis B. Linking information security awareness to information security management strategy. A study in an IT company [Master's thesis]. Sweden: Linnaeus University; 2015.
Tallon PP. Do you see what I see? The search for consensus among executives' perceptions of IT business value. Eur J Inf Syst 2014;23(3):306–25.
Tsohou A, Karyda M, Kokolakis S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. Comput Secur 2015;52:128–41.
Whitman NE, Mattord HJ. Principles of information security. Canada: Thomson, Course Technology; 2003.

WD Kearney has over 25 years of experience in the assurance field obtained in a number of positions in utilities, mining and banking environments. He has an MSc degree, numerous diplomas and earned a number of certifications, including Certified Information Security Manager (CISM) and Certified Information Security Auditor (CISA). He also served as an Extraordinary Senior Lecturer in the School of Computer, Statistical and Mathematical Sciences at North-West University in South Africa. He is actively involved in ongoing research in the corporate governance field and is a current PhD candidate.

HA Kruger is Professor in the School of Computer, Statistical and Mathematical Sciences at the North-West University (Potchefstroom Campus) in South Africa. He previously worked for a large international mining company and has a number of years experience in Information Risk Management. He has a PhD in Computer Science, a MCom (Information Systems), an MSc (Mathematical Statistics) and an MPhil (Philosophy). His current interests include information security, decision modelling and the use of linear programming models.

Chapter 7

Theorising on Risk Homeostasis in the Context of Information Security Behaviour

7.1 Introduction

Chapter 7 is presented in the form of a journal article that was accepted for publication in *Information and Computer Security* (Accepted – see Appendix J for proof of acceptance).

The previous chapters have all led to this final paper on risk homeostasis as a factor in information security. The paper suggests that risk homeostasis is an understudied topic in the context of information security and that it should be considered as an alternative framework in information security and risk management to understand, predict and manage information security behaviour.

Figure 7.1 (on the next page) shows how the chapter is linked to the research objectives and research questions. This is then followed by the article as it was published. Guidelines of the journal are presented in Appendix J.

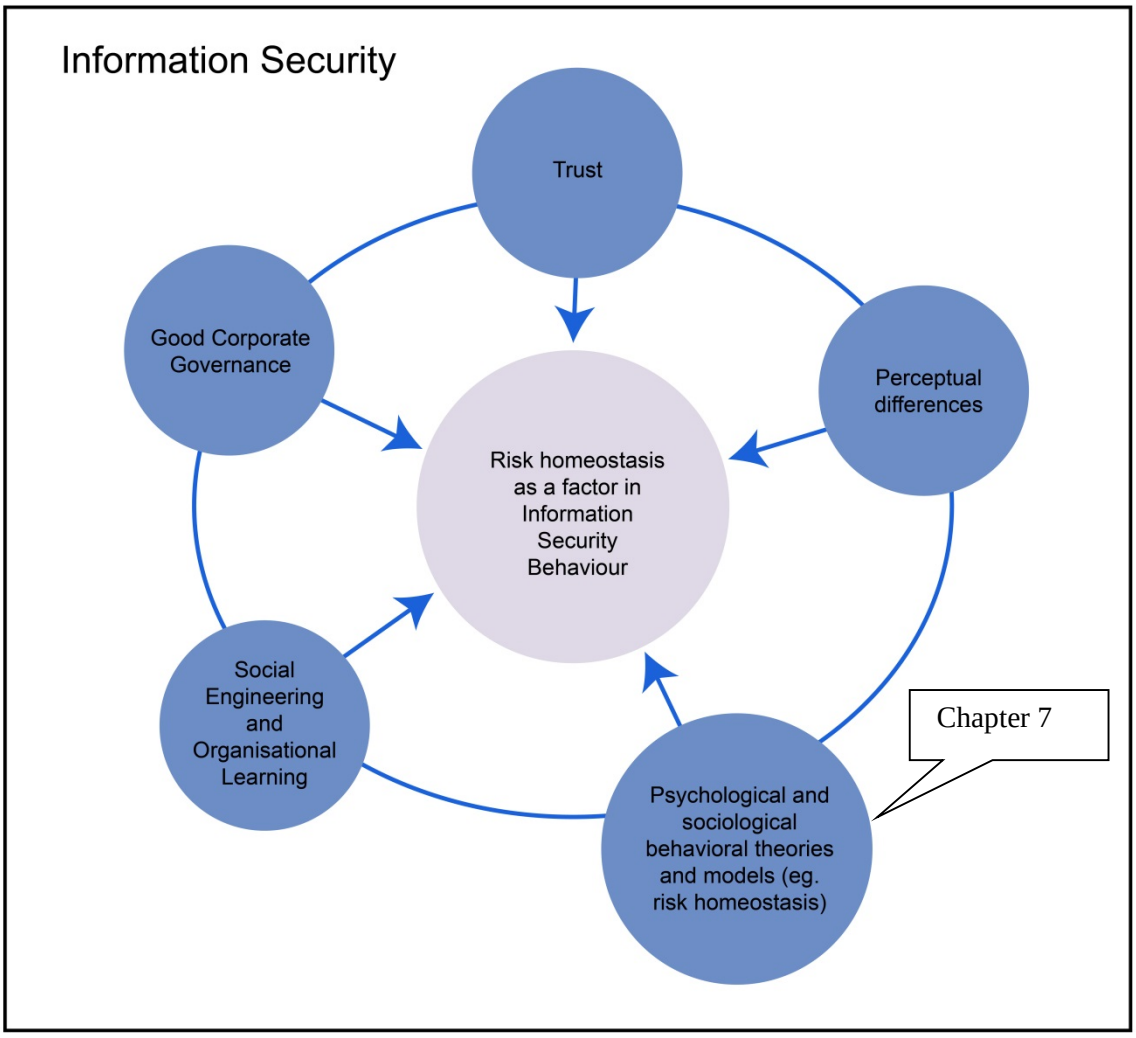


Figure 7.1 – Chapter 7 as part of the research study

Theorising on risk homeostasis in the context of information security behaviour

Kearney WD[1], Kruger HA[2]
[1,2]School of Computer, Statistical and Mathematical Sciences
North-West University
Potchefstroom, South Africa
[1]Kearneys@iinet.net.au [2]Hennie.Kruger@nwu.ac.za

[2]Corresponding author

Abstract

Purpose

The purpose of this paper is to discuss and theorise on the appropriateness and potential impact of risk homeostasis in the context of information security

Design/Methodology/Approach

The discussion is mainly based on a literature survey, backed up by illustrative empirical examples.

Findings

Risk homeostasis in the context of information security is an under-explored topic. The principles, assumptions and methodology of a risk homeostasis model offer new insights and knowledge to explain and predict contradictory human behaviour in information security.

Practical implications

The paper shows that explanations for contradictory human behaviour (e.g. the privacy paradox) would gain from considering risk homeostasis as an information security risk management model. The ideas discussed open up the prospect to theorise on risk homeostasis as a model in information security and should form a basis for further research and practical implementations. On a more practical level, it offers decision-makers useful information and new insights that could be advantageous in a strategic security planning process.

Originality/value

This is the first systematic comprehensive review of risk homeostasis in the context of information security behaviour and readers of the paper will find new theories, guidelines and insights on risk homeostasis.

Keywords – Risk homeostasis, information security, security fatigue, information risk, behavioural frameworks, information security behaviour

1. Introduction

Modern-day information security cannot be defined or understood as a pure technical problem. Information technology is a commodity that is used by humans and is therefore a function of the combined effect of human and technological aspects. These human factors ultimately determine the success or failure of information security programmes. The statement on the role of humans in information security is nothing new and a large number of research projects dealing with the problem

exist (Frangopoulos et al., 2014; Furnell and Clarke, 2012; Parsons et al., 2010). Despite the comprehensive research efforts in this area, there is still no absolute or definitive solution for what seems to be a very basic problem. The privacy paradox (Kokolakis, 2015) or the knowing-doing gap (Cox, 2012a) are good examples of a problem that remains almost a mystery or at least an enigmatic problem. This problem refers specifically to users with a perceived high level of security awareness who also possess sufficient information security knowledge, but who are then easily persuaded to reveal confidential information such as passwords. It is exactly because of the human element in information security that these types of problems occur and persist. Many researchers have acknowledged this and there are a significant number of studies calling for a more holistic approach to information security (Soomro et al., 2016) or attempting to provide new directions and guidelines for behavioural information security research (Crossler et al., 2013).

Several studies related to the behavioural information security problem apply different theories to try and understand human behaviour in the context of information security. Lebek et al. (2013) reported that a literature review had indicated that at least 54 different theories have been identified that were applied in the area of information security awareness and behaviour. Of these, the primary behavioural theories (based on the number of publications) are the theory of reasoned action (TRA); the theory of planned behaviour (TPB); the general deterrence theory (GDT); and the protection motivation theory (PMT).

The TRA framework deals with a user's behavioural intention and its two associated components, namely attitude and subjective norm (Gundu and Flowerday, 2013). This framework is often combined with or integrated into other theories and then used to explain aspects of information security awareness (Gundu and Flowerday, 2013; Khan et al., 2011) or information security policy compliance (Siponen et al., 2007). The TPB is an extension of TRA and suggests that individual behaviour is influenced by attitude, subjective norms and perceived behavioural control – the latter being the perceived ease or difficulty in performing a particular behaviour (Ifinedo, 2012). This theory has also been widely applied in information security and includes studies that are linked mainly to information security policy compliance (Bulgurcu et al., 2010; Ifinedo, 2012; Kim et al., 2014; Sommestad and Hallberg, 2013). The rationale for GDT is that people will respond to security countermeasures and the associated severity of punishment for a security violation. Straub (1990) applied this theory and surveyed 1 211 organisations, concluding that security countermeasures that include deterrent procedures result in lower computer abuse. Other examples where GDT or variations thereof were applied can be found in D'Arcy et al. (2008), Siponen et al. (2007) and Vaidyanathan and Berhanu (2012). PMT is another psychological theory that was originally developed within a framework of fear-arousing communication (Boer and Seydel, 1996). The theory is often used to predict behaviour and is based on two cognitive processes, namely threat appraisal and coping appraisal (Jansen, 2015). Threat appraisal is composed of a perceived vulnerability and a perceived severity component, whereas coping appraisal consists of elements such as self-efficacy, response efficacy and response cost (Ifinedo, 2012). PMT has been applied in a number of information security behaviour studies and was found to be useful to predict security behaviour (Crossler, 2010; Herath and Rao, 2009a; Ifinedo, 2012; Jansen, 2015; Meso et al., 2013; Vance et al., 2012).

Behavioural theories on their own do not always provide sufficient answers to information security behaviour problems. As mentioned, the theories are often combined in an effort to obtain new insights into security problems. Also associated with these psychological theories are a large number of other human-related aspects that may be utilised to influence change in behaviour. An example of one factor that is strongly linked to the theories highlighted above is fear. Fear is regularly used as a persuasion technique to change behaviour (Bada and Sasse, 2014) and is also a driver of the PMT framework

(Crossler et al, 2013). Closely related to fear is the role of penalties as an enabler for change in security behaviour (Herath and Rao, 2009b). Other interesting factors that may influence a user's perception of risk and information security are the availability heuristic, optimism bias, omission bias et cetera (Parsons et al, 2010). The role of these and other cognitive biases has also been studied by other researchers (Tsohou et al., 2015).

Despite all the comprehensive and well-researched theories, models and factors that influence information security behaviour, it may take only one simple phishing test to prove that there are still significant and perhaps serious challenges in the security behaviour arena – an example of such a phishing test can be found in Kearney and Kruger (2013). With this brief mention of the more prominent theories and influential factors in mind, the ensuing paper theorises on risk homeostasis as a relevant factor (or possible theory) in information security and subsequently discusses one or two other relevant options that may be associated with information security and the theories surrounding it. The study is guided by a primary research question that asks whether the understudied risk homeostasis theory (in the context of information security) may offer any new insights into the paradoxical information security behaviour of users.

The remainder of the paper is organised as follows: The next section provides a short background or motivation for considering a theoretical contemplation of risk homeostasis as a factor in information security. This will be followed by an overview of risk homeostasis and how it relates to information security. The penultimate section will then focus on some further ideas in the context of information security. Concluding remarks are presented in the final section.

2. Motivational background

The significant role that the human element plays in information security means that information security behaviour cannot be understood completely by relying only on human data that are normally obtained from surveys and other measuring instruments. Doing this turns a complex human-scientific problem into a data-driven science that may present a whole new host of problems.

Consider a situation in which respondents are asked to write down the most important risk to privacy. Based on the results (and usually a few statistical tests) it would be possible to state that the number one risk to privacy is risk *x*. It seems fair to say that some valuable learning has taken place and that decision-makers are now better informed to make more appropriate human security decisions. However, we are no closer to a greater understanding of anything and the results are far from a generalisation of users and their perception of risk. A response to the same question may be entirely different the next day, week or year. Circumstances, perceptions, technology et cetera change over time and differ from one organisation to the next. This makes the initial results valid for only a short and undetermined period of time. In addition to this, Roghanizad and Neufeld (2015) state that decisions entailing risk are reliant on a user's non-rational, gut-level intuition – a clear indication that responses cannot and should not be generalised. A survey, measuring or even observations are acceptable, but the methodology of these techniques is aimed at generating more data which in themselves offer no or very little explanation or understanding of information security behaviour – they provide lists, catalogues and classifications (Fricke, 2015).

Statistical tests that are frequently used with surveys and questionnaires present their own unique problems and Fricke (2015) lists, with supporting literature sources, a number of common errors in statistical analysis. These techniques and their associated errors are regularly employed in information security studies and include null hypothesis significance testing, stepwise regression, multiple

comparisons, subsetting, overfitting, univariate screening and dichotomising continuous variables. Also in the context of information security, Frangopoulos et al. (2014) warn against the problem of respondents being biased when completing questionnaires. They refer to social desirability (responding in a way that is socially acceptable) as one of the problems that is also confirmed by other information security researchers (Crossler et al., 2013). A survey on previous work on quantitative representation and analysis of information security shows that the validity of most of these methods is unclear and, based on this, it is then concluded that quantified security is a "weak hypothesis" (Verendel, 2009). Methodological challenges in quantitative empirical research are also recorded from time to time in other IT-related studies (Vehovar et al., 2006).

The above arguments are by no means an objection to surveys, questionnaires or generating data pertaining to information security behaviour. These techniques do have advantages such as the continuous assessment of security-related outcomes; their usefulness in testing theories; and the fact that it is an easy way to get access to larger sample sizes. However, to be able to make new discoveries in information security behaviour that is beyond a dataset and the inductivism that goes with it, more theories, thoughts and problems are needed. This is exactly why, to a certain extent, researchers investigate psychological theories such as those mentioned in the introduction.

There are also other theories that need to be considered in the context of information security behaviour. Examples include the well-known risk homeostasis theory that was introduced by Wilde (1994); theories on users who suffer from security fatigue (Furnell and Thomson, 2009); the theory of narcissism in organisations (Cox, 2012b); and the so called "slower is faster" theory (Gershenson and Helbing, 2015). Some of these theories have already been touched on in an information security context but need to be explored in more depth, as it appears that they are able to offer some conceptual explanations without relying too much on data that have been obtained from questionnaires. Risk homeostasis is one of the theories that has been associated with information security a number of times (Pattinson and Anderson, 2004; Stewart, 2004). In the next section, risk homeostasis will be investigated theoretically as a model that may assist in understanding some of the recurring information security behaviour problems. It will be argued, amongst other things, that there may be certain commonalities between risk homeostasis and other theories such as the PMT framework that has been mentioned earlier. If there are indeed links between the two frameworks, the large number of studies on PMT certainly warrants a closer look to risk homeostasis and it may be worthwhile to at least start theorising on the risk homeostasis theory and what it may offer to information security.

3. The theory of risk homeostasis

It is clear from the literature that the different behavioural theories that have been mentioned in the introduction are popular and well-researched topics in information security. The risk homeostasis theory, however, seems to be a topic that is not one of the current focus points in information security. Very few resources on studies exist in which risk homeostasis is treated as a factor or an influential theory in information security. Pattinson and Anderson (2004) have performed an introductory study of risk homeostasis as a factor in information security, but other researchers only briefly mention the theory as a possible explanatory tool (Albrechtsen and Hovden, 2009; Parsons et al., 2010).

3.1 Risk homeostasis explained

Risk homeostasis is a risk compensation or behavioural adaptation theory that was introduced by Wilde (1994, 2001). According to the theory, people will accept a certain level of risk until the situation changes, for example by introducing new or additional safety measures. People will then change their behaviour to compensate for a change in risk levels. Parsons et al. (2010) state succinctly that "if conditions are perceived to be less risky, then people may take more risk, and if the conditions are perceived to be more risky, then the amount of risk taken may be reduced". Wilde (2001) explains the theory by using a thermostatic control model that continuously changes to maintain a desired temperature. The theory was primarily developed and demonstrated in the area of road safety with the 1967 Sweden change from left-hand to right-hand traffic (Wilde, 1998) and the accident rate per head of a population (Wilde, 2001) as representative examples. Application of the theory is not just limited to road safety and similar examples, though; it can be found in the medical field where vaccination, for example, may encourage promiscuity (Brewer et al., 2007; Pinkerton, 2001). The homeostatic model that has been suggested by Wilde is depicted in Figure 1 with some minor word changes to reflect an information security environment.

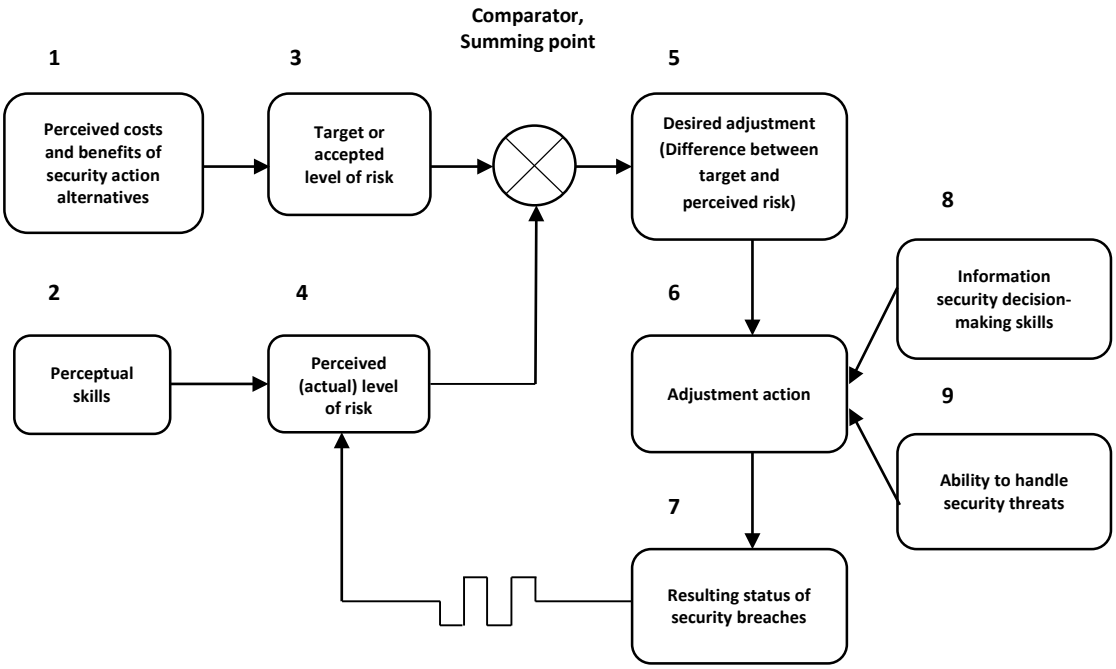


Figure 1: Risk homeostasis model, adapted from Wilde (2001)

The principles of the model in Figure 1 can be summarised in the context of information security as follows:

A user may determine a preferred or target level of risk (box 3), based on factors such as experience, information security training and awareness programmes, cultural factors and social factors (box 1). Wilde (2001) argues that this target level of risk is specifically determined by four categories of motivating (subjective utility) factors, namely the expected *advantages* of comparatively *risky* behaviour alternatives (e.g. saving time by ignoring a security measure); the expected *costs* of comparatively *risky* behaviour alternatives (e.g. time and effort to recover from a computer virus); the expected *benefits* of comparatively *safe* behaviour alternatives (e.g. maintaining the confidentiality,

integrity and availability of information); and the expected *costs* of comparatively *safe* behaviour alternatives (e.g. cumbersome procedures). Based on these four categories, it is then concluded that if the expected advantage of risky behaviour (category 1) and the expected costs of save behaviour (category 4) are high, the target level of risk will also be high. Conversely, the target level of risk will be low if the expected costs of risky behaviour (category 2) and the expected benefits of safe behaviour (category 3) are high. Any significant information-security-related event will cause a change in the perceived level of risk (box 4). If new security measures are implemented, for example, or if new security threats emerge, the perceived level of risk will be lower or higher accordingly. This change means that the perceived risk has become notably different (lower or higher) than the target level of risk. In the case of a new threat, users tend to change their security behaviour by choosing more secure alternative options (box 6). This, in turn, will result in a change of status (rate) of security breaches (box 7). As time passes and users become more informed about the new threat, they may realise that the threat is not that serious, or they may discover that the new threat is well controlled through new security measures, or they may simply become used to the new threat. The level of perceived risk may then drop below the target risk and users may start to behave less cautiously, which will then result in a new surge in the number of security breaches. A risk homeostasis model is therefore a closed loop of processes and variables that are continuously adjusted and does not imply constancy. It should thus be seen as a process and not an outcome (Wilde, 2001). The homeostasis process operates on the level of individuals, but Wilde also argues that individuals collectively represent larger groups or populations of people.

It is noteworthy that the risk homeostasis theory is not free from negative critique and there are researchers who do not agree with the theory. O'Neill and Williams (1998) present a rather sarcastic rebuttal of the theory and reject it as a mere hypothesis. Their arguments are based on road safety examples and may be debatable. Trimpop (1996) provides further details and literature references on arguments for and against risk homeostasis.

3.2 Risk homeostasis in information security

Surprisingly, there is very little in the literature on risk homeostasis in the context of information security. Pattinson and Anderson (2004) believe that risk homeostasis applies to many information security scenarios. According to them, risk homeostasis is a management theory and the essence of information security is to manage risk. To demonstrate its applicability, they describe a few practical (hypothetical) examples that include firewalls and anti-virus software, the introduction of a new security-related policy, physical security and the use of specific software controls. Based on these examples, they then conclude that there may be a number of advantages for organisations if they recognise risk homeostasis as a valid component of information security risk. Stewart (2004) also contends that risk homeostasis is a factor in information security and presents new directions for security professionals, companies and the security industry on how to treat risk. Risk homeostasis theory in the context of information security was also referred to in a study by Sawyer et al. (1999). In this research report, the authors studied the role of risk homeostasis in response to the well-known Michelangelo computer virus threat and concluded that risk homeostasis does indeed play a role in risk perceptions, risky behaviours and protective behaviours. Other researchers mention risk homeostasis only briefly as a possible tool for explaining risk issues in information security. Examples include Farahmand et al. (2008), who presented risk homeostasis as background information in their study on incentives and perceptions of information security risks; Pattinson and Anderson (2007), who listed the theory of risk homeostasis as one of the human factors that will impact upon an organisation's information security environment; Albrechtsen (2007), who suggested risk homeostasis theory as an explanation for poor security behaviour of users and, based on this, concluded that new approaches are needed to manage the role of users in information security; and D'Arcy and Green (2014), who noted an unexpected

negative association between perceived organisational support and security compliance intention. They posited that the explanation for this observation is related to the concept of risk homeostasis, as employees who perceive strong organisational support in general may feel that information security problems will be handled by the IT department and that compliance practices are therefore not critical. Studies also exist where the focus is on different (but related) topics, but where the risk homeostasis theory is mentioned, for example in a study of Williams and Noyes (2007) on perceptions of risk in decision-making, and in a study of Workman et al. (2008), who constructed a threat control model to understand the knowing-doing gap of users.

One of the problems of accepting the risk homeostasis theory in the context of information security is the difficulty in determining the extent of its application (Pattinson and Anderson, 2004). The use of a repertory grid technique to try and measure risk-taking behaviour has been proposed by Pattinson and Anderson (2004), whereas Hoyes et al. (1996) list four approaches to evaluate the claims of risk homeostasis. These four approaches are the construction of theoretical/cognitive and mathematical models; the examination of loss statistics; the performance of experiments in which measures are taken before and after an intervention; and simulation studies. It is important to note that all these proposed methodologies have their own unique shortcomings and may not be suitable in all circumstances. What is significant, though, is that the mechanism in risk homeostasis (to adjust or regulate risk) involves three behavioural changes, namely behavioural adjustments within the environment (to do the same thing but in a different manner); "mode migration" (to stop doing something and to do something else in order to achieve the same objective); and avoidance (to stop doing something) (Hoyes et al., 1996).

In an effort to demonstrate (not to prove) the possible presence of homeostatic principles in information security behaviour, the ensuing paragraphs of this section refer to case studies that were conducted earlier and that have already been reported on in the literature (Kearney and Kruger, 2013; 2014). The case studies entail practical information security exercises that were conducted at a very large utility company with over 3,500 IT users. The company has an in-house information security training programme that is mandatory for all staff with access to the IT infrastructure. The main objective of this programme is to make IT users aware of information security threats and risks, as well as to explain to them their responsibilities and role in protecting the company's information assets. There are also a variety of formal and informal channels to inform users on an on-going basis of the importance of information security and its associated risks. Top management views information security as a vital function and promotes its support for a strong and secure information environment publicly. All of these are indicators that a high level of information security awareness is maintained in the company. The high level of information security awareness is further confirmed by formal (e.g. internal audits) and informal (e.g. conversations, newsletters and seminars) activities in various sections of the company. It is therefore reasonable to assume that IT workers in the company under study are well informed about information security, the associated risks and threats and how to react or respond to them.

Against this background of a high level of information security awareness, a practical phishing experiment was conducted in which users were asked (via email) to provide their usernames and passwords on a web link. The results were unexpected and contradictory to the high levels of security awareness; of the 280 users who responded over a short period of time, 231 (83%) revealed the required personal details. Complete details of the phishing exercise were reported in Kearney and Kruger (2013). This test was later on followed up with a similar phishing test and results showed that there was no improvement in terms of the number of people who gave away their personal details; in fact, the numbers increased from the first to the second test. Detailed results on this follow-up test were presented in Kearney and Kruger (2014).

In an effort to understand the observed security behaviour better, a trust survey was conducted (Kearney and Kruger, 2014). The aim of the trust survey that was carried out on an interview basis was to determine whether trust plays a role in information security behaviour. A secondary objective was to obtain specific information on how users perceive risks and controls pertaining to email and social engineering threats. Results of the trust survey have shown that there is a significant high level of trust amongst employees in the ability of the company to provide a safe, secure and trustworthy environment. Without exception, responses to questions such as "Do you think the organisation protects and secures email communications and related data adequately?" were all positive. A significant number of respondents also indicated that they prefer to do their home banking and other online transactions from work as they feel protected and safe in the work IT environment. Further significant and insightful information was obtained (and confirmed) during follow-up informal discussions with some of the respondents. Explanations on why certain actions are normally taken, including aspects such as workload, limited time to complete tasks, trust and experience of well-controlled risk areas, were given by a large number of respondents.

Based on the results of these practical tests, it appears as if risk homeostatic principles do play a role in information security behaviour. When employees, for example, know or perceive that adequate controls are in place, they will adjust their risk exposure upwards. Users may become more careless and respond to the phishing scam when they know (or perceive) that adequate controls (e.g. spam filters) are in place. The observed high level of trust and associated high number of phishing victims are in line with the risk homeostasis concept, that is, the high level of trust (and thus the low level of risk experienced by users) apparently leads to users compensating for low risk by changing their behaviour and taking more risks, eventually becoming victims of a security breach such as the phishing test. Furthermore, circumstances and feedback that has been received fit perfectly into the motivating factors that Wilde (2001) claims to be determinants of the target level of risk (see section 3.1). The advantage of risky behaviour that is fuelled by the high level of trust is fairly high – this is evidenced by remarks of respondents such as "I have a high workload" (and thus no time for random small problems); "I need to complete certain tasks"; and "I do not have time for cumbersome procedures to investigate or report emails". These issues make it much more attractive to choose the riskier option of providing the required details. It is also a fact that the cost of safe behaviour is high. If a user wants to investigate or report the incident, it will take time – something that users are not prepared to give up easily. Users confirmed that they trust and have experience of good controls; this contributes to an attitude of "no need for concern". The high levels of these two motivating factors will drive the target risk that users are willing to take higher, whereas the perceived risk is low; this, in turn, will result in riskier behaviour such as falling for a phishing scam. It may be argued that users can simply ignore the phishing email, which is the correct thing to do. However, the high levels of trust, coupled with a perceived safe and secure environment, cause many users to believe that if they do receive an email, it will be a legitimate message to which they should respond – a typical homeostatic assumption.

The real world example described here does not prove that risk homeostasis is present in each and every security incident. It is a practical test and observation that support the homeostatic arguments of other researchers and provide new insights into security behaviour. More importantly, it opens up new and exciting avenues that can be explored (together with other psychological models) to explain the sometimes paradoxical information security behaviour.

3.3 Risk homeostasis: similarities with other models

As mentioned in the introduction, the use of psychological and other cognitive models in information security has almost become a de facto standard. Some of the more prominent models and their

application were briefly discussed in the introduction. Additional support for this type of approach in information security can also be found in other more generic studies of researchers such as Anderson and Moore (2009), Enrici et al. (2010) and Tsohou et al. (2015).

Risk homeostasis is also considered a behavioural framework that tries to explain behaviour in terms of risk and there are many conspicuous similarities between risk homeostasis and the other prominent behaviour models. Given the popularity of these other models and approaches in information security behaviour, it is noteworthy that there is a considerable lack of studies on risk homeostasis as a potential explanatory theory for information security behaviour. The rationale of this section is therefore to highlight some of the similarities between risk homeostasis and other well-studied behavioural models briefly. The idea is to show the need for more focused risk homeostasis studies in the context of information security.

The theory of reasoned action (TRA) and its extension, the theory of planned behaviour (TPB), are mainly based on users' intention which is driven by their attitude towards security behaviour. Bulgurcu et al. (2010) have drawn on the TPB model and state that attitude is influenced by *benefit of compliance, cost of compliance* and *cost of non-compliance*. Wilde's (2001) motivating factors in risk homeostasis are also significantly influenced by attitudes and perceived behavioural control. The statements by Bulgurcu et al. (2010) may therefore also be stated in terms of the motivating factors in risk homeostasis, for example the *benefit of safe behaviour (compliance), cost of safe behaviour (compliance)* and *cost of risky behaviour (non-compliance).*

There also seems to be an "overlap" amongst concepts in protection motivation theory (PMT) and the motivating factors in risk homeostasis. Ifinedo (2012) explains that PMT consists of two distinct processes called a threat appraisal and a coping appraisal. Part of the threat appraisal is an evaluation of the perceived severity, in other words the severity of the consequences of the event, for example non-compliance (behaviour) with a security policy. This is an analogous statement of Wilde's motivating factors where the advantages and costs of behaviour are weighed. The coping appraisal process consists of elements such as response efficacy (the belief about the perceived benefits of the action taken) and response cost (the perceived opportunity cost adopting a recommended behaviour). Again, these elements translate seemingly easy into the motivating factors of risk homeostasis.

Other theories such as the general deterrence theory (GDT) and the closely related factor of fear are also related to the motivating factors, as an emotion such as fear will influence a user's decision on expected cost benefits of a safe or risky behaviour option. This is confirmed by Johnston and Warkentin (2010) who concluded that fear appeals do impact end user behavioural intentions to comply with recommended individual acts of security.

The aim of this summarised section is not to provide a comparative analysis of risk homeostasis with other well-known behavioural models, but rather to point out that all these models have similarities and are, to a certain degree, in one way or another linked to each other. It therefore seems that if the (other) psychological models are frequently studied in the context of information security, the seemingly associated risk homeostasis theory will probably also provide new insights and explanations to the recurring information security problems that are linked to the human element in information security.

4. Discussion and concluding remarks

Risk homeostasis on its own cannot provide absolute answers to information security behaviour. Shameli-Sendi et al. (2016) rightly pointed out that risk is also dependent on other factors that are constantly changing. These other factors will influence the perceived benefits and costs of a chosen

behaviour. One example is the personal trait of narcissism that will influence perceptions and behaviour. Narcissism is described by Campbell et al. (2011) as a stable individual difference consisting of grandiosity, self-love and inflated self-views but except for the work of Cox (2012a, 2012b), there is very little on narcissism and information security in the literature.

The objective of the brief discussion of risk homeostasis in this paper is to highlight the opportunity to further theorise on information security risks, behaviour and a possible model that can help in explaining these intricacies. Security specialists and decision-makers will have to acknowledge that risk is not really quantifiable and that the evaluation of multiple risk factors pertaining to the human aspects of information security is only subjective. Due to the overwhelming human aspects and the many influencing factors, it is also necessary to accept that information security no longer operates in a paradigm of order where it is assumed that all phenomena are context-free; what is needed is a multi-level understanding of information security and the environment in which it operates. Stewart (2004) clearly explains the difference between another control measure and the creating of an environment in which users understand risks. According to his explanation, Western Australia passed a law in 1992 that made the wearing of a safety helmet for cyclers compulsory. However, the number of fatalities remained more or less on the same level after the law was passed. In the Netherlands, with more cyclists and only a few of them wearing helmets, the fatality and injury rates were much lower. The difference, according to Stewart, is that Australia identified a risk and implemented a control, whereas the Netherlands created an environment in which cyclists (users) could understand the risks and implemented new strategies (e.g. dedicated cycle lanes) to deal with the problem.

In general, the acceptance of a risk homeostasis model implies two important concepts to be dealt with, namely monitoring and intervention. It is important that a monitoring system is implemented to determine whether risk homeostasis principles are present and whether target and actual risk levels are appropriately evaluated. A natural starting point in the management and monitoring of information security risks is to ensure that the expectations of different groups of people are well managed. One way to do this is to assess the level of possible perceptual differences, which may give an indication of differences in the perceived and target levels of risk. Measuring techniques to achieve this are well documented in the literature (Ackam et al., 2015; Albrechtsen and Hovden, 2009; Posey et al., 2014). Another tool is trust surveys that may be employed to identify the presence of homeostatic activities. In section 3.2, an example of such a trust survey and the way in which it may be linked to risk homeostasis have been presented. Furthermore, certain practical, information security-related tests may be used to reveal information on risk levels and a need for intervention. An example of a practical security test is a phishing exercise – also briefly described in section 3.2. These types of security tests will provide valuable insights into risk levels of a risk homeostasis model and are also well documented in the literature (Jansson and Von Solms, 2013; Pattinson et al., 2012). Finally, more direct and intensive investigations into different cost/benefit scenarios may be performed to monitor and evaluate risks in a risk homeostasis model. Beautement et al. (2008) have conducted an informative study in this regard that can be translated directly to the principles of a risk homeostasis model. In this study, examples of specific scenarios of cost/benefit perceptions that were evaluated through user interviews are presented. Examples of such practical scenarios and monitoring opportunities documented by Beautement et al. include the cost or benefits of centrally scheduled tasks (e.g., automated virus scans); additional authentication; use of encryption; and restrictive firewalls.

In addition to the monitoring aspect, the risk homeostasis theory also suggests that interventions (usually technology, new policies or new awareness campaigns) be implemented to adjust perceived risk levels. A major issue with this, again, is the link between the human aspects and the interventions. In his recommendations, Stewart (2004) posits that this is frustrating for users, especially when users

believe that the level of security is sufficient. This implies that whenever risk homeostasis is considered as a model for managing risk, special attention should be given to the way in which risks and awareness are presented to users. Security measures may sometimes be perceived as being an obstacle and are then simply ignored (Bada and Sasse, 2014). In other cases, security-related information passed on to users may be so overwhelming that users may filter them out mentally as being something similar to spam (Furnell and Thomson, 2009). This important aspect of security fatigue should be taken into account when using the risk homeostasis model to manage risks and security behaviour. Bada and Sasse (2014) refer to the security versus usability triangle and argue that security fatigue will become an issue if security and usability are not balanced. The two concepts tend to be inversely related and a high secure system with low usability will result in a secure system that no one uses, whereas a low secure system with high usability will be used by everyone, including unauthorised users. Security fatigue is a real threat in general, but also specifically in the risk homeostasis model when the aim is to change perceptions of users. Furnell and Thomson (2009) offer guidelines on security fatigue factors that include effort (the requirement to comply); difficulty (ease in providing the required effort); and importance (way in which a user prioritise the need to secure an asset).

When considering security fatigue and security measures, Norman (2010) makes the following statement: “The more secure you make something, the less secure it becomes”. This is an issue that should be considered seriously by security specialists. A possible framework to understand this contradictory principle that has not yet been applied in an information security context is the *slower is faster* (SIF) effect that has been described by Gershenson and Helbing (2015). The basic premise behind the SIF effect is that a system performs worse when the components of the system are trying to do better. Gershenson and Helbing present various examples to illustrate this effect. Some of the examples include pedestrian dynamics (individuals trying to evacuate a room too quickly, leading to clogging and a reduced outflow as opposed to a calmer and slower evacuation), vehicle traffic, social dynamics, ecological systems, logistics and supply chains. The most probable message from the SIF effect to information security is that security awareness programmes need to contain selective material and should not be bombarding users with overwhelming amounts of security information that may ultimately result in less security.

Presenting less (security) information to achieve better (security) behaviour appears to be viable. Bargh et al. (1996) performed interesting experiments to show that behaviour is often triggered automatically in the mere presence of relevant situational factors. In one of these experiments, participants were asked to construct short sentences from a few scrambled words. The authors used three versions of the scrambled-sentence test with the first one being intended to prime the construct *rude* (using words such as aggressive, annoying, interrupt and infringe); the next one intended to prime the construct *polite* (using words such as respect, cordial and courteous); and the last one intended to prime a *neutral* condition. Once a participant had constructed the sentences in one of the three categories, he/she was asked to proceed to the next room in order to receive further instructions. In this room, the instructor was talking to another person, causing the arriving participant to wait. The time taken before the arriving participant would interrupt them was recorded and the interesting and surprising results were that those who were exposed to “rude” words would interrupt them quicker than those who were exposed to “neutral” words. The participants exposed to “polite” words would wait the longest before they would interrupt. Using the results of this automaticity of social behaviour experiment, the question for information security specialists is the following: Would it not be more advantageous to have a security awareness programme (or whatever is used to try and influence behaviour) that focuses on “short” pieces of information rather than the traditional “longer” security and awareness programmes? This

approach will not only influence behaviour but will also serve as a counter measure for security fatigue. It also fits in perfectly with the SIF effect.

To further illustrate the potential problem of too much security information and too many controls, a small practical test was conducted by using a non-probability convenience sampling method. These types of sampling methods provide a quick and easy way to poll the opinion of people (Wegner, 1993). Twenty five fourth-year students in Computer Science were asked to express what their preference was between two different instructions on how to choose a password. The first option simply states, "Choose and manage your password in a safe and secure manner to ensure that it stays confidential at all times". The second option also instructs them to choose a password and then presents a list of 14 properties of a safe password (e.g. length, characters to use etc.) that respondents have to comply with. A total of 18 students responded and 50% of them indicated that they would prefer the shorter instruction in the first option. Comments on why they chose the shorter instruction include the following: "I know the importance of passwords"; "Too many instructions will lead to people not worrying anymore"; and "Too many rules are irritating". It should be noted that these respondents were students who had not yet entered the work place and had not yet been exposed to formal information security training and awareness programmes. Despite these facts, they already showed a preference for shorter or easier security messages – and maybe they already suffered from security fatigue, albeit to a lesser extent.

To summarise: Risk homeostasis offers to decision-makers a different (and not sufficiently explored) way of understanding and managing risk and information security behaviour. The homeostatic principle of interventions to adjust perceived and target risk may cause other difficulties of which security fatigue appears to be an important role player. The potential problems associated with security fatigue may, however, be addressed with other sociological approaches such as the slower is faster (SIF) effect and the automaticity of social behaviour experiments that complement each other.

5. Conclusion

The human aspect of information security has turned it into a complex area of study. There is widespread recognition of the fact that technology on its own does no longer offer complete solutions to the information security problem. New models, approaches and techniques are needed to manage and understand information security risks and behaviour. What seems to be popular amongst security specialists is to investigate and apply behavioural theories that originate from the psychological and social sciences. One such theory that appears to be almost ignored in the context of information security is the theory of risk homeostasis. Some information security researchers have touched on this theory (Farahmad et al., 2008; Pattinson and Anderson, 2004; Stewart, 2004), but there is a general lack of literature on risk homeostasis in information security. This paper attempts to create an opportunity to begin theorising on risk homeostasis as a model that should be considered, along with other factors, in information security frameworks.

The paper suggests that risk homeostasis offers a different view and way of understanding security behaviour. A brief motivation on why risk homeostasis should be considered was followed by a description of the theory. The model's applicability to information security was explained and similarities with other behavioural frameworks were highlighted. In the final concluding remarks, it was also pointed out that there are two issues attached to the adoption of a risk homeostasis model – a need for a monitoring function as well as a need to implement specific interventions to adjust perceived risk levels. Linked to these two issues are specific difficulties, of which security fatigue is a major role player that may occur when applying the homeostatic principles. Suggestions to deal with this problem were made and include approaches that have not yet been implemented in information security – the

two approaches that were suggested are the slower is faster (SIF) effect and an automaticity of social behaviour assumption.

In general, the paper opens up the prospect to theorise on the risk homeostasis concept in information security behaviour and culture. At a more practical level, it offers decision-makers and security specialists useful information and new insights that could be advantageous in a strategic security planning process.

References

Akcam, B.K., Hekim, H. and Guler, A. (2015). "Exploring business student perception of information and technology". *Procedia – Social and Behavioral Sciences*, 195:182-191.

Albrechtsen, E. (2007). "A qualitative study of users' view on information security". *Computers & Security*, 26:276-289.

Albrechtsen, E. and Hovden, J. (2009). "The information security digital divide between information security managers and users". *Computers & Security*, 28:476-490.

Anderson, R. and Moore, T. (2009). "Information security: where computer science, economics and psychology meet". *Philosophical Transactions of the Royal Society A*, 367:2717-2727.

Bada, M. and Sasse, A. (2014). "Cyber security awareness campaigns. Why do they fail to change behavior?" Global Cyber Security Capacity Centre: Draft working paper. July 2014.

Bargh, J.A., Chen, M. and Burrows, L. (1996). "Automaticity of social behavior: direct effects of trait construct and stereotype activation on action". *Journal of Personality and Social Psychology*, 71(2):230-244.

Beautement, A., Sasse, M.A. and Wonham, M. (2008). "The compliance budget: Managing security behaviour in organisations". Proceedings of the New Security Paradigms Workshop (NSPW08). DOI: 10.1145/1595676.1595684.

Boer, H. and Seydel, E.R. (1996). "Protection Motivation Theory", available at doc.utwente.nl/34896/1/K465_.pdf (accessed 12 November 2015).

Brewer, N.T., Cuite, L.C., Herrington, J.E. and Weinstein, N.D. (2007). "Risk compensation and vaccination: can getting vaccinated cause people to engage in risky behaviours?" *Annals of Behavioural Medicine*, 34(1):95-98.

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.

Campbell, W.K., Hoffman, B.J., Campbell, S.M. and Marchisio, G. (2011). "Narcissism in organizational contexts". *Human Resource Management Review*, 21:268-284.

Cox, J.A. (2012a). "Information systems user security: A structured model of the knowing-doing gap". *Computers in Human Behavior*, 28:1849-1858.

Cox, J.A. (2012b). “Organizational narcissism as a factor in information security: a structured model of the user knowing-doing gap”. PhD Dissertation, Capella University.

Crossler, R.E. (2010). “Protection motivation theory: understanding determinants to backing up personal data”. The 43rd Hawai International Conference on System Sciences. DOI: 10.1109/HICSS.2010.306.

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*, 32:90-101.

D’Arcy, J., Hovav, A. and Galletta, D. (2008). “User awareness of security countermeasurers and its impact on information systems misuse: a deterrence approach”. *Information Systems Research*. DOI: 10.1287/isre.1070.0160.

D’Arcy, J. and Green, G. (2014). “Security culture and the employment relationship as drivers of employees’ security compliance”. *Information Management & Computer Security*, 22(5):474-489.

Enrici, I., Ancilli, M. and Lioy, A. (2010). “A psychological approach to information technology security”. 3rd International Conference on Human System Interaction, HSI2010. DOI: 10.1109/HIS.2010.5514528.

Farahmand, F., Atallah, M. and Konsynski, B. (2008). “Incentives and perceptions of information security risks”. Proceedings of the 29th International Conference on Information Systems (ICIS). Available at http://aisel.aisnet.org/icis2008/25 (accessed 13 June 2016).

Frangopoulos, E.D., Eloff, M.M. and Venter, L.M. (2014). “Human aspects of information insurance: a questionnaire-based quantitative approach to assessment”. Proceedings of the 8th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014).

Fricke, M. (2015). “Big data and its epistemology”. *Journal of the Association for Information Science and Technology*, 66(4):651-661.

Furnell, S. and Clarke, N. (2012). “Power to the people? The evolving recognition of human aspects of security”. *Computers & Security*, 31:983-988.

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

Gershenson, C. and Helbing, D. (2015). “When slower is faster”. *Complexity*, 21(2):9-15.

Gundu, T. and Flowerday, S.V. (2013). “Ignorance to awareness: towards an information security awareness process”. *South African Institute of Electrical Engineers*, 104(2):69-79.

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

Herath, T. and Rao, H.R. (2009b). “Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness”. *Decision Support Systems*, 47(2):1546-165.

Hoyes, T.W., Stanton, N.A. and Taylor, R.G. (1996). “Risk homeostasis theory – a study of intrinsic compensation”. *Safety Science*, 22(1-3):77-86.

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

Jansen, J. (2015). “Studying safe online banking behavior: a protection motivation theory approach”. Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015).

Jansson, K. and Von Solms, R. (2013). “Phishing for phishing awareness”. *Behaviour and Information Technology*, 32(6):584-593.

Johnston, A.C. and Warkentin, M. (2010). “Fear appeals and information security behaviors: an empirical study”. *MIS Quarterly*, 34(3):549-566.

Kearney, W.D. and Kruger, H.A. (2013). “Phishing and organizational learning”, In SEC2013, IFIP AICT 405, eds. Janczewski, LJ, Wolf, H, Shenoi, S. p379-390.

Kearney, W.D. and Kruger, H.A. (2014). “Considering the influence of human trust in practical social engineering”. 13th International Information Security for South Africa Conference (ISSA 2014).

Khan, B., Alghatbar, 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.

Kim, S.H., Yang, K.H. and Park, S. (2014). “An integrative behavioral model of information security policy compliance”. *The Scientific World Journal*, available at http://dx.doi.org/10.1155/2014/463870 (accessed 14 May 2015).

Kokolakis, S. (2015). “Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon”. *Computers & Security*, In Press.

Lebek, B., Uffen, J., Breitner, M.H., Neumann, M. and Hohler, B. (2013). “Employees’ information security awareness and behavior: a literature review”. The 46th Hawai International Conference on System Sciences. DOI: 10.1109/HICSS.2013.192.

Meso, P., Ding, Y. and Xu, S. (2013). “Applying protection motivation theory to information security training for college students”. *Journal of Privacy and Security*, 9(1):47-67.

Norman, D.A. (2010). “When security gets in the way”, available at http://jnd.org/dn.mss/when_security_gets_in_the_way.hmtl (accessed 20 November 2015).

O’Neill, B. and Williams, A. (1998). “Risk homeostasis hypothesis: a rebuttal”. *Injury Prevention*, 4:92-93.

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010). “Human factors and information security: Individual, culture and security environment”. Australia Government, Department of Defence. Command Control, Communications and Intelligence Division, Defense Science and Technology Organisation, Edinburgh, Australia.

Pattinson, M.R. and Anderson, G. (2004). “Risk homeostasis as a factor of information security”, available at http://www.igneous.scis.ecu.edu.au (accessed 13 April 2015).

Pattinson, M.R. and Anderson, G. (2007). “How well are information risks being communicated to your computer end-users?”. *Information Management & Computer Security*, 15(5):362-371.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A. and Butavicius, M. (2012). “Why do some people manage phishing e-mails better than others?”. *Information Management and Computer Security*, 20(1):18-28.

Pinkerton, S.D. (2001). “Sexual risk compensation and HIV/STD transmission: empirical evidence and theoretical considerations”. *Risk Analysis*, 21(4):727-736.

Posey, C., Roberts, T.L., Lowry, P.B. and Hightower, R.T. (2014). “Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders”. *Information and Management*, 51:551-567.

Roghanizad, M.M. and Neufeld, D.J. (2015). “Intuition, risk, and the formation of online trust”. *Computers in Human Behavior*, 50:489-498.

Sawyer, J.E., Kernan, M.C., Conlon, D.E. and Garland, H. (1999). “Responses to the Michelangelo computer virus threat: The role of information sources and risk homeostasis theory”. *Journal of Applied Social Psychology*, 29(1):23-51.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016). “Taxonomy of information security risk assessment (ISRA)”. *Computers & Security*, 57:14-30.

Siponen, M., Pahnila, S. and Mahmood, A. (2007). “Employees’ adherence to information security policies: an empirical study”, In IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, *eds*. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer). p133-144.

Sommestad, T. and Hallberg, J. (2013). “A review of the theory of planned behavior in the context of information security policy compliance”, In SEC2013, IFIP AICT 405, eds. Janczewski, L.J., Wolfe, H.B., Shenoi, S. p257-271.

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.

Stewart, A. (2004). “On risk: perception and direction”. *Computers & Security*, 23:362-270.

Straub, D.W. (1990). “Effective IS security: an empirical study”. *Information Systems Research*, 1(3):255-276.

Trimpop, R.M. (1996). “Risk homeostasis theory: problems of the past and promises for the future”. *Safety Science*, 22(1-3):119-130.

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*, 52:128-141.

Vaidyanathan, G. and Berhanu, N. (2012). “Impact of security countermeasurers in organizational information convergence: a theoretical model”. *Issues in Information Systems*, 13(2):21-25.

Vance, A., Siponen, M. and Pahnila, S. (2012). “Motivating IS security compliance: Insights from habit and protection motivation theory”. *Information and Management*, 49(3-4):190-198.

Vehovar, V., Sicherl, P., Husing, T. and Dolnicar, V. (2006). “Methodological challenges of digital divide measurements”. *The Information Society: An International Journal*, 22(5):279-290.

Verendel, V. (2009). “Quantified security is a weak hypothesis. A critical survey of results and assumptions”. Proceedings of the 2009 workshop on new security paradigms workshop, ACM Digital Library.

Wegner, T. (1993). *Applied business statistics. Methods and applications*, Juta and Co, Ltd.

Wilde, G.J.S. (1994). *Target risk*. PDE Publications, Toronto, Canada.

Wilde, G.J.S. (1998). “Risk homeostasis: an overview”. *Injury Prevention*, 4:89-91.

Wilde, G.J.S. (2001). *Target Risk 2*. PDE Publications, Toronto, Canada.

Williams, D.J. and Noyes, J.M. (2007). “How does our perception of risk influence decision-making? Implications for the design of risk information”. *Theoretical Issues in Ergonomics Science*, 8(1):1-35.

Workman, M., Bommer, W.H. and Straub, D. (2008). “Security lapses and the omission of information security measures: A threat control model and empirical test”. *Computers in Human Behavior*, 24: 2799-2816.

Chapter 8
Summary and conclusion

8.1 Introduction

Chapter 8 is the final chapter of the research project. A synopsis of the study and the way in which the research objectives have been achieved are presented. The chapter is then concluded with some limitations as well as direction for further research.

8.2 Synopsis of the study

The thesis comprises seven chapters, followed by this final summary and conclusion chapter. The first chapter is an introductory chapter that contextualises the study. The next chapter presents a high-level summary of examples of literature used in the study. Five articles are then presented, each as a chapter. A synopsis of each of the first seven chapters will be given in this section.

Chapter 1 serves as an introduction and orientation to the study. Background information to the information security behaviour problem was presented, which gave rise to the problem statement, research objectives, and the research design and paradigm. The research aims and objectives of the study, as set out in Chapter 1, were as follows:

Primary objective

- To research the link between risk homeostasis and aspects of information security behaviour

Secondary objectives

- The construction of an appropriate framework that can be used to identify unique dimensions of good corporate governance
- A demonstration of how a security incident (social engineering) can create opportunities for organisational learning
- Investigating the role of trust as a possible explanatory variable in the privacy paradox
- Studying the influence of perceptual differences in contradictory information security behaviours

Chapter 2 was devoted to a high-level summary of examples of literature resources used in the study. Each of the other chapters contains a comprehensive bibliography, hence the summarised literature review presented in Chapter 2.

In Chapter 3, the manuscript entitled “A framework for good corporate governance and organisational learning – an empirical study” was presented. This paper details the use of a value-focused approach to determine unique dimensions of good corporate governance. This resulted in a framework for

practitioners to determine fundamental objectives and how to achieve them. The framework, as well as the methodology to construct the framework, is a new contribution in the field of corporate governance, particularly in the risk management area. In offering this framework, Chapter 3 realised the first secondary research objective of the study successfully.

In Chapter 4, the manuscript entitled “Phishing and organisational learning” was presented. This paper shows firstly how a practical security incident can create an opportunity for organisational learning. Secondly, the practical social engineering test provides empirical evidence to highlight information security behaviour problems (i.e. the privacy paradox) despite high levels of information security awareness. The combination of a security incident and organisational learning, and the empirical confirmation of problems such as the privacy paradox are new contributions in the field of both information security behaviour and organisational learning. This fulfilled the requirements for the second secondary research objective of the study.

Chapter 5 comprises the manuscript entitled “Considering the influence of human trust in practical social engineering”. The paper describes a unique trust survey linked to the practical social engineering tests and confirms that human trust plays a role in the information security knowing-doing gap. The specially focused trust survey provides empirical evidence of the trust aspect in information security behaviour and is an early indication of risk homeostasis as a factor in information security. This insight and empirical confirmation addressed the third secondary research objective successfully.

The manuscript “Can perceptual differences account for enigmatic information security behaviour in an organisation?” is presented as Chapter 6. In this paper, a specially focused survey on perceptual differences is described between different groups of people. The paper then shows that perceptual congruence is a prerequisite for a successful information security environment. Finally, based on this result, a new model is proposed for a safe and secure information environment. The perceptual differences survey and the new proposed model constitute contributions and realised the fourth secondary research objective successfully.

In Chapter 7, the manuscript entitled “Theorising on risk homeostasis in the context of information security behaviour” was presented. The previous chapters on risk dimensions, phishing and organisational learning, trust and perceptual differences all lead to this final paper on risk homeostasis as a factor in information security. The paper opens up new prospects to theorise on the risk homeostasis model (which is understudied in information security) as a framework that can be used to explain and predict information security behaviour. At a more practical level, the results from this paper offer decision makers and security specialists useful information and new insights in order to perform proper, strategic security planning activities. Theorising on risk homeostasis in information security at the level

of detail that has been presented in this study is a new contribution to the body of knowledge in information risk management, information security behaviour and the use of psychological models in the field of information security. The results of this paper fulfilled the requirements for meeting the primary objective of the study.

Figure 8.1 is a graphical illustration of how the research objectives were linked to the research questions (see Section 1.3, Chapter 1) and how they were addressed.

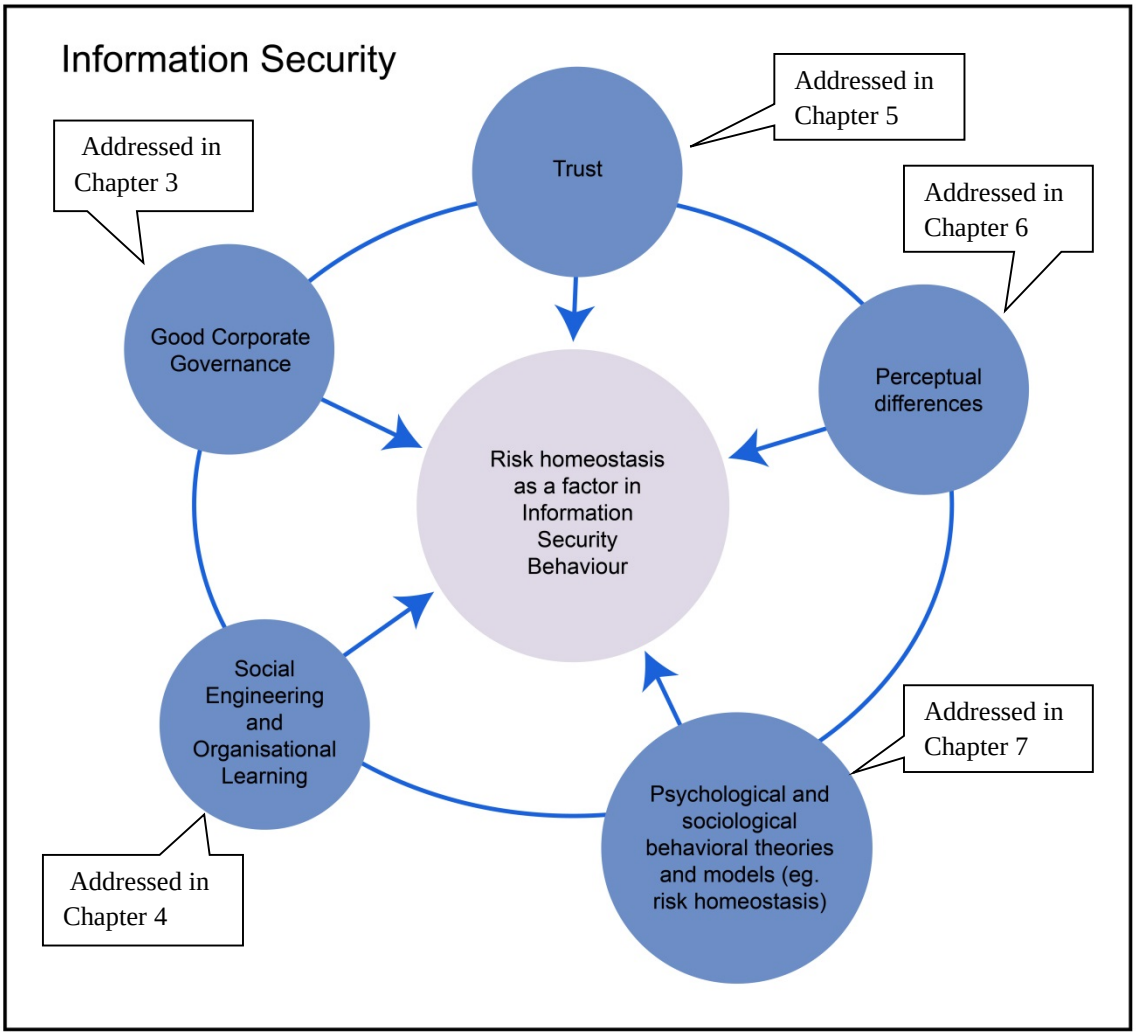


Figure 8.1: Assessment of the research objectives

The contributions made by this research study (and briefly mentioned above) were presented in Section 1.8 of Chapter 1.

8.3 Limitations of the study

This thesis is based on work that was performed at one large utility organisation. This may be seen as a limitation. However, the company that had been selected for the study is a perfect representative of modern day companies. The size of the company, as well as the state-of-the-art technology used in the company and the well educated workforce at the company, makes it a suitable candidate for these types of studies.

Owing to time considerations, a key limitation of the project was the inability to fully apply a risk homeostasis model in the company under study and to evaluate such a model in practice. For this reason, the researcher has to content himself with a theoretical overview of risk homeostasis as a factor in information security. However, the theoretical overview, together with the results of the empirical experiments and the surveys, does provide sufficiently new knowledge and insights that open up new research avenues and create new practical and strategic opportunities.

8.4 Direction for future research

Although all objectives of the study were achieved successfully, the work performed here can be further evaluated in different sized organisations and different industry sectors. The practical utilisation of a newly developed theory or model takes time, as information security practitioners may be cautious to apply new methodologies in information security behaviour areas. The proposed approach therefore needs to be constantly tested, adapted and improved over time.

Despite the uniqueness of different organisations, it may be worthwhile to research the feasibility of standardised measuring instruments (i.e. to determine trust levels, perceptual differences etc.). A universal assessment method that can be used in conjunction with a risk homeostasis framework should also be of great advantage.

The use of a risk homeostasis model encourages the updating of information security policies, controls and awareness programmes. Further research could focus on the best way in which to integrate these aspects into a risk homeostasis model.

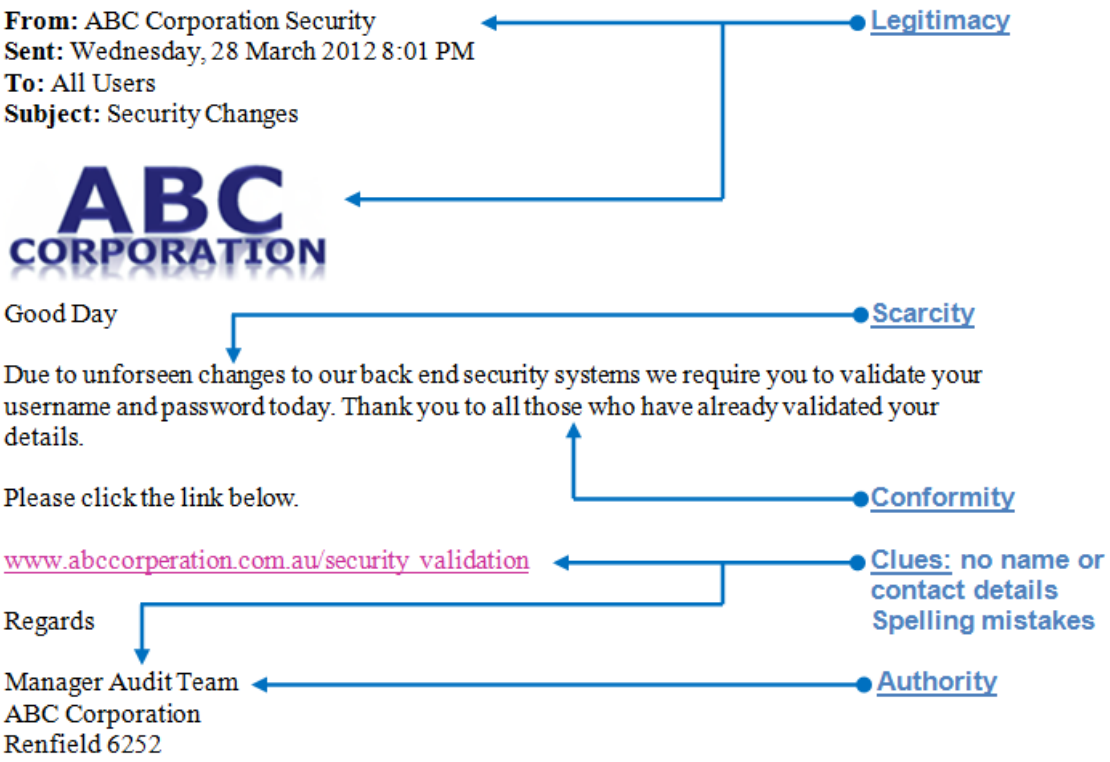
8.5 Chapter conclusion

Chapter 8 is the final chapter of this research project. The chapter presented a synopsis of the study and showed how the research objectives had been achieved. In conclusion, limitations of the study and possible future research opportunities were outlined.

Appendix A

Phishing e-mail message used in first practical test

To protect confidentiality and ensure privacy and anonymity of the organisation where the study was conducted, the company's real name was changed for publication purposes (e.g. ABC Corporation).

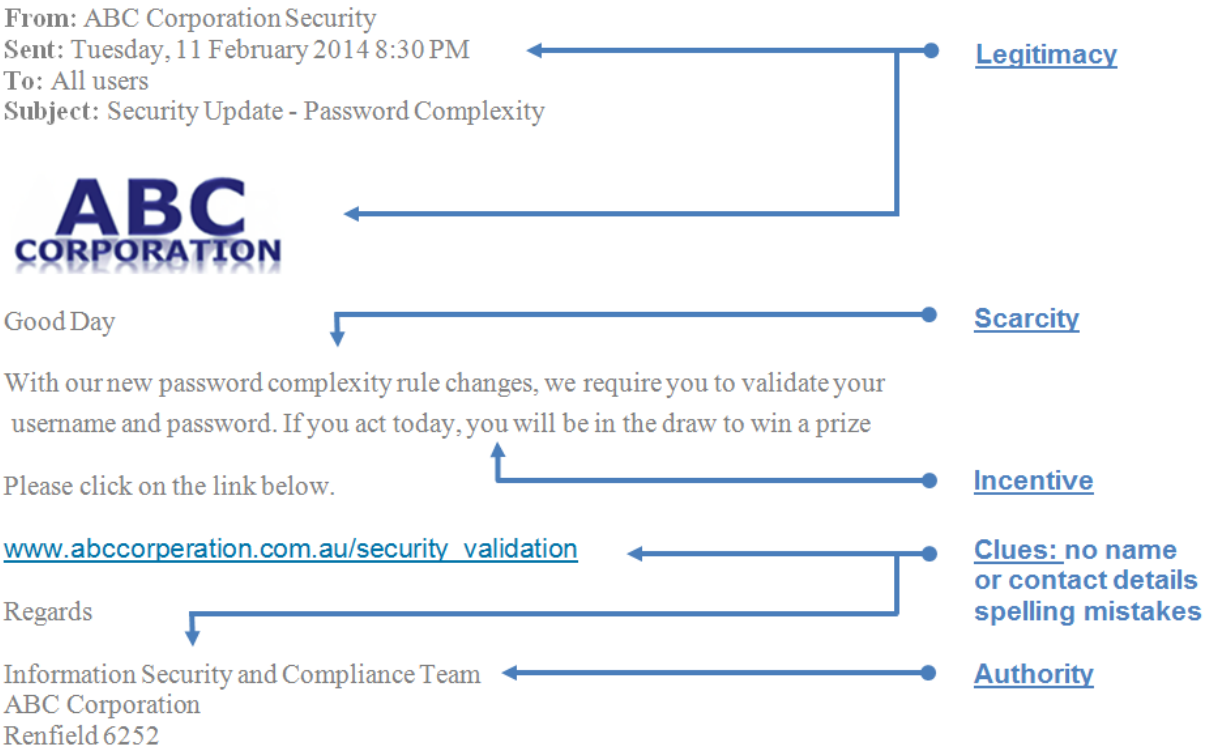


Appendix B

Phishing e-mail message used in follow-up practical test

To protect confidentiality and ensure privacy and anonymity of the organisation where the study was conducted, the company's real name was changed for publication purposes (e.g. ABC Corporation).

The details of 2nd phishing e-mail were the same as the first one (Appendix A) except for the wording of the short message.



Appendix C

Measuring instrument – trust survey

Date:
Name:

Business Unit: ☐ _____Managerial ☐_____Non-Managerial: ☐ _____

1. Have you ever been a victim of online fraud or cyber-crime in any form in the last 12 months? Yes☐ No ☐

2. Do you have both personal and work/corporate email accounts? Yes☐ No ☐

3. Are you aware of the compulsory Information Security training course in the Corporation? Yes☐ No ☐

4. Have you completed the information security course? Yes☐ No ☐

5. Are you aware of or know what the word or term "phishing" means?

Fully aware	Little aware	Heard the term	Not quite sure	Never heard of it
1☐	2☐	3☐	4☐	5☐

6. Have you ever received an email message or SMS on any of your private devices or emails asking for banking details, giving you a lottery win, asking to facilitate a large cash transaction or anything similar? Yes☐ No ☐

7. Have you ever received an email message or SMS on Corporate devices or emails asking for banking details, giving you a lottery win, asking to facilitate a large cash transaction or anything similar? Yes☐ No ☐

8. Do you treat suspicious emails received at home differently from those at work? Yes☐ No ☐

9. To what extent do you think the Corporation provides a secure or trustworthy IT environment?

Very secure	Somewhat secure	Neutral	Not very secure	Very insecure
1☐	2☐	3☐	4☐	5☐

10. Do you know what to do with a suspicious email at work?

Fully aware	Somewhat aware	Neutral	Not very secure	Very insecure
1☐	2☐	3☐	4☐	5☐

11. How often do you get suspicious emails at work?

At least daily	Weekly	Fortnightly	Monthly	Yearly or less

1☐	2☐	3☐	4☐	5☐

12. To what extent do you think the corporation responsible for the legitimacy or authenticity of emails received in your work Outlook in-box?

Fully responsible	Somewhat responsible	Unsure	A little responsible	Not at all
1☐	2☐	3☐	4☐	5☐

13. How often do you get suspicious email's at your private or personal address?

At least daily	Weekly	Fortnightly	Monthly	Yearly of less
1☐	2☐	3☐	4☐	5☐

14. Do you consider email’s received at the Corporation as safe and trustworthy?

Strongly agree	Agree	Neutral	Disagree	Strongly disagree
1☐	2☐	3☐	4☐	5☐

15. Do you do feel confident enough in the corporate systems to do your personal online banking?

Always	Possibly	Not sure	Doubtful	Never
1☐	2☐	3☐	4☐	5☐

16. Do you do feel confident enough in your own home systems to do your personal online banking?

Always	Possibly	Not sure	Doubtful	Never
1☐	2☐	3☐	4☐	5☐

17. Do you think the corporation protects and secures email communications and related data adequately?

Fully	Somewhat	Neutral	Not entirely	Not at all
1☐	2☐	3☐	4☐	5☐

18. Do you believe that you have enough knowledge or information to manage your information security risks?

Completely	Somewhat	Neutral	Not entirely	Not at all
1☐	2☐	3☐	4☐	5☐

19. Would you do internet banking at an internet café, free wifi hotspot or somewhere similar?

Always	Possibly	Not sure	Doubtful	Never
1☐	2☐	3☐	4☐	5☐

20. Do you think the Corporation should be testing staff awareness of "phishing" by conduction tests using dummy or fake emails?

Always	Possibly	Not sure	Doubtful	Never
1☐	2☐	3☐	4☐	5☐

Signature_____

Appendix D

Consent and measuring instrument – perceptual differences survey

Survey Title

Date: Time:

Name:

Title or Role:

Gender _____ Age_____ Years service _____

1. In your opinion, how well does the corporation manage their cyber risks (information security)

Poor	Neither Well nor Poor	Well	Very Well	Excellent
☐	☐	☐	☐	☐

Comment_____
_____
_____
_____

2. How many of the following measures does the corporation use to manage information security risks?

2.1. Firewalls	Yes☐	No ☐	Don't No ☐
2.2. Intrusion detection	Yes☐	No ☐	Don't No ☐
2.3. Latest software and updates	Yes☐	No ☐	Don't No ☐
2.4. Anti-virus	Yes☐	No ☐	Don't No ☐
2.5. Well trained staff/training	Yes☐	No ☐	Don't No ☐
2.6. Password complexity	Yes☐	No ☐	Don't No ☐
2.7. Password expiry rules	Yes☐	No ☐	Don't No ☐
2.8. Supporting policies and procedures	Yes☐	No ☐	Don't No ☐
2.9. Vendor and supplier management	Yes☐	No ☐	Don't No ☐
2.10. Awareness programs	Yes☐	No ☐	Don't No ☐
2.11. Monitoring	Yes☐	No ☐	Don't No ☐
2.12. Management reporting (reactive)	Yes☐	No ☐	Don't No ☐
2.13. Incident Management	Yes☐	No ☐	Don't No ☐
2.14. Physical security	Yes☐	No ☐	Don't No ☐

2.15. Regulatory/legislative	Yes☐	No ☐	Don't No ☐
2.16. Internal audit/assurance functions	Yes☐	No ☐	Don't No ☐

3. List the top 8 measures above in order of importance as a control to manage/mitigate information security risk (1 most important 5 least important) (See above)

Measure	1	2	3	4	5
1.	☐	☐	☐	☐	☐
Measure	1	2	3	4	5
2.	☐	☐	☐	☐	☐
Measure	1	2	3	4	5
3.	☐	☐	☐	☐	☐
Measure	1	2	3	4	5
4.	☐	☐	☐	☐	☐
Measure	1	2	3	4	5
5.	☐	☐	☐	☐	☐
Measure	1	2	3	4	5
6.	☐	☐	☐	☐	☐
Measure	1	2	3	4	5
7.	☐	☐	☐	☐	☐
Measure	1	2	3	4	5
9.	☐	☐	☐	☐	☐

4. Rank the following 14 information or cyber threats or vulnerabilities facing the Corporation with a 5 point scale, 1 being no risk, 2 little risk, 3 moderate, 4 high risk and 5 very high.(inherent, assuming no controls).

1. Human error

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

2. Virus/malware infections

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

3. Complacency

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

4. Misuse of sensitive information

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

5. Loss of information

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

6. Inappropriate use of email

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

7. Software vulnerability

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

8. Improper or inappropriate use of internet

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

9. Excessive private use

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

10. Social Engineering

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

11. Spam

No risk	Little risk	Moderate	High risk	Very high

☐	☐	☐	☐	☐

12. Hacking

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

13. Theft of equipment (hardware & software)

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

14. Illegal use

No risk	Little risk	Moderate	High risk	Very high
☐	☐	☐	☐	☐

5. Rank the top 5 vulnerabilities/risks identified in order of severity, 1 being the most severe, 5 being less but not insignificant. (Opinion only)

i. (most severe)_____
ii. _____
iii. _____
iv. _____
v. (least severe)_____

6. For each of the risks mentioned in Q5 above, list what you believe are the primary controls in place to mitigate them.

No Primary Controls

5i _____
5ii _____
5iii _____
5iv _____
5v _____

7. Rank these primary controls in terms of effectiveness using a 5 point scale

5i

Poor	Neither Well nor Poor	Well	Very Well	Excellent
☐	☐	☐	☐	☐

5ii

Poor	Neither Well nor Poor	Well	Very Well	Excellent
☐	☐	☐	☐	☐

5iii

Poor	Neither Well nor Poor	Well	Very Well	Excellent
☐	☐	☐	☐	☐

5iv

Poor	Neither Well nor Poor	Well	Very Well	Excellent
☐	☐	☐	☐	☐

5v

Poor	Neither Well nor Poor	Well	Very Well	Excellent
☐	☐	☐	☐	☐

8. Do you believe that the trade-off between the effectiveness of information security versus system functionality and performance is at the right level (the right balance of security vs ease of use)?

Yes ☐ No ☐

9. What do you believe are the reasons for your answer to Q8 above?

_____
_____
_____

10. In your opinion, who is responsible for information security in the Corporation?

_____
_____
_____

11. Is information security (in your opinion) considered a problem to be resolved with technology?

Yes ☐ No ☐

Comment_____
_____
_____
_____

Confirm consent form signed and dated

X_____

Consent Form – to take part in the research project

Research Project Participation

The purpose of this research project is to evaluate perceptions of respondents to determine if a form of digital divide exists at the XXXXXX Corporation. It is part of a broader study investigating whether risk homeostasis theory can be used to explain why social engineering experiments have the levels of success they do.

This is a research project being conducted by Wayne Kearney and North-West University as part of a PhD research study. You are invited to participate in this research project as an employee or contractor associated with the XXXXX Corporation.

Your participation in this research study is voluntary. You may choose not to participate. If you decide to participate in this research survey, you may withdraw at any time. If you decide not to participate in this study or if you withdraw from participating at any time, you will not be penalised.

The procedure involves a series of questions. Your responses will be confidential and we do not use identifying information such as your name or position. The XXXXX Corporation will also not be identified.

The survey questions will be about information security risks, threats and vulnerabilities and how they are controlled.

All raw data and your personal information will be kept confidential. The results of this study will be used for scholarly purposes.

If you have any questions about the research study, please contact Wayne Kearney or Prof Hennie Kruger.

Name:_____

Title or role:_____

Date:_____

Signature_____

Appendix E

Consent and ethical clearance from CEO

Details of the organisation are taken out for publication purposes. The original letter of consent and clearance is available from the researcher.

[redacted] [redacted]

[redacted]

Our Ref [redacted]

22 January 2015

Professor Hennie Kruger
School of Computer, Statistical and Mathematical Sciences
North-West University
Private Bag X6001, Potchefstroom
SOUTH AFRICA 2520

Dear Professor Kruger

I write to confirm that the "phishing" testing performed by the [redacted] in March 2012 and February 2014 were planned audit tests approved by myself.

Controlled phishing tests are an important part of our internal control defence mechanisms. Testing has been, and will be done, on an ongoing basis as part of user awareness training, and as part of a full penetration test to determine the level of risk and effectiveness of our controls. These tests are conducted by the [redacted] and managed by [redacted] Mr Kearney has permission to use the results for academic research purposes subject to normal commercial sensitivity and privacy protocols.

[redacted] systems are subject to monitoring and audit at any time. When a user logs onto the system they have to acknowledge acceptance of these conditions by clicking "OK". Access to this system is restricted to employees of, and persons, specifically authorised by the [redacted], and solely for use for lawful purposes and in accordance with the [redacted] policies and related standards.

Yours sincerely

[redacted]

CHIEF EXECUTIVE OFFICER [redacted]

Appendix F

Guidelines – The International Journal of Cyber-Security and Digital Forensics

In accordance with the rules of the North-West University, it is a requirement to include author guidelines for articles presented in a thesis. This appendix contains the author guidelines for the article presented in Chapter 3 (The International Journal of Cyber-Security and Digital Forensics).

The author guidelines was obtained from the following URL: http://sdiwc.net/ijcsdf/Author-Guidelines.php

Author Guidelines

The IJCSDF is published four (4) times a year and accepts three types of papers as follows:

1. **Research papers**: that are presenting and discussing the latest, and the most profound research results in the scope of IJCSDF. Papers should describe new contributions in the scope of IJCSDF and support claims of novelty with citations to the relevant literature. Maximum word limit of 8000!.
2. **Technical papers**: that are establishing meaningful forum between practitioners and researchers with useful solutions in various fields of digital security and forensics. It includes all kinds of practical applications, which covers principles, projects, missions, techniques, tools, methods, processes etc. Maximum word limit of 5000
3. **Review papers**: that are critically analyzing past and current research trends in the field. Maximum word limit of 12000!
4. **Book reviews**: providing critical review of a recently published book in the scope of IJCSDF. Maximum word limit of 1000!

Submitted papers should include at least 8 pages and we are highly recommending authors to give references to previously published papers in this journal. Referencing to previously published papers of our journal shows your interest as well as continues involvement in the field and as such would increase the chance of paper acceptance.

Initial Submission of manuscripts

1. **Format and Presentation**: The journal only accepts paper submissions as electronic versions of Word documents. Keep acronyms and abbreviations to a minimum and define those that do appear in the text. The Footnotes are not typically used; if you need to include them, use the endnote format. The authors are suggested to follow the journal **template format** in the initial submission.
2. **Figures, Tables, and Graphics**: Upon initial manuscript submission, figures, tables, and other graphics should be included as part of the Word document. All tables and figures must be mentioned in the text of a paper, and include a caption. All illustrations must be clear enough to be read when printed in black-and-white.
3. **References**: References should appear at the end of the article in the text, use square brackets and consecutive numbers: [1], [2-4], [3,4] for citations. References should be listed in the order they appear in the text. Use Times Roman 10 point font format. Samples are provided below:

    1. Hyvarinen, A., Oja, E.: Independent Component Analysis: Algorithms and Applications. Neural Networks 13, 411--430 (2000).

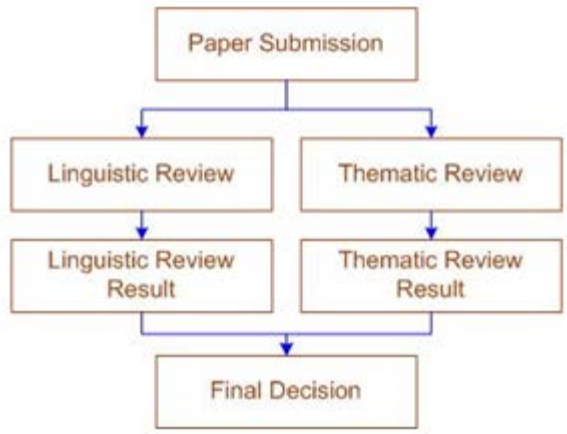
2. May, P., Ehrlich, H.C., Steinke, T.: ZIB Structure Prediction Pipeline: Composing a Complex Biological Workflow through Web Services. In: Nagel, W.E., Walter, W.V., Lehner, W. (eds.) Euro-Par 2006. LNCS, vol. 4128, pp. 1148--1158. Springer, Heidelberg (2006).
3. Volkov, V., Demmel, J.W.: Benchmarking GPUs to Tune Dense Linear Algebra. In: Proc. 2008 ACM/IEEE Conference on Supercomputing, pp. 1--11, IEEE Press, New York (2008).
4. Stone, J.V.: Independent Component Analysis: A Tutorial Introduction. MIT Press, Cambridge, MA (2004).
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

4. **Nominating preferred reviewers**: during initial submission, the authors are required to nominate at least two reviewers as preferred reviewers for the paper. We strongly recommend nominating reviewers from the list of authors whose papers are referenced at your submission. However, the journal keeps the right to give your papers for review to any other reviewer as well!
5. **Language and Writing**: All papers should be easy to read and understand with no writing or grammar error! The papers have to minimally meet requirements as "Doctorate/Postgraduate" educational level by automatic paper analyzers like: http://www.paperrater.com/free_paper_grader

Journal Review Process: All papers undergo an initial review by the journal's editor-in-chief. After a positive initial review, papers undergo a blind review process by two or more subject matter experts. Reviews are received by the editor-in-chief, who then provides the author with an editor's report that includes the final recommendation: a conditional acceptance, a request for further revisions, or rejection.

The linguistic consistency criterion addresses the level of written English and layout of the paper. A native speaker will check the papers submitted for linguistic consistency. The level of written English of submitted papers will be ranked between 1-5 where five (5) is for paper with excellent English and 1 is for paper whose English is subjected to major revision. Top three (3) levels will be considered for acceptance. The lower levels will be proposed for revision and could be conditionally accepted. Thematic review will decide whether to accept or reject according to the originality, significance for theory and practice, quality of content and presentation of submitted paper.

Linguistic Review	Technical Review	Decision
5 (excellent)	Accept Reject	Accept Reject
4 (good)	Accept Reject	Accept Reject
3 (normal)	Accept Reject	Accept Reject
2 (Need minor revision)	Accept Reject	Accept Reject
1 (Need major revision)	Accept Reject	Accept Reject



Papers satisfying both criteria will be considered for acceptance. Papers failing one of the two criteria will be recommended for revision and could be conditionally accepted. The feedback results would be emailed to authors no matter the paper is accepted or rejected.

Submission of Final Paper:

Prior to publication, all accepted papers should submit:

A camera-ready version which strictly follows the journal **template format**.

The author is also requested to complete a **copyright form.** The authors are requested to either apply requested reviewers comments or justify the reason that they ignore any comments of reviewers and **submit author-response form** as well.

Appendix G

Guidelines – Security and Privacy Protection in Information Processing Systems, SEC 2013, IFIP AICT (Springer)

In accordance with the rules of the North-West University, it is a requirement to include author guidelines for articles presented in a thesis. This appendix contains the author guidelines for the article presented in Chapter 4 (The IFIP SEC Conference).

The IFIP SEC conference is the flagship event of the International Federation for Information Processing (IFIP) Technical Committee 11 on Security and Privacy Protection in Information Processing Systems (TC-11, www.ifiptc11.org). Previous SEC conferences were held in Heraklion (Greece) 2012, Lucerne (Switzerland) 2011, and Brisbane (Australia) 2010. We seek submissions from academia, industry, and government presenting novel research on all theoretical and practical aspects of security and privacy protection in ICT Systems.

TOPICS OF INTEREST

- Access control and authentication
- Applied cryptography
- Audit and risk analysis
- Big data security and privacy
- Cloud security and privacy
- Critical infrastructure protection
- Cyber-physical systems security
- Data and applications security
- Digital forensics
- Human aspects of security and privacy
- Identity management
- Information security education
- Information security management
- Information technology mis-use and the law
- Managing information security functions
- Mobile security
- Multilateral security
- Network & distributed systems security
- Pervasive systems security
- Privacy protection and privacy enhancing technologies
- Surveillance and counter-surveillance
- Trust management

SUBMISSION GUIDELINES

Submitted papers must be original, unpublished, and not submitted to another conference or journal for consideration. Accepted papers will be presented at the conference and included in the conference proceedings published in the IFIP AICT series by Springer Science and Business Media.

All papers must be written in English. Submissions should be at most 14 pages long in total including references and appendices. PC members are not required to read the appendices, so the paper should be intelligible without them.

Authors must follow the Springer LNCS formatting instructions. Each paper will receive at least four reviews. At least one author of each accepted paper must register by the early date indicated on the conference website and present the paper.

Appendix H

Guidelines – 13th International Information Security South Africa Conference (ISSA)

In accordance with the rules of the North-West University, it is a requirement to include author guidelines for articles presented in a thesis. This appendix contains the author guidelines for the article presented in Chapter 5 (The 13th ISSA 2014 Conference).

The author guidelines was obtained from the following URL: http://infosecsa.co.za

Review Process

ISSA uses a double blind peer-review process to ensure the quality of submissions before acceptance. Authors initially submit abstracts to determine if the paper meets the goals and fits into the theme of the conference. The ISSA Program Committee assesses each submission for relevance and fit. Authors are then notified whether their abstracts were accepted, and if so, invited to submit a full paper for peer review.

On the due date, authors submit full papers. Each paper goes through an administrative review to confirm that the paper conforms to the specifications. If a paper does not meet the requirements, the author is asked to resubmit the paper.

A ***Review Committee*** is invited to participate, consisting of both local and international experts in the field of Information Security. A process is followed by the Program Committee to allocate papers to reviewers based on their area of expertise. Reviewers are subject matter experts, of which over 50% are international. Reviewers usually have 5 or 6 categories that they are willing to review against. Each reviewer will establish the number of papers they can review in a specific time period and are allowed to bid on the papers they want to review. An automated process allocated papers to each reviewer according to their preferences.

Each paper is reviewed by a minimum of two reviewers in a double blind review process. Papers are reviewed and rated on a 10 point system with 1 being poor and 10 being excellent as follows:

- Originallity (1-10)
- Significance (1-10)
- Technical quality (1-10)
- Relevance (1-10)
- Presentation (1-10)
- Overall Rating (1-10)

Reviewers' confidence in their own rating is also taken into account by the algorithm that calculates the final score. Reviewers are encouraged to make anonymous suggestions to the author(s) of the paper.

Based on the final score (1-10), a paper with 5 or below points can be recommended for a poster/research-in-progress session and a 9 to 10 point paper can be put in the "best paper" category. An acceptance rate of between 30% and 40% is expected for the conference.

Authors are notified of the outcome of the review process which includes the anonymous suggestions and recommendations of the reviewers. Authors then have to submit the final version of the paper that will then be included in the formal conference proceedings. The proceedings are published electronically on a CD with an ISBN number. All proceedings from all previous ISSA conferences are also available.

Authors are requested to submit original work, not previously published, on any topics mentioned below (or on any other security-related topic) *[topics are available on the abovementioned website]*. Abstracts should not be more than 350 words with full papers not exceeding 8 pages in the standard IEEE format Please choose any of the following templates, as acquired from the IEEE Web site at: **http://www.ieee.org/web/publications/pubservices/confpub/AuthorTools/conferenceTemplates.html**

Microsoft Word 2000	**LaTeX (PDF,64 KB)**	**LaTeX (Bibliography Files)**
A4 (DOC, 97 KB)	***Unix*** (TAR.GZ, 655 KB)	***Unix*** (TAR.GZ, 307 KB)
	Windows (ZIP, 674 KB)	***Windows*** (ZIP, 309 KB)

Appendix I

Guidelines – Computers & Security

In accordance with the rules of the North-West University, it is a requirement to include author guidelines for articles presented in a thesis. This appendix contains the author guidelines for the article presented in Chapter 6 (Computers & Security).

COMPUTERS & SECURITY

The International Source of Innovation for the Information Security and IT Audit Professional

AUTHOR INFORMATION PACK

TABLE OF CONTENTS

ISSN: 0167-4048

DESCRIPTION

The official journal of Technical Committee 11 (computer security) of the International Federation for Information Processing.

Computers & Security is the most respected technical journal in the IT security field. With its high-profile editorial board and informative regular features and columns, the journal is essential reading for IT security professionals around the world.*Computers & Security* provides you with a unique blend of leading edge research and sound practical management advice. It is aimed at the professional involved with **computer security**, **audit**, **control** and **data integrity** in all sectors - industry, commerce and academia. Recognized worldwide as THE primary source of reference for applied research and technical expertise it is your first step to fully secure systems.

Subscribe today and see the benefits immediately!

• Our cutting edge research will help you secure and maintain the integrity of your systems
• We accept only the highest quality of papers ensuring that you receive the relevant and practical advice you need
• Our editorial board's collective expertise will save you from paying thousands of pounds to IT consultants
• We don't just highlight the threats, we give you the solutions

Benefits to authors
We also provide many author benefits, such as free PDFs, a liberal copyright policy, special discounts on Elsevier publications and much more. Please click here for more information on our author services.

Please see our Guide for Authors for information on article submission. If you require any further information or help, please visit our support pages: http://support.elsevier.com

AUDIENCE

Organizational top and middle management, industrial security officers, computer specialists working in: systems design, implementation and evaluation; computer personnel selection, training and supervision; database development and management; operating systems design and maintenance; applications programming; telecommunications hardware and software development; computer

architecture design; computer security, attorneys, accountants and auditors, industrial and personnel psychologists.

IMPACT FACTOR

2014: 1.031 © Thomson Reuters Journal Citation Reports 2015

ABSTRACTING AND INDEXING

Current Contents/Engineering, Computing & Technology
Engineering Index
Science Citation Index
Scopus

EDITORIAL BOARD

GUIDE FOR AUTHORS

Your Paper Your Way

We now differentiate between the requirements for new and revised submissions. You may choose to submit your manuscript as a single Word or PDF file to be used in the refereeing process. Only when your paper is at the revision stage, will you be requested to put your paper in to a 'correct format' for acceptance and provide the items required for the publication of your article.
To find out more, please visit the Preparation section below.

INTRODUCTION

Computers & Security is the most comprehensive, authoritative survey of the key issues in computer security today. It aims to satisfy the needs of managers and experts involved in the computer security field by providing a combination of leading edge research developments, innovations and sound practical management advice for computer security professionals worldwide. Computers & Security provides detailed information to the professional involved with computer security, audit, control and data integrity in all sectors – industry, commerce and academia.

Submissions

Original submissions on all computer security topics are welcomed, especially those of practical benefit to the computer security practitioner.
From 1 April 2006, submissions with cryptology theory as their primary subject matter will no longer be accepted by Computers & Security as anything other than invited contributions. Authors submitting papers that feature cryptologic results as an important supporting feature should ensure that the paper, as a whole, is of importance to the advanced security practitioner or researcher, and ensure that the paper advances the overall field in a significant manner. Authors who submit purely theoretical papers on cryptology may be advised to resubmit them to a more appropriate journal; the Editorial Board reserves the right to reject such papers without the full reviewing process. Cryptography papers submitted before this date will be subject to the usual reviewing process, should the paper pass the pre-review process which has been in place since 2004.

All contributions should be in English and, since the readership of the journal is international, authors are reminded that simple, concise sentences are our preferred style. It is also suggested that papers are spellchecked and, if necessary, proofread by a native English speaker in order to avoid grammatical errors. All technical terms that may not be clear to the reader should be clearly explained.

Copyright is retained by the Publisher. Submission of an article implies that the paper has not been published previously; that it is not under consideration for publication elsewhere; that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out; and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.
All papers will be submitted to expert referees from the editorial board for review. The usual size of a paper is 5000 to 10 000 words.

BEFORE YOU BEGIN

Ethics in publishing

For information on Ethics in publishing and Ethical guidelines for journal publication see https://www.elsevier.com/publishingethics and https://www.elsevier.com/journal-authors/ethics.

Conflict of interest

All authors are requested to disclose any actual or potential conflict of interest including any financial, personal or other relationships with other people or organizations within three years of beginning the submitted work that could inappropriately influence, or be perceived to influence, their work. See also https://www.elsevier.com/conflictsofinterest. Further information and an example of a Conflict of Interest form can be found at: http://service.elsevier.com/app/answers/detail/a_id/286/supporthub/publishing.

Submission declaration and verification

Submission of an article implies that the work described has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see https://www.elsevier.com/sharingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the

responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. To verify originality, your article may be checked by the originality detection service CrossCheck https://www.elsevier.com/editors/plagdetect.

Contributors

Each author is required to declare his or her individual contribution to the article: all authors must have materially participated in the research and/or article preparation, so roles for all authors should be described. The statement that all authors have approved the final article should be true and included in the disclosure.

Changes to authorship

Authors are expected to consider carefully the list and order of authors **before** submitting their manuscript and provide the definitive list of authors at the time of the original submission. Any addition, deletion or rearrangement of author names in the authorship list should be made only **before** the manuscript has been accepted and only if approved by the journal Editor. To request such a change, the Editor must receive the following from the **corresponding author**: (a) the reason for the change in author list and (b) written confirmation (e-mail, letter) from all authors that they agree with the addition, removal or rearrangement. In the case of addition or removal of authors, this includes confirmation from the author being added or removed.
Only in exceptional circumstances will the Editor consider the addition, deletion or rearrangement of authors **after** the manuscript has been accepted. While the Editor considers the request, publication of the manuscript will be suspended. If the manuscript has already been published in an online issue, any requests approved by the Editor will result in a corrigendum.

Copyright

Upon acceptance of an article, authors will be asked to complete a 'Journal Publishing Agreement' (for more information on this and copyright, see https://www.elsevier.com/copyright). An e-mail will be sent to the corresponding author confirming receipt of the manuscript together with a 'Journal Publishing Agreement' form or a link to the online version of this agreement.

Subscribers may reproduce tables of contents or prepare lists of articles including abstracts for internal circulation within their institutions. Permission of the Publisher is required for resale or distribution outside the institution and for all other derivative works, including compilations and translations (please consult https://www.elsevier.com/permissions). If excerpts from other copyrighted works are included, the author(s) must obtain written permission from the copyright owners and credit the source(s) in the article. Elsevier has preprinted forms for use by authors in these cases: please consult https://www.elsevier.com/permissions.

For open access articles: Upon acceptance of an article, authors will be asked to complete an 'Exclusive License Agreement' (for more information see https://www.elsevier.com/OAauthoragreement). Permitted third party reuse of open access articles is determined by the author's choice of user license (see https://www.elsevier.com/openaccesslicenses).

Author rights

As an author you (or your employer or institution) have certain rights to reuse your work. For more information see https://www.elsevier.com/copyright.

Role of the funding source

You are requested to identify who provided financial support for the conduct of the research and/or preparation of the article and to briefly describe the role of the sponsor(s), if any, in study design; in the collection, analysis and interpretation of data; in the writing of the report; and in the decision to submit the article for publication. If the funding source(s) had no such involvement then this should be stated.

Funding body agreements and policies

Elsevier has established a number of agreements with funding bodies which allow authors to comply with their funder's open access policies. Some authors may also be reimbursed for associated publication fees. To learn more about existing agreements please visit https://www.elsevier.com/fundingbodies.

Open access

This journal offers authors a choice in publishing their research:

Open access
• Articles are freely available to both subscribers and the wider public with permitted reuse
• An open access publication fee is payable by authors or on their behalf e.g. by their research funder or institution
Subscription
• Articles are made available to subscribers as well as developing countries and patient groups through our universal access programs (https://www.elsevier.com/access).
• No open access publication fee payable by authors.

Regardless of how you choose to publish your article, the journal will apply the same peer review criteria and acceptance standards.

For open access articles, permitted third party (re)use is defined by the following Creative Commons user licenses:

Creative Commons Attribution (CC BY)
Lets others distribute and copy the article, create extracts, abstracts, and other revised versions, adaptations or derivative works of or from an article (such as a translation), include in a collective work (such as an anthology), text or data mine the article, even for commercial purposes, as long as they credit the author(s), do not represent the author as endorsing their adaptation of the article, and do not modify the article in such a way as to damage the author's honor or reputation.

Creative Commons Attribution-NonCommercial-NoDerivs (CC BY-NC-ND)
For non-commercial purposes, lets others distribute and copy the article, and to include in a collective work (such as an anthology), as long as they credit the author(s) and provided they do not alter or modify the article.

The open access publication fee for this journal is **USD 2400**, excluding taxes. Learn more about Elsevier's pricing policy: http://www.elsevier.com/openaccesspricing.

Green open access
Authors can share their research in a variety of different ways and Elsevier has a number of green open access options available. We recommend authors see our green open access page for further information (http://elsevier.com/greenopenaccess). Authors can also self-archive their manuscripts immediately and enable public access from their institution's repository after an embargo period. This is the version that has been accepted for publication and which typically includes author-incorporated changes suggested during submission, peer review and in editor-author communications. Embargo period: For subscription articles, an appropriate amount of time is needed for journals to deliver value to subscribing customers before an article becomes freely available to the public. This is the embargo period and it begins from the date the article is formally published online in its final and fully citable form.

This journal has an embargo period of 24 months.

Language (usage and editing services)
Please write your text in good English (American or British usage is accepted, but not a mixture of these). Authors who feel their English language manuscript may require editing to eliminate possible grammatical or spelling errors and to conform to correct scientific English may wish to use the English Language Editing service available from Elsevier's WebShop (http://webshop.elsevier.com/languageediting/) or visit our customer support site (http://support.elsevier.com) for more information.

Submission
Our online submission system guides you stepwise through the process of entering your article details and uploading your files. The system converts your article files to a single PDF file used in the peer-review process. Editable files (e.g., Word, LaTeX) are required to typeset your article for final publication. All correspondence, including notification of the Editor's decision and requests for revision, is sent by e-mail.

Referees
Please submit the names and institutional e-mail addresses of several potential referees. For more details, visit our Support site. Note that the editor retains the sole right to decide whether or not the suggested reviewers are used.

PREPARATION

NEW SUBMISSIONS

Submission to this journal proceeds totally online and you will be guided stepwise through the creation and uploading of your files. The system automatically converts your files to a single PDF file, which is used in the peer-review process.

As part of the Your Paper Your Way service, you may choose to submit your manuscript as a single file to be used in the refereeing process. This can be a PDF file or a Word document, in any format or lay-out that can be used by referees to evaluate your manuscript. It should contain high enough quality figures for refereeing. If you prefer to do so, you may still provide all or some of the source files at the initial submission. Please note that individual figure files larger than 10 MB must be uploaded separately.

References

There are no strict requirements on reference formatting at submission. References can be in any style or format as long as the style is consistent. Where applicable, author(s) name(s), journal title/book title, chapter title/article title, year of publication, volume number/book chapter and the pagination must be present. Use of DOI is highly encouraged. The reference style used by the journal will be applied to the accepted article by Elsevier at the proof stage. Note that missing data will be highlighted at proof stage for the author to correct.

Formatting requirements

There are no strict formatting requirements but all manuscripts must contain the essential elements needed to convey your manuscript, for example Abstract, Keywords, Introduction, Materials and Methods, Results, Conclusions, Artwork and Tables with Captions.

If your article includes any Videos and/or other Supplementary material, this should be included in your initial submission for peer review purposes.

Divide the article into clearly defined sections.

Figures and tables embedded in text

Please ensure the figures and the tables included in the single file are placed next to the relevant text in the manuscript, rather than at the bottom or the top of the file.

REVISED SUBMISSIONS

Use of word processing software

Regardless of the file format of the original submission, at revision you must provide us with an editable file of the entire article. Keep the layout of the text as simple as possible. Most formatting codes will be removed and replaced on processing the article. The electronic text should be prepared in a way very similar to that of conventional manuscripts (see also the Guide to Publishing with Elsevier: https://www.elsevier.com/guidepublication). See also the section on Electronic artwork.

To avoid unnecessary errors you are strongly advised to use the 'spell-check' and 'grammar-check' functions of your word processor.

Article structure

Subdivision - numbered sections

Divide your article into clearly defined and numbered sections. Subsections should be numbered 1.1 (then 1.1.1, 1.1.2, ...), 1.2, etc. (the abstract is not included in section numbering). Use this numbering also for internal cross-referencing: do not just refer to 'the text'. Any subsection may be given a brief heading. Each heading should appear on its own separate line.

Introduction

State the objectives of the work and provide an adequate background, avoiding a detailed literature survey or a summary of the results.

Material and methods

Provide sufficient detail to allow the work to be reproduced. Methods already published should be indicated by a reference: only relevant modifications should be described.

Theory/calculation

A Theory section should extend, not repeat, the background to the article already dealt with in the Introduction and lay the foundation for further work. In contrast, a Calculation section represents a practical development from a theoretical basis.

Results

Results should be clear and concise.

Discussion
This should explore the significance of the results of the work, not repeat them. A combined Results and Discussion section is often appropriate. Avoid extensive citations and discussion of published literature.

Conclusions
The main conclusions of the study may be presented in a short Conclusions section, which may stand alone or form a subsection of a Discussion or Results and Discussion section.

Appendices
If there is more than one appendix, they should be identified as A, B, etc. Formulae and equations in appendices should be given separate numbering: Eq. (A.1), Eq. (A.2), etc.; in a subsequent appendix, Eq. (B.1) and so on. Similarly for tables and figures: Table A.1; Fig. A.1, etc.

Vitae
For Full Length Articles a Biographical Sketch for each author (50-100 words) is required.

Essential title page information
• ***Title.*** Concise and informative. Titles are often used in information-retrieval systems. Avoid abbreviations and formulae where possible.
• ***Author names and affiliations.*** Please clearly indicate the given name(s) and family name(s) of each author and check that all names are accurately spelled. Present the authors' affiliation addresses (where the actual work was done) below the names. Indicate all affiliations with a lower-case superscript letter immediately after the author's name and in front of the appropriate address. Provide the full postal address of each affiliation, including the country name and, if available, the e-mail address of each author.
• ***Corresponding author.*** Clearly indicate who will handle correspondence at all stages of refereeing and publication, also post-publication. **Ensure that the e-mail address is given and that contact details are kept up to date by the corresponding author.**
• ***Present/permanent address.*** If an author has moved since the work described in the article was done, or was visiting at the time, a 'Present address' (or 'Permanent address') may be indicated as a footnote to that author's name. The address at which the author actually did the work must be retained as the main, affiliation address. Superscript Arabic numerals are used for such footnotes.

Abstract
A concise and factual abstract is required. The abstract should state briefly the purpose of the research, the principal results and major conclusions. An abstract is often presented separately from the article, so it must be able to stand alone. For this reason, References should be avoided, but if essential, then cite the author(s) and year(s). Also, non-standard or uncommon abbreviations should be avoided, but if essential they must be defined at their first mention in the abstract itself.

Graphical abstract
Although a graphical abstract is optional, its use is encouraged as it draws more attention to the online article. The graphical abstract should summarize the contents of the article in a concise, pictorial form designed to capture the attention of a wide readership. Graphical abstracts should be submitted as a separate file in the online submission system. Image size: Please provide an image with a minimum of 531 × 1328 pixels (h × w) or proportionally more. The image should be readable at a size of 5 × 13 cm using a regular screen resolution of 96 dpi. Preferred file types: TIFF, EPS, PDF or MS Office files. See https://www.elsevier.com/graphicalabstracts for examples.
Authors can make use of Elsevier's Illustration and Enhancement service to ensure the best presentation of their images and in accordance with all technical requirements: Illustration Service.

Highlights
Highlights are a short collection of bullet points that convey the core findings of the article. Highlights are optional and should be submitted in a separate editable file in the online submission system. Please use 'Highlights' in the file name and include 3 to 5 bullet points (maximum 85 characters, including spaces, per bullet point). See https://www.elsevier.com/highlights for examples.

Keywords
Immediately after the abstract, provide 5-10 keywords, avoiding general and plural terms and multiple concepts (avoid, for example, "and", "of"). Be sparing with abbreviations: only abbreviations firmly established in the field may be eligible. These keywords will be used for indexing purposes.

Abbreviations

Define abbreviations that are not standard in this field in a footnote to be placed on the first page of the article. Such abbreviations that are unavoidable in the abstract must be defined at their first mention there, as well as in the footnote. Ensure consistency of abbreviations throughout the article.

Acknowledgements

Collate acknowledgements in a separate section at the end of the article before the references and do not, therefore, include them on the title page, as a footnote to the title or otherwise. List here those individuals who provided help during the research (e.g., providing language help, writing assistance or proof reading the article, etc.).

Math formulae

Please submit math equations as editable text and not as images. Present simple formulae in line with normal text where possible and use the solidus (/) instead of a horizontal line for small fractional terms, e.g., X/Y. In principle, variables are to be presented in italics. Powers of e are often more conveniently denoted by exp. Number consecutively any equations that have to be displayed separately from the text (if referred to explicitly in the text).

Footnotes

Footnotes should be used sparingly. Number them consecutively throughout the article. Many word processors build footnotes into the text, and this feature may be used. Should this not be the case, indicate the position of footnotes in the text and present the footnotes themselves separately at the end of the article.

Artwork

Electronic artwork

General points

• Make sure you use uniform lettering and sizing of your original artwork.
• Preferred fonts: Arial (or Helvetica), Times New Roman (or Times), Symbol, Courier.
• Number the illustrations according to their sequence in the text.
• Use a logical naming convention for your artwork files.
• Indicate per figure if it is a single, 1.5 or 2-column fitting image.
• For Word submissions only, you may still provide figures and their captions, and tables within a single file at the revision stage.
• Please note that individual figure files larger than 10 MB must be provided in separate source files.

A detailed guide on electronic artwork is available on our website:
https://www.elsevier.com/artworkinstructions.
You are urged to visit this site; some excerpts from the detailed information are given here.

Formats

Regardless of the application used, when your electronic artwork is finalized, please 'save as' or convert the images to one of the following formats (note the resolution requirements for line drawings, halftones, and line/halftone combinations given below):
EPS (or PDF): Vector drawings. Embed the font or save the text as 'graphics'.
TIFF (or JPG): Color or grayscale photographs (halftones): always use a minimum of 300 dpi.
TIFF (or JPG): Bitmapped line drawings: use a minimum of 1000 dpi.
TIFF (or JPG): Combinations bitmapped line/half-tone (color or grayscale): a minimum of 500 dpi is required.

Please do not:

• Supply files that are optimized for screen use (e.g., GIF, BMP, PICT, WPG); the resolution is too low.
• Supply files that are too low in resolution.
• Submit graphics that are disproportionately large for the content.

Color artwork

Please make sure that artwork files are in an acceptable format (TIFF (or JPEG), EPS (or PDF), or MS Office files) and with the correct resolution. If, together with your accepted article, you submit usable color figures then Elsevier will ensure, at no additional charge, that these figures will appear in color online (e.g., ScienceDirect and other sites) regardless of whether or not these illustrations are reproduced in color in the printed version. **For color reproduction in print, you will receive information regarding the costs from Elsevier after receipt of your accepted article**. Please indicate your preference for color: in print or online only. For further information on the preparation of electronic artwork, please see https://www.elsevier.com/artworkinstructions.

Figure captions
Ensure that each illustration has a caption. A caption should comprise a brief title (**not** on the figure itself) and a description of the illustration. Keep text in the illustrations themselves to a minimum but explain all symbols and abbreviations used.

Tables

Please submit tables as editable text and not as images. Tables can be placed either next to the relevant text in the article, or on separate page(s) at the end. Number tables consecutively in accordance with their appearance in the text and place any table notes below the table body. Be sparing in the use of tables and ensure that the data presented in them do not duplicate results described elsewhere in the article. Please avoid using vertical rules.

References

Citation in text
Please ensure that every reference cited in the text is also present in the reference list (and vice versa). Any references cited in the abstract must be given in full. Unpublished results and personal communications are not recommended in the reference list, but may be mentioned in the text. If these references are included in the reference list they should follow the standard reference style of the journal and should include a substitution of the publication date with either 'Unpublished results' or 'Personal communication'. Citation of a reference as 'in press' implies that the item has been accepted for publication.

Reference links
Increased discoverability of research and high quality peer review are ensured by online links to the sources cited. In order to allow us to create links to abstracting and indexing services, such as Scopus, CrossRef and PubMed, please ensure that data provided in the references are correct. Please note that incorrect surnames, journal/book titles, publication year and pagination may prevent link creation. When copying references, please be careful as they may already contain errors. Use of the DOI is encouraged.

Web references
As a minimum, the full URL should be given and the date when the reference was last accessed. Any further information, if known (DOI, author names, dates, reference to a source publication, etc.), should also be given. Web references can be listed separately (e.g., after the reference list) under a different heading if desired, or can be included in the reference list.

References in a special issue
Please ensure that the words 'this issue' are added to any references in the list (and any citations in the text) to other articles in the same Special Issue.

Reference management software
Most Elsevier journals have their reference template available in many of the most popular reference management software products. These include all products that support Citation Style Language styles (http://citationstyles.org), such as Mendeley (http://www.mendeley.com/features/reference-manager) and Zotero (https://www.zotero.org/), as well as EndNote (http://endnote.com/downloads/styles). Using the word processor plug-ins from these products, authors only need to select the appropriate journal template when preparing their article, after which citations and bibliographies will be automatically formatted in the journal's style. If no template is yet available for this journal, please follow the format of the sample references and citations as shown in this Guide.

Users of Mendeley Desktop can easily install the reference style for this journal by clicking the following link:
http://open.mendeley.com/use-citation-style/computers-and-security
When preparing your manuscript, you will then be able to select this style using the Mendeley plug-ins for Microsoft Word or LibreOffice.

Reference formatting
There are no strict requirements on reference formatting at submission. References can be in any style or format as long as the style is consistent. Where applicable, author(s) name(s), journal title/book title, chapter title/article title, year of publication, volume number/book chapter and the pagination must be present. Use of DOI is highly encouraged. The reference style used by the journal will be

applied to the accepted article by Elsevier at the proof stage. Note that missing data will be highlighted at proof stage for the author to correct. If you do wish to format the references yourself they should be arranged according to the following examples:

Reference style
Text: All citations in the text should refer to:
1. *Single author:* the author's name (without initials, unless there is ambiguity) and the year of publication;
2. *Two authors:* both authors' names and the year of publication;
3. *Three or more authors:* first author's name followed by 'et al.' and the year of publication.
Citations may be made directly (or parenthetically). Groups of references should be listed first alphabetically, then chronologically.
Examples: 'as demonstrated in wheat (Allan, 2000a, 2000b, 1999; Allan and Jones, 1999). Kramer et al. (2010) have recently shown ....'
List: References should be arranged first alphabetically and then further sorted chronologically if necessary. More than one reference from the same author(s) in the same year must be identified by the letters 'a', 'b', 'c', etc., placed after the year of publication.
Examples:
Reference to a journal publication:
Van der Geer J, Hanraads JAJ, Lupton RA. The art of writing a scientific article. J Sci Commun 2010;163:51–9.
Reference to a book:
Strunk Jr W, White EB. The elements of style. 4th ed. New York: Longman; 2000.
Reference to a chapter in an edited book:
Mettam GR, Adams LB. How to prepare an electronic version of your article. In: Jones BS, Smith RZ, editors. Introduction to the electronic age. New York: E-Publishing Inc; 2009. p. 281–304.
Note shortened form for last page number. e.g., 51–9, and that for more than 6 authors the first 6 should be listed followed by "et al." For further details you are referred to "Uniform Requirements for Manuscripts submitted to Biomedical Journals" (J Am Med Assoc 1997;277:927–34) (see also http://www.nlm.nih.gov/bsd/uniform_requirements.html).
Reference to a website:
Cancer Research UK, Cancer statistics reports for the UK. http://www.cancerresearchuk.org/aboutcancer/statistics/cancerstatsreport/, 2003 (accessed 13.03.03).

Journal abbreviations source
Journal names should be abbreviated according to the List of Title Word Abbreviations: http://www.issn.org/services/online-services/access-to-the-ltwa/.

Video data

Elsevier accepts video material and animation sequences to support and enhance your scientific research. Authors who have video or animation files that they wish to submit with their article are strongly encouraged to include links to these within the body of the article. This can be done in the same way as a figure or table by referring to the video or animation content and noting in the body text where it should be placed. All submitted files should be properly labeled so that they directly relate to the video file's content. In order to ensure that your video or animation material is directly usable, please provide the files in one of our recommended file formats with a preferred maximum size of 150 MB. Video and animation files supplied will be published online in the electronic version of your article in Elsevier Web products, including ScienceDirect: http://www.sciencedirect.com. Please supply 'stills' with your files: you can choose any frame from the video or animation or make a separate image. These will be used instead of standard icons and will personalize the link to your video data. For more detailed instructions please visit our video instruction pages at https://www.elsevier.com/artworkinstructions. Note: since video and animation cannot be embedded in the print version of the journal, please provide text for both the electronic and the print version for the portions of the article that refer to this content.

AudioSlides

The journal encourages authors to create an AudioSlides presentation with their published article. AudioSlides are brief, webinar-style presentations that are shown next to the online article on ScienceDirect. This gives authors the opportunity to summarize their research in their own words and to help readers understand what the paper is about. More information and examples are available at https://www.elsevier.com/audioslides. Authors of this journal will automatically receive an invitation e-mail to create an AudioSlides presentation after acceptance of their paper.

Supplementary material

Supplementary material can support and enhance your scientific research. Supplementary files offer the author additional possibilities to publish supporting applications, high-resolution images, background datasets, sound clips and more. Please note that such items are published online exactly as they are submitted; there is no typesetting involved (supplementary data supplied as an Excel file or as a PowerPoint slide will appear as such online). Please submit the material together with the article and supply a concise and descriptive caption for each file. If you wish to make any changes to supplementary data during any stage of the process, then please make sure to provide an updated file, and do not annotate any corrections on a previous version. Please also make sure to switch off the 'Track Changes' option in any Microsoft Office files as these will appear in the published supplementary file(s). For more detailed instructions please visit our artwork instruction pages at https://www.elsevier.com/artworkinstructions.

Interactive plots

This journal enables you to show an Interactive Plot with your article by simply submitting a data file. For instructions please go to https://www.elsevier.com/interactiveplots.

Submission checklist

The following list will be useful during the final checking of an article prior to sending it to the journal for review. Please consult this Guide for Authors for further details of any item.

Ensure that the following items are present:

One author has been designated as the corresponding author with contact details:

• E-mail address
• Full postal address

All necessary files have been uploaded, and contain:

• Keywords
• All figure captions
• All tables (including title, description, footnotes)

Further considerations

• Manuscript has been 'spell-checked' and 'grammar-checked'
• All references mentioned in the Reference list are cited in the text, and vice versa
• Permission has been obtained for use of copyrighted material from other sources (including the Internet)

Printed version of figures (if applicable) in color or black-and-white

• Indicate clearly whether or not color or black-and-white in print is required.

For any further information please visit our customer support site at http://support.elsevier.com.

AFTER ACCEPTANCE

Use of the Digital Object Identifier

The Digital Object Identifier (DOI) may be used to cite and link to electronic documents. The DOI consists of a unique alpha-numeric character string which is assigned to a document by the publisher upon the initial electronic publication. The assigned DOI never changes. Therefore, it is an ideal medium for citing a document, particularly 'Articles in press' because they have not yet received their full bibliographic information. Example of a correctly given DOI (in URL format; here an article in the journal *Physics Letters B*):

http://dx.doi.org/10.1016/j.physletb.2010.09.059

When you use a DOI to create links to documents on the web, the DOIs are guaranteed never to change.

Online proof correction

Corresponding authors will receive an e-mail with a link to our online proofing system, allowing annotation and correction of proofs online. The environment is similar to MS Word: in addition to editing text, you can also comment on figures/tables and answer questions from the Copy Editor. Web-based proofing provides a faster and less error-prone process by allowing you to directly type your corrections, eliminating the potential introduction of errors.

If preferred, you can still choose to annotate and upload your edits on the PDF version. All instructions for proofing will be given in the e-mail we send to authors, including alternative methods to the online version and PDF.

We will do everything possible to get your article published quickly and accurately. Please use this proof only for checking the typesetting, editing, completeness and correctness of the text, tables and figures. Significant changes to the article as accepted for publication will only be considered at this

stage with permission from the Editor. It is important to ensure that all corrections are sent back to us in one communication. Please check carefully before replying, as inclusion of any subsequent corrections cannot be guaranteed. Proofreading is solely your responsibility.

Offprints

The corresponding author, at no cost, will be provided with a personalized link providing 50 days free access to the final published version of the article on ScienceDirect. This link can also be used for sharing via email and social networks. For an extra charge, paper offprints can be ordered via the offprint order form which is sent once the article is accepted for publication. Both corresponding and co-authors may order offprints at any time via Elsevier's WebShop (http://webshop.elsevier.com/myarticleservices/offprints). Authors requiring printed copies of multiple articles may use Elsevier WebShop's 'Create Your Own Book' service to collate multiple articles within a single cover (http://webshop.elsevier.com/myarticleservices/booklets).

AUTHOR INQUIRIES

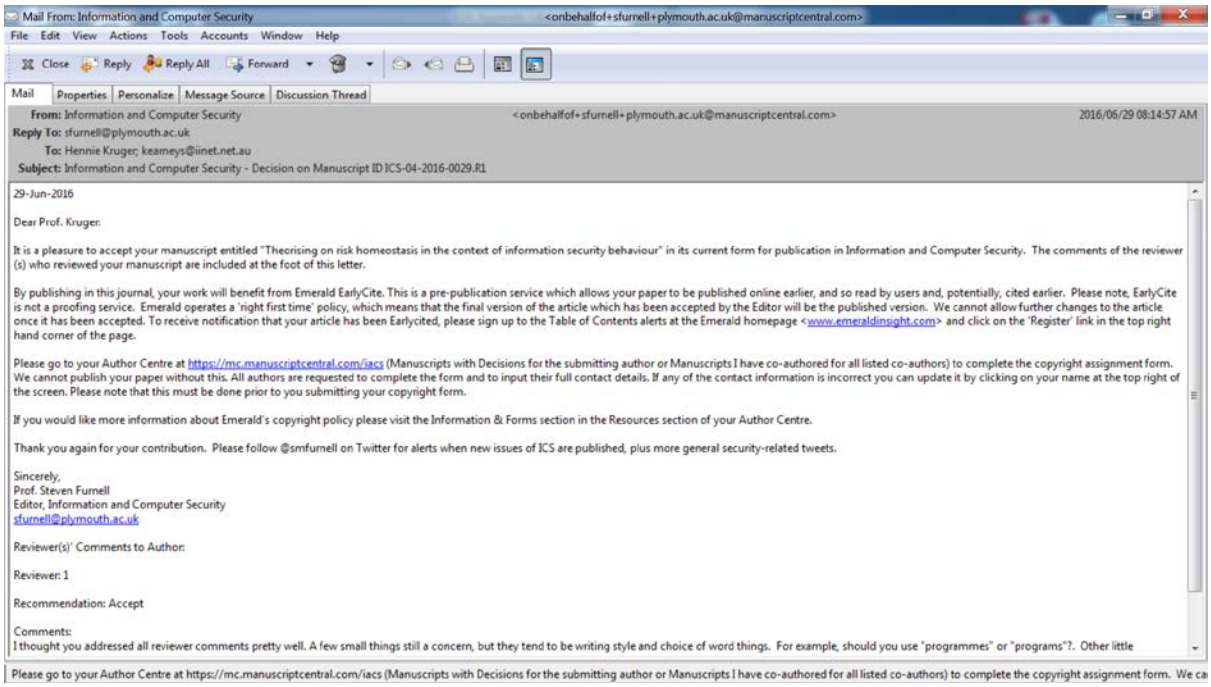
You can track your submitted article at https://www.elsevier.com/track-submission. You can track your accepted article at https://www.elsevier.com/trackarticle. You are also welcome to contact Customer Support via http://support.elsevier.com.

Appendix J

Guidelines – Information and Computer Security

In accordance with the rules of the North-West University, it is a requirement to include author guidelines for articles presented in a thesis. This appendix contains the author guidelines for the article presented in Chapter 7 (Information and Computer Security).

Proof of acceptance



Mail From: Information and Computer Security <onbehalfof+sfurnell+plymouth.ac.uk@manuscriptcentral.com>

File Edit View Actions Tools Accounts Window Help

Close Reply Reply All Forward

Mail Properties Personalize Message Source Discussion Thread

From: Information and Computer Security <onbehalfof+sfurnell+plymouth.ac.uk@manuscriptcentral.com> 2016/06/29 08:14:57 AM
Reply To: sfurnell@plymouth.ac.uk
To: Hennie Kruger; kearneys@iinet.net.au
Subject: Information and Computer Security - Decision on Manuscript ID ICS-04-2016-0029.R1

29-Jun-2016

Dear Prof. Kruger:

It is a pleasure to accept your manuscript entitled "Theorising on risk homeostasis in the context of information security behaviour" in its current form for publication in Information and Computer Security. The comments of the reviewer (s) who reviewed your manuscript are included at the foot of this letter.

By publishing in this journal, your work will benefit from Emerald EarlyCite. This is a pre-publication service which allows your paper to be published online earlier, and so read by users and, potentially, cited earlier. Please note, EarlyCite is not a proofing service. Emerald operates a 'right first time' policy, which means that the final version of the article which has been accepted by the Editor will be the published version. We cannot allow further changes to the article once it has been accepted. To receive notification that your article has been Earlycited, please sign up to the Table of Contents alerts at the Emerald homepage <www.emeraldinsight.com> and click on the 'Register' link in the top right hand corner of the page.

Please go to your Author Centre at https://mc.manuscriptcentral.com/iacs (Manuscripts with Decisions for the submitting author or Manuscripts I have co-authored for all listed co-authors) to complete the copyright assignment form. We cannot publish your paper without this. All authors are requested to complete the form and to input their full contact details. If any of the contact information is incorrect you can update it by clicking on your name at the top right of the screen. Please note that this must be done prior to you submitting your copyright form.

If you would like more information about Emerald's copyright policy please visit the Information & Forms section in the Resources section of your Author Centre.

Thank you again for your contribution. Please follow @smfurnell on Twitter for alerts when new issues of ICS are published, plus more general security-related tweets.

Sincerely,
Prof. Steven Furnell
Editor, Information and Computer Security
sfurnell@plymouth.ac.uk

Reviewer(s)' Comments to Author:

Reviewer: 1

Recommendation: Accept

Comments:
I thought you addressed all reviewer comments pretty well. A few small things still a concern, but they tend to be writing style and choice of word things. For example, should you use "programmes" or "programs"?. Other little

Please go to your Author Centre at https://mc.manuscriptcentral.com/iacs (Manuscripts with Decisions for the submitting author or Manuscripts I have co-authored for all listed co-authors) to complete the copyright assignment form. We ca

The author guidelines was obtained from the following URL:
http://emeraldgrouppublishing.com/products/journals/author_guidelines.htm?id=ics#2

Author Guidelines

Quick index

Manuscript requirements

Submit to the journal

Submissions to Information and Computer Security are made using ScholarOne Manuscripts, the online submission and peer review system. Registration and access is available at https://mc.manuscriptcentral.com/iacs. Full information and guidance on using ScholarOne Manuscripts is available at the Emerald ScholarOne Manuscripts Support Centre: http://msc.emeraldinsight.com.

Registering on ScholarOne Manuscripts

If you have not yet registered on ScholarOne Manuscripts, please follow the instructions below:

- Please log on to: https://mc.manuscriptcentral.com/iacs
- Click on Create Account
- Follow the on-screen instructions, filling in the requested details before proceeding
- Your username will be your email address and you have to input a password of at least 8 characters in length and containing two or more numbers
- Click Finish and your account has been created.

Submitting an article to Information and Computer Security on ScholarOne Manuscripts

- Please log on to Information and Computer Security at https://mc.manuscriptcentral.com/iacs with your username and password. This will take you through to the Welcome page (To consult the Author Guidelines for this journal, click on the Home Page link in the Resources column)
- Click on the Author Centre button
- Click on the submit a manuscript link which will take you through to the Manuscript Submission page
- Complete all fields and browse to upload your article
- When all required sections are completed, preview your .pdf proof
- Submit your manuscript

Review process

Each paper is reviewed by the editor and, if it is judged suitable for this publication, it is then sent to two referees for double blind peer review. Based on their recommendation, as well as consultation between relevant Editorial Board members the editor then decides whether the paper should be accepted as is, revised or rejected.

Copyright

Articles submitted to the journal should not have been published before in their current or substantially similar form, or be under consideration for publication with another journal. Please see Emerald's originality guidelines for details. Use this in conjunction with the points below about references, before submission i.e. always attribute clearly using either indented text or quote marks as well as making use of the preferred Harvard style of formatting. Authors submitting articles for publication warrant that the work is not an infringement of any existing copyright and will indemnify the publisher against any breach of such warranty. For ease of dissemination and to ensure proper policing of use, papers and contributions become the legal copyright of the publisher unless otherwise agreed.

The editor may make use of iThenticate software for checking the originality of submissions received. Please see our press release for further details.

Third party copyright permissions

Prior to article submission, authors should clear permission to use any content that has not been created by them. Failure to do so may lead to lengthy delays in publication. Emerald is unable to publish any article which has permissions pending. The rights Emerald requires are:

1. Non-exclusive rights to reproduce the material in the article or book chapter.
2. Print and electronic rights.
3. Worldwide English language rights.
4. To use the material for the life of the work (i.e. there should be no time restrictions on the re-use of material e.g. a one-year licence).

When reproducing tables, figures or excerpts (of more than 250 words) from another source, it is expected that:

1. Authors obtain the necessary **written** permission in advance from any third party owners of copyright for the use in print and electronic formats of any of their text, illustrations, graphics, or other material, in their manuscript. Permission must also be cleared for any minor adaptations of any work not created by them.
2. If an author adapts significantly any material, the author must inform the copyright holder of the original work.
3. Authors obtain any proof of consent statements
4. Authors must always acknowledge the source in figure captions and refer to the source in the reference list.
5. Authors should not assume that any content which is freely available on the web is free to use. Authors should check the website for details of the copyright holder to seek permission for re-use.

Emerald is a member of the STM Association and participates in the reciprocal free exchange of material with other STM members. This may mean that in some cases, authors do not need to clear permission for re-use of content. If so, please highlight this upon submission. For more information and additional help, please follow the Permissions for your Manuscript guide.

Committee on Publication Ethics (COPE)

Emerald supports the development of, and practical application of consistent ethical standards throughout the scholarly publishing community. All Emerald's journals and editors are members of the Committee on Publication Ethics (COPE) which provides advice on all aspects of publication ethics. Emerald follows the Committee's flowcharts in cases of research and publication misconduct, enabling journals to adhere to the highest ethical standards in publishing. For more information on Emerald's publication ethics policy, please click here.

Copyright forms

Where possible, Emerald seeks to obtain copyright for the material it publishes, without authors giving up their scholarly rights to reuse the work.

Assigning copyright to Emerald allows us to:

- Act on your behalf in instances such as copyright infringement or unauthorised copying
- Protect your moral rights in cases of plagiarism or unauthorised derivative works
- Offer a premium service for permission requests
- Invest in new platforms and services for the journals or book series you have published in
- Disseminate your work as widely as possible, ensuring your work receives the citations it deserves
- Recoup copyright fees from reproduction rights organisations to reinvest in new initiatives and author/user services, such as the Research Fund Awards and the Outstanding Doctoral Research Awards.

If an article is accepted for publication in an Emerald journal authors will be asked to submit a copyright form through ScholarOne. All authors are sent an email with links to their copyright forms which they must check for accuracy and submit electronically.

If authors can not assign copyright to Emerald, they should discuss this with the journal Content Editor. Each journal has an Editorial Team page which will list the Content Editor for that journal.

Emerald Editing Service

Emerald is pleased to partner with The Charlesworth Group in providing its Editing Service. The Charlesworth Group offers expert Language Editing services for non-native English-speaking authors, and is pleased to offer exclusive discounts to authors planning to submit to Emerald's journal(s).

Final submission

Authors should note that proofs are not supplied prior to publication. The manuscript will be considered to be the definitive version of the article. The author must ensure that it is complete, grammatically correct and without spelling or typographical errors. Before submitting, authors should check their submission completeness using the available Article Submission Checklist.

Open access submissions and information

Emerald currently offers two routes for Open Access in all journal publications, Green Open Access (Green OA) and Gold Open Access (Gold OA). Authors who are mandated to make the branded Publisher PDF (also known as the "Version of Record") freely available immediately upon publication can select the Gold OA route during the submission process. More information on all Open Access options can be found here.

Manuscript requirements

Please prepare your manuscript before submission, using the following guidelines:

Format	Article files should be provided in Microsoft Word format. LaTex files can be used if an accompanying PDF document is provided. PDF as a sole file type is not accepted, a PDF must be accompanied by the source file. Acceptable figure file types are listed further below.
Article Length	Articles should be a maximum of 7500 words in length.
Article Title	A title of not more than eight words should be provided.

Author details	All contributing authors' names should be added to the ScholarOne submission, and their names arranged in the correct order for publication. • Correct email addresses should be supplied for each author in their separate author accounts • The full name of each author must be present in their author account in the exact format they should appear for publication, including or excluding any middle names or initials as required • The affiliation of each contributing author should be correct in their individual author account. The affiliation listed should be where they were based at the time that the research for the paper was conducted
Biographies and acknowledgements	Authors who wish to include these items should save them together in an MS Word file to be uploaded with the submission. If they are to be included, a brief professional biography of not more than 100 words should be supplied for each named author.
Research funding	Authors must declare all sources of external research funding in their article and a statement to this effect should appear in the Acknowledgements section. Authors should describe the role of the funder or financial sponsor in the entire research process, from study design to submission.
Structured Abstract	Authors must supply a structured abstract in their submission, set out under 4-7 sub-headings (see our "How to... write an abstract" guide for practical help and guidance): • Purpose (mandatory) • Design/methodology/approach (mandatory) • Findings (mandatory) • Research limitations/implications (if applicable) • Practical implications (if applicable) • Social implications (if applicable) • Originality/value (mandatory) Maximum is 250 words in total (including keywords and article classification, see below). Authors should avoid the use of personal pronouns within the structured abstract and body of the paper (e.g. "this paper investigates..." is correct, "I investigate..." is incorrect).
Keywords	Authors should provide appropriate and short keywords in the ScholarOne submission that encapsulate the principal topics of the paper (see the How to... ensure your article is highly downloaded guide for practical help and guidance on choosing search-engine friendly keywords). The maximum number of keywords is 12. Whilst Emerald will endeavour to use submitted keywords in the published version, all keywords are subject to approval by Emerald's in house editorial team and may be replaced by a matching term to ensure consistency.
Article Classification	Authors must categorize their paper as part of the ScholarOne submission process. The category which most closely describes their paper should be selected from the list below. **Research paper.** This category covers papers which report on any type of research undertaken by the author(s). The research may involve the construction or testing of a model or framework, action research, testing of data, market research or surveys, empirical, scientific or clinical research. **Viewpoint.** Any paper, where content is dependent on the author's opinion and interpretation, should be included in this category; this also includes journalistic pieces. **Technical paper.** Describes and evaluates technical products, processes or services. **Conceptual paper.** These papers will not be based on research but will develop hypotheses. The papers are likely to be discursive and will cover philosophical discussions and comparative studies of others' work and thinking. **Case study.** Case studies describe actual interventions or experiences within organizations. They may well be subjective and will not generally report on research. A description of a legal case or a hypothetical case study used as a teaching exercise would also fit into this category. **Literature review.** It is expected that all types of paper cite any relevant literature so this category should only be used if the main purpose of the paper is to annotate and/or critique the literature in a particular subject area. It may be a selective bibliography providing advice on information sources or it may be comprehensive in that the paper's aim is to cover the main contributors to the development of a topic and explore their different views. **General review.** This category covers those papers which provide an overview or historical

	examination of some concept, technique or phenomenon. The 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 distinction between the hierarchy of headings. The preferred format is for first level headings to be presented in bold format and subsequent sub-headings to be presented in medium italics.
Notes/Endnotes	Notes or Endnotes should be used only if absolutely necessary and must be identified in the text by consecutive numbers, enclosed in square brackets and listed at the end of the article.
Figures	All Figures (charts, diagrams, line drawings, web pages/screenshots, and photographic images) should be submitted in electronic form. All Figures should be of high quality, legible and numbered consecutively with arabic numerals. Graphics may be supplied in colour to facilitate their appearance on the online database. • Figures created in MS Word, MS PowerPoint, MS Excel, Illustrator should be supplied in their native formats. Electronic figures created in other applications should be copied from the origination software and pasted into a blank MS Word document or saved and imported into an MS Word document or alternatively create a .pdf file from the origination software. • Figures which cannot be supplied as above are acceptable in the standard image formats which are: .pdf, .ai, and .eps. If you are unable to supply graphics in these formats then please ensure they are .tif, .jpeg, or .bmp at a resolution of at least 300dpi and at least 10cm wide. • To prepare web pages/screenshots simultaneously press the "Alt" and "Print screen" keys on the keyboard, open a blank Microsoft Word document and simultaneously press "Ctrl" and "V" to paste the image. (Capture all the contents/windows on the computer screen to paste into MS Word, by simultaneously pressing "Ctrl" and "Print screen".) • Photographic images should be submitted electronically and of high quality. They should be saved as .tif or .jpeg files at a resolution of at least 300dpi and at least 10cm wide. Digital camera settings should be set at the highest resolution/quality possible.
Tables	Tables should be typed and included in a separate file to the main body of the article. The position of each table should be clearly labelled in the body text of article with corresponding labels being clearly shown in the separate file. Ensure that any superscripts or asterisks are shown next to the relevant items and have corresponding explanations displayed as footnotes to the table, figure or plate.
References	References to other publications must be in **Harvard** style and carefully checked for completeness, accuracy and consistency. This is very important in an electronic environment because it enables your readers to exploit the Reference Linking facility on the database and link back to the works you have cited through CrossRef. You should cite publications in the text: (Adams, 2006) using the first named author's name or (Adams and Brown, 2006) citing both names of two, or (Adams *et al.*, 2006), when there are three or more authors. At the end of the paper a reference list in alphabetical order should be supplied:
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, *Title of Book*, Publisher, Place of publication, pages. e.g. Calabrese, F.A. (2005), "The early pathways: theory to practice – a continuum", in 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, number, pages. 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 Surname, Initials (Ed.), *Title of published proceeding which may include place and date(s) held*, Publisher, Place of publication, Page numbers. e.g. Jakkilinki, R., Georgievski, M. and Sharda, N. (2007), "Connecting destinations with an ontology-based e-tourism planner", in *Information and communication technologies in tourism 2007 proceedings of the international conference in Ljubljana, Slovenia, 2007*, Springer-Verlag, Vienna, pp. 12-32.

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 encyclopedia entries (with no author or editor)	*Title of Encyclopedia* (year) "Title of entry", volume, edition, Title of Encyclopedia, Publisher, Place of publication, pages. e.g. *Encyclopaedia Britannica* (1926) "Psychology of culture contact", Vol. 1, 13th ed., Encyclopaedia Britannica, London and New York, NY, pp. 765-71. (For authored entries please refer to book chapter guidelines above)
For newspaper articles (authored)	Surname, Initials (year), "Article title", *Newspaper*, date, pages. 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, pages. 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 a date that the resource was accessed. e.g. Castle, B. (2005), "Introduction to web services for remote portlets", available at: http://www-128.ibm.com/developerworks/library/ws-wsrp/ (accessed 12 November 2007). Standalone URLs, i.e. without an author or date, should be included either within 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).

- See more at: http://emeraldgrouppublishing.com/products/journals/author_guidelines.htm?id=ics#2