

# Determining a standard for information security culture

**F Nel**  
**21769028**

Dissertation submitted in partial fulfilment of the requirements for the degree *Magister Scientiae* in *Computer Science* at the Potchefstroom Campus of the North-West University

Supervisor: Dr L Drevin

May 2017

## **PREFACE**

There are some people who have to be thanked and acknowledged for their help in this study.

I would like to thank my parents, Hans and Sara Nel as well as my fiancée, Helene Joubert for all their support during the writing process.

This study would not have been possible without the patient and sensible leadership of Dr Lynette Drevin. She is and will always be a great teacher and study leader.

Dr Erika Fourie from statistical consultation services is the next person to thank. She did all the statistical analysis and provided regular advice regarding data analysis.

The last person to acknowledge is Prof Marthie Grobler who helped to make this document readable and did the language editing.

## ABSTRACT

Information is a valuable asset and many organisations cannot survive or function without it. Protecting the information becomes very important. Statistics show that a large percentage of organisations are threatened by security breaches, with most anticipating more frequent attacks. The importance of an information security solution in an organisation cannot be overstated. An organisation's success or failure in implementing information system security depends on the actions of its employees. To reduce the risk of security failures, organisations should focus more on employee behaviour. Cultivating an information security aware culture will decrease risk to information assets. it. The primary objective (aim) of this study is to investigate a measuring mechanism and acceptable standards for information security culture in order to improve organisational culture using appropriate methods in awareness and training programmes.

This study uses different studies presented in literature to identify a number of aspects, methods and topics:

- 21 information security culture aspects: policy, compliance, managerial trust/information security leadership, education and training, information security awareness, information asset management, information monitoring and audit, business continuity plan/incident management, information security programme, change management, communication, management's perspective, strategy, delegation of responsibility, risk analysis, ROI (Return on Investment), legal and regulatory, ethical conduct, accountability, fairness towards employees, fulfilment of personal needs of employee;
- five training and awareness delivery methods: formal training sessions, informal training, short messages around the office, employee sitting in front of computer, and other;
- 18 important topics that should be included in an awareness and training programme: the need of an anti-virus program, the need of updating virus definitions, regularly scan a computer and storage devices, use a personal firewall, install software patches, use pop-up blockers, the risk of downloading programs or files, risks of peer-to-peer (P2P) file sharing, the risk of clicking on e-mail links, the risk of e-mailing passwords, the risk of e-mail attachments, regularly backup important files, the risk of smartphone viruses, the need of anti-virus program for a smart phone, the characteristics of a strong password, use different passwords for different systems, change passwords regularly, and legal, regulatory and ethical issues of information security.

In an online questionnaire, respondents were asked to rate the importance of each of the information security culture aspects. This provided a minimum acceptable baseline for each

aspect – a level of each aspect that any organisation should have as minimum. The respondents were also asked to choose the best delivery method for each aspect, providing a list of preferred delivery methods for each of the culture aspects. Important topics were also discussed and respondents rated the importance of each, assessing which are the most important. Additional open-ended questions allowed them to include other security culture aspects, delivery methods and important topics not named in the questionnaire. Additional open-ended questions also allowed for comments and feedback.

The results from the questionnaire were used to create a framework that presents all the results in table format. It was also used to create a mobile application that an organisation can use to measure the strength of their information security culture and each individual security culture aspect. It provides advice on which delivery methods can be used for each security culture aspect, and gives information on the important topics.

Key terms: Awareness and training programme; Information security culture; Information security culture aspects

## OPSOMMING

Inligting is 'n waardevolle bate en baie organisasies kan nie daarsonder oorleef of funksioneer nie. Gevolglik is dit baie belangrik om die inligting te beskerm. Statistiek toon aan dat 'n groot persentasie van organisasies bedreig word deur sekuriteitverbrekings en die meeste verwag meer dikwels aanvalle. Die belangrikheid van 'n inligtingsekuriteitoplossing in 'n organisasie kan nie oorbeklemtoon word nie. Die sukses of mislukking van die implementering van 'n inligtingsekuriteitstelsel in 'n organisasie is afhanklik van die optrede van die werknemers. Om die risiko van sekuriteitsmislukkings te verminder, moet organisasies meer fokus op werknemersgedrag. Die kweek van 'n kultuur van inligtingsekuriteitsbewustheid sal die risiko vir inligtingsbates verminder. Die primere doel van hierdie studie is om 'n meting meganisme en aanvaarbare standaarde vir inligting-sekuriteit kultuur te ondersoek ten einde organisatoriese kultuur te verbeter deur gepaste metodes in bewustheid en opleidingsprogramme. Hierdie studie maak gebruik verskillende studies wat in die literatuur aangebied is om sekere aspekte, metodes en onderwerpe te identifiseer:

- 21 aspekte van inligtingsekuriteitskultuur: beleid, nakoming, bestuursvertroue/ inligtingsekuriteitsleierskap, opvoeding en opleiding, bewustheid van inligtingsekuriteit, bestuur van inligting as bate, monitering en audit van inligting, besigheids-kontinuïteitsplan/voorvalbestuur, inligtingsekuriteitsprogram, veranderingsbestuur, kommunikasie, bestuurdersperspektief, strategie, delegering van verantwoordelikheid, risiko-ontleding, ROI (opbrengs op belegging), regs- en regulatoriese aspekte, etiese gedrag, aanspreeklikheid, billikheid teenoor werknemers, vervulling van persoonlike behoeftes van werknemers;
- vyf opleiding en bewusmaking afleweringsmetodes: formele opleidingsessies, informele opleiding, kort boodskappe rondom die kantoor, werknemer wat voor 'n rekenaar sit, en ander);
- 18 belangrike onderwerpe wat ingesluit moet word in 'n bewustheid- en opleidings-program: die behoefte van 'n anti-virus program, die behoefte om virusdefinisies op te dateer, gereelde skandering van 'n rekenaar en bergingstoestelle, 'n persoonlike netskans, installering van sagteware opdaterings, gebruik van 'pop-up blockers', die risiko van die aflaai van programme of lêers, die risiko van peer-tot-peer (P2P) lêerdeel, die risiko om op skakels in e-pos te klik, die risiko om wagwoorde per e-pos te stuur, die risiko van e-posaanhegsels, gereelde rugsteun van belangrike datalêers, die risiko van slimfoonvirusse, die behoefte van 'n anti-virusprogram vir 'n slimfoon, die eienskappe van 'n sterk wagwoord, die gebruik van verskillende wagwoorde vir verskillende

stelsels, gereelde verandering van wagwoorde, en wetlike, regulatoriese en etiese kwessies van inligtingsekuriteit. In 'n aanlyn vraelys is die respondente gevra om die belangrikheid van elke aspek van die inligtingsekuriteitskultuur te evalueer. Dit het 'n minimum aanvaarbare basislyn vir elke aspek verskaf - 'n vlak van elke aspek wat enige organisasie as minimum moet hê. Die respondente is ook gevra om die beste aflewering metode vir elke aspek te kies, waar 'n lys van voorkeur-aflewering metodes vir elkeen van die kultuuraspekte verskaf was. Belangrike onderwerpe is ook bespreek en respondente het die belangrikheid van elkeen geëvalueer om te bepaal watter die belangrikste is. Bykomende oop vrae het respondente toegelaat om aspekte van sekuriteitskultuur, aflewering metodes en belangrike onderwerpe wat nie in die vraelys is nie, by te voeg. Addisionele oop vrae het hul ook in staat gestel om kommentaar en terugvoering te verskaf.

Die resultate van die vraelys is gebruik om 'n raamwerk te skep wat al die resultate in tabelvorm vertoon. Dit is ook gebruik om 'n mobiele toepassing te skryf wat 'n organisasie kan gebruik om die sterkte van hul inligtingsekuriteitskultuur te meet, sowel as elkeen van die individuele inligtingsekuriteitsaspekte te evalueer. Dit verskaf ook raad oor watter aflewering metodes gebruik kan word vir elke kultuuraspek en gee inligting oor die belangrikste onderwerpe in 'n bewusmakingsprogram vir inligtingsekuriteit.

Sleuteltermes: Aspekte van inligtingsekuriteitskultuur; inligtingsekuriteitskultuur; opleiding- en bewusmakingprogram

# TABLE OF CONTENTS

<b>PREFACE .....</b>	<b>I</b>
<b>ABSTRACT .....</b>	<b>II</b>
<b>OPSOMMING .....</b>	<b>IV</b>
<b>1            CHAPTER 1: INTRODUCTION AND BACKGROUND .....</b>	<b>1</b>
1.1           Problem Statement .....	2
1.2           Aims and Objectives .....	3
1.3           Research Methods.....	5
1.4           Chapter Division .....	6
1.5           Summary .....	6
<b>2            CHAPTER 2: LITERATURE REVIEW.....</b>	<b>7</b>
2.1           Part One: Organisational Culture .....	8
2.1.1        Introduction.....	8
2.1.2        Description of Organisational Culture .....	9
2.2           Part Two: Information Security.....	11
2.2.1        Introduction.....	11
2.2.2        Information Security Management .....	11
2.2.2.1      Top Management Support .....	12
2.2.2.2      Information Security Policy .....	12
2.2.2.3      Information Security Training.....	13
2.2.2.4      Information Security Awareness .....	14

2.2.2.5	Information Security Culture .....	15
2.2.2.6	Information Security Audit.....	15
2.2.2.7	Information Security Management Best Practices.....	16
2.2.2.8	Asset Management.....	17
2.2.2.9	Information Security Incident Management.....	18
2.2.2.10	Information Security Regulations Compliance .....	19
2.2.3	Conclusion of Information Security .....	19
<b>2.3</b>	<b>Part Three: Information Security Culture.....</b>	<b>20</b>
2.3.1	Important Aspects of Information Security Culture .....	22
2.3.1.1	First Framework.....	22
2.3.1.2	Second Framework .....	23
2.3.1.3	Third Framework .....	24
2.3.1.4	Fourth Framework .....	25
2.3.1.5	Fifth Framework.....	26
2.3.2	Assessing Information Security Culture .....	27
2.3.2.1	Sixth Framework.....	28
2.3.3	Identified Aspects .....	29
2.3.4	Conclusion of Information Security Culture .....	33
<b>2.4</b>	<b>Part Four: Information Security Awareness and Training Programmes.....</b>	<b>34</b>
2.4.1	Awareness and Training Topics.....	35
2.4.2	Delivery Methods.....	37
2.4.3	Conclusion of Awareness and Training.....	39



<b>2.5</b>	<b>Summary .....</b>	<b>39</b>
<b>3</b>	<b>CHAPTER 3: RESEARCH METHODOLOGY .....</b>	<b>40</b>
<b>3.1</b>	<b>Paradigms .....</b>	<b>41</b>
3.1.1	Positivistic Paradigm.....	41
3.1.2	Interpretive/Constructivist Paradigm .....	42
3.1.3	Critical Social Paradigm.....	43
3.1.4	Appropriate Paradigm.....	44
<b>3.2</b>	<b>Research Approach.....</b>	<b>44</b>
3.2.1	Quantitative Research .....	44
3.2.2	Qualitative Research .....	44
3.2.3	Mixed Methods .....	45
3.2.4	Approach Used in This Study .....	45
<b>3.3</b>	<b>Data Collection .....</b>	<b>45</b>
3.3.1	Survey design.....	45
3.3.2	Participants.....	50
<b>3.4</b>	<b>Data Analysis .....</b>	<b>51</b>
<b>3.5</b>	<b>Ethical Considerations.....</b>	<b>53</b>
<b>3.6</b>	<b>Data Analysis Process .....</b>	<b>53</b>
<b>3.7</b>	<b>Summary .....</b>	<b>53</b>
<b>4</b>	<b>CHAPTER 4: EMPIRICAL STUDY AND RESULTS.....</b>	<b>54</b>
<b>4.1</b>	<b>Questionnaire Results.....</b>	<b>54</b>

4.1.1	Demographical Details.....	55
4.1.2	Information Security Culture Aspects.....	59
4.1.3	Awareness and Training Delivery Methods.....	67
4.1.4	Important Topics of Information Security Awareness and Training Programmes.....	74
<b>4.2</b>	<b>Data Analysis .....</b>	<b>80</b>
4.2.1	Demographics Inferential Statistics.....	81
4.2.1.1	T-Test.....	81
4.2.1.2	Analysis of Variance (ANOVA) .....	86
4.2.2	Open-ended Questions.....	90
<b>4.3</b>	<b>Building the Framework.....</b>	<b>101</b>
<b>4.4</b>	<b>Summary .....</b>	<b>102</b>
<b>5</b>	<b>CHAPTER 5: FRAMEWORK AND MOBILE APPLICATION .....</b>	<b>103</b>
<b>5.1</b>	<b>Framework .....</b>	<b>103</b>
<b>5.2</b>	<b>Mobile Application.....</b>	<b>108</b>
5.2.1	Aim of the Mobile Application.....	108
5.2.2	Design and Technical Aspects.....	109
<b>5.3</b>	<b>Summary .....</b>	<b>113</b>
<b>6</b>	<b>CHAPTER 6: CONCLUSION AND RECOMMENDATIONS.....</b>	<b>114</b>
<b>6.1</b>	<b>Aims .....</b>	<b>114</b>
<b>6.2</b>	<b>Results .....</b>	<b>116</b>
<b>6.3</b>	<b>Contributions .....</b>	<b>117</b>

6.4	Limitations .....	118
6.5	Future Work .....	119
	BIBLIOGRAPHY .....	120
7	APPENDIX A: CERTIFICATE OF LANGUAGE EDITING.....	124
8	APPENDIX B: QUESTIONNAIRE .....	125

## LIST OF TABLES

Table 1.1: Research scope.....	4
Table 2.1: Information Security Culture Framework (Adapted from Da Veiga & Eloff, 2010)....	23
Table 2.2: Information System Security Culture Aspects .....	31
Table 4.1: Demographical Details - Part 1 .....	57
Table 4.2: Demographical Details - Part 2 .....	58
Table 4.3: Information Security Culture Aspects 1 to 5 .....	60
Table 4.4: Information Security Culture Aspects 6 to 10 .....	61
Table 4.5: Information Security Culture Aspects 11 to 16 .....	62
Table 4.6: Information Security Culture Aspects 17 to 21 .....	63
Table 4.7: Additional Information Security Culture Aspects .....	65
Table 4.8: Culture Aspects Rated According to Importance.....	66
Table 4.9: Delivery Methods Key .....	67
Table 4.10: Awareness and Training Delivery Methods for Aspects 1 to 5 .....	68
Table 4.11: Awareness and Training Delivery Methods for Aspects 6 to 10.....	69
Table 4.12: Awareness and Training Delivery Methods for Aspects 11 to 16.....	69
Table 4.13: Awareness and Training Delivery Methods for Aspects 16 to 21 .....	70
Table 4.14: Additional Awareness and Training Delivery Methods .....	72
Table 4.15: Total Responses Regarding Delivery Method .....	73
Table 4.16: Responses for Important Topics 1 to 6 .....	75
Table 4.17: Responses for Important Topics 7 to 12 .....	76
Table 4.18: Responses for Important Topics 13 to 18 .....	77

Table 4.19: Additional Important Awareness and Training Programme Topics .....	78
Table 4.20: Important Topics Rated According to Importance .....	80
Table 4.21: Effect sizes - Information Security Culture Aspects (Gender).....	82
Table 4.22: Effect sizes - Information Security Important Topics (Gender) .....	83
Table 4.23: Independent T-Test (Gender) .....	84
Table 4.24: T-Test for Significant Aspects and Topics (Location) .....	85
Table 4.25: Independent T-Test (Location).....	86
Table 4.26: Significant Results Using ANOVA (Level of Employment).....	87
Table 4.27: Trend Analysis (Level of Employment).....	88
Table 4.28: Significant Results Using ANOVA (Level of Education) .....	88
Table 4.29: Trend Analysis (Level of Education).....	89
Table 4.30: Significant Results Using ANOVA (Organisation Type).....	89
Table 4.31: Trend Analysis (Organisation Type).....	90
Table 4.32: Open-ended Question Results - Part 1 .....	92
Table 4.33: Open-ended Question Results - Part 2 .....	95
Table 4.34: Open-ended Question Results - Part 3 .....	97
Table 4.35: Open-ended Question Results - Part 4 .....	99
Table 4.36: Open-ended Questions - Respondent Mapping .....	100
Table 4.37: Framework Design and Structure .....	102
Table 5.1: Framework - Part 1 .....	104
Table 5.2: Framework - Part 2.....	105
Table 5.3: Framework - Part 3.....	106

Table 5.4: Framework - Part 4.....	107
Table 5.5: Framework - Part 5.....	108
Table 5.6: ISC Percentage Calculation.....	111

## LIST OF FIGURES

Figure 1.1: Introduction Chapter 1 .....	1
Figure 2.1: Introduction Chapter 2 .....	7
Figure 2.2: Organisational Culture .....	9
Figure 2.3: Levels of Organisational Culture .....	10
Figure 2.4: Possible Vulnerabilities of Assets .....	17
Figure 2.5: Various Definitions Combined into Information Security Culture Aspects.....	22
Figure 3.1: Introduction Chapter 3 .....	40
Figure 3.2: Key Terms, Aim and Consent Form in Questionnaire .....	46
Figure 3.3: Example of Questions Related to Demographical Details in Questionnaire .....	47
Figure 3.4: Example of Questions Related to Information Security Culture Aspects in Questionnaire.....	47
Figure 3.5: Example of Questions Related to Awareness and Training Delivery Methods in Questionnaire.....	48
Figure 3.6: Important Topics of Awareness and Training Programmes in Questionnaire .....	49
Figure 3.7: Final Page of Questionnaire .....	50
Figure 4.1: Introduction Chapter 4 .....	54
Figure 4.2: Respondents' Level of Education .....	56
Figure 4.3: Respondents' Type of Organisation.....	56
Figure 4.4: Number of Employees in Organisation According to Respondents .....	57
Figure 4.5: Respondent Confidence 1 .....	58
Figure 4.6: Respondent Confidence 2 .....	59
Figure 4.7: Managerial Trust/Information Security Leadership Responses .....	60

Figure 4.8: Information Monitoring and Audit Responses .....	62
Figure 4.9: Communication Responses.....	63
Figure 4.10: Accountability Responses.....	64
Figure 4.11: Delivery Methods for Managerial Trust/Information Security Leadership .....	68
Figure 4.12: Delivery Methods for Information Monitoring and Audit.....	69
Figure 4.13: Delivery Methods for Communication .....	70
Figure 4.14: Delivery Methods for Fulfilment of Personal Needs of Employee .....	71
Figure 4.15: Total Responses for Delivery Methods .....	74
Figure 4.16: Response for Important Topic 1.....	75
Figure 4.17: Response for Important Topic 11 .....	76
Figure 5.1: Introduction Chapter 5 .....	103
Figure 5.2: Application Home Page and Definitions Page.....	109
Figure 5.3: Application Important Topics and Culture Aspect Testing Page.....	110
Figure 5.4: Application Results Page.....	112
Figure 5.5: Application Delivery Methods Page .....	112
Figure 6.1: Introduction Chapter 6 .....	114



# 1 CHAPTER 1: INTRODUCTION AND BACKGROUND

Figure 1.1 indicates how this chapter is structured within the context of the larger document. The chapters are Introduction, Literature review, Research methodology, Empirical study and results, Framework and mobile application, and Conclusions and recommendations. This chapter provides a description of the problem, states the research aims and objectives, the research methods, and how the dissertation is structured.

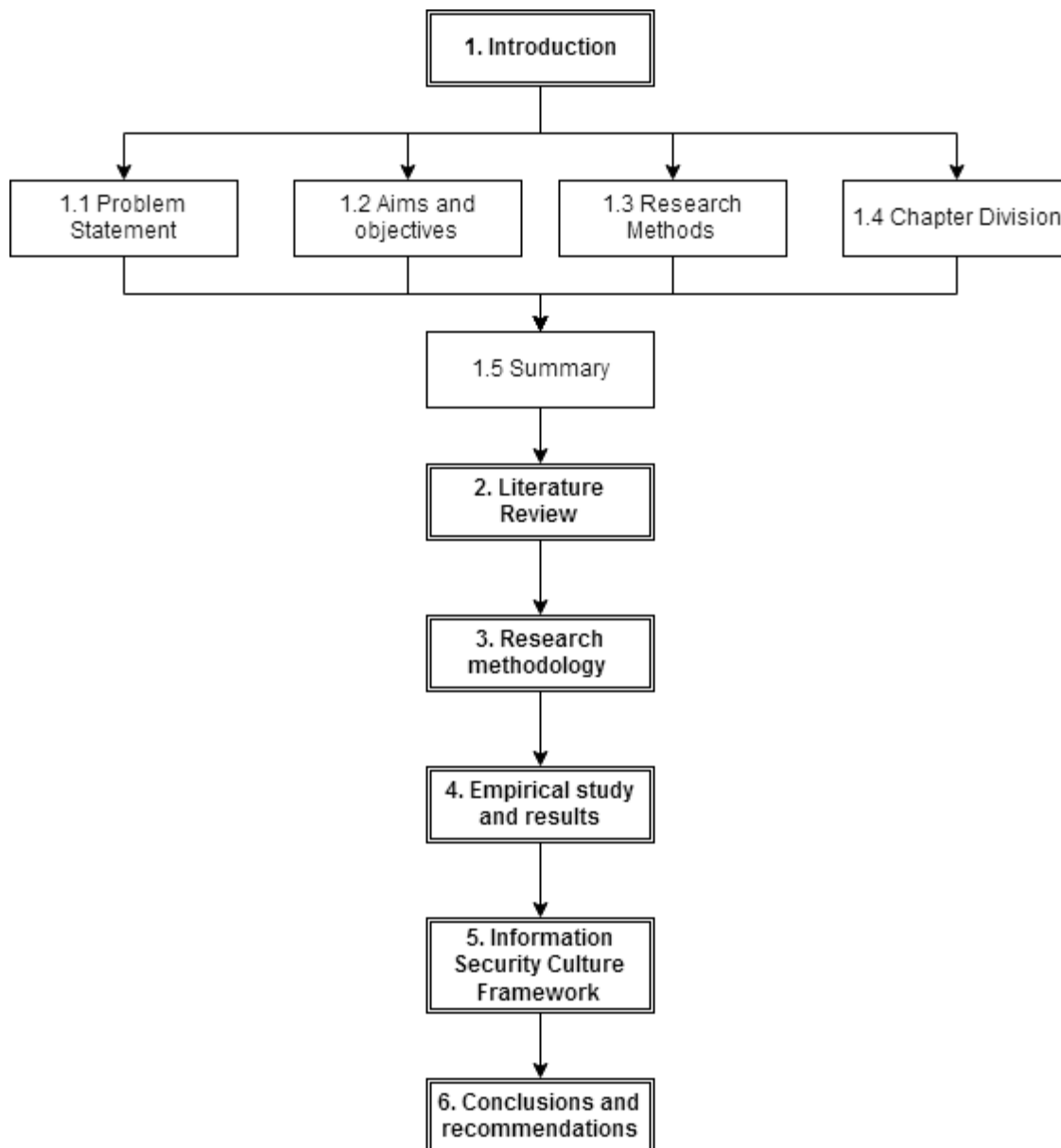


Figure 1.1: Introduction Chapter 1

## 1.1 Problem Statement

Information security has become an important part of everyday life. Every aspect of our business and private lives use information. Many organisations cannot survive without information and they need to be very serious about protecting their information assets (Van Niekerk & Von Solms, 2010). According to an information security breaches survey, at least 69% of large organisations were attacked by an unauthorised outsider in the year 2014 with most respondents anticipating attacks to happen more frequently (PricewaterhouseCoopers, 2015). It is fundamental that an information security solution should be an important component in any organisation (Thomson, von Solms & Louw, 2006).

Despite many technically sophisticated solutions, managing information security has remained a persistent challenge for organisations (Singh, Gupta & Ojha, 2014). To reduce the risk of security failures, organisations should focus more on employee behaviour since an organisation's success or failure in implementing information system security depends on the actions of its employees. Cultivating an information security aware culture will decrease the risk to information assets (Da Veiga & Eloff, 2010). The actions and behaviour of employees are one of the biggest difficulties with information management. Despite the application of assorted technical and physical controls, the human factor is often not addressed and is the most significant vulnerability. It is known that employees are regularly seen as the weakest link in information security (Bulgurcu, Cavusoglu & Benbasat, 2010). The human element has not been given enough attention and needs to be examined and improved (Metalidou, Marinagi, Trivellas, Eberhagen & Skourlas, 2014). In order to protect information assets, it is imperative that information security practices are taught to employees to apply into their everyday behaviour (Thomson et al., 2006). The study of behavioural information security is a relatively new field of research that targets the individual user in an organisation, since they are a major weakness in the security of information security assets (Crossler, Johnston, Lowry, Hu, Warkentin & Baskerville, 2013).

Regardless of being a potential problem, employees have the capacity to be a great advantage in reducing risk to information assets. The key to strengthening information security is to have employees comply with the security rules and regulations. Organisations should provide employees with awareness and training programmes to ensure that they are properly equipped to follow policy regulations regarding information security (Bulgurcu et al., 2010). Employees that are properly trained have the potential to be the strongest link in an organisation's infrastructure (Thomson et al., 2006). The protection of information should be second nature to employees and a natural part of their daily activities. This ensures that information security is integrated into the corporate culture. The security behaviour of employees should be moulded

as they are influenced by the corporate culture of the organisation (Thomson et al., 2006). Organisations should create fitting security awareness and training programmes to ensure employees' information security awareness (Bulgurcu et al., 2010). Creating a security aware culture within an organisation will improve information security.

An organisational culture that includes information security awareness will minimise risks to information assets and ensure that the risk of employee misbehaviour and harmful interaction with information assets is decreased (O'Brien, Islam, Bao, Weng, Xiong & Ma, 2013). Organisations already spend a large amount of money on on-going security training to their staff, yet these security failures persist. Despite many training and awareness programmes available, as well as guides for creating such programmes, there is no standard for what organisational security culture should look like.

The problem statement of this study is that there is no clear standard for information security culture and that this causes potential security risks. This study aims to improve on information security culture by investigating a possible standard for acceptable information security culture in organisations. The research question is: What is an acceptable information security culture baseline/standard in organisations and how can an organisation achieve that level/standard?

This study will attempt to answer the question by investigating aspects that can be used to measure organisational information security culture. These aspects will further be used to acquire a baseline for acceptable information security culture. Each aspect that forms part of an information security culture will have a standard and each of these will have associated awareness/training methods used to improve it.

In doing this research, the contribution is a standard with which organisations can compare their own level of information security culture. This will allow organisations to measure how they relate to the accepted baseline/standard for each identified aspect in order to learn where they have to improve to reach the baseline. This will also make organisations aware of the preferred delivery methods used for each aspect. The value of this research is in the data that can be used to improve information security within an organisation, as well as the data used to compare and improve an organisation's own information security culture.

## **1.2 Aims and Objectives**

The primary objective (aim) of this study is to investigate a measuring mechanism and acceptable standards for information security culture in order to improve organisational culture using appropriate methods in awareness and training programmes.

In order to reach the aim, the following secondary objectives have to be met:

- Investigate organisational culture and information security culture, as well as determine important aspects of information security culture;
- Use these aspects within different organisations to determine an acceptable baseline/standard;
- Identify delivery methods of training/awareness in literature and within organisations relating to information security culture;
- Investigate which training/awareness delivery methods can be used to improve each identified information security culture aspect in order to reach the identified standard/baseline;
- Identify important topics for an information security awareness and training programme in literature and in organisations;
- Use the results of the information security culture aspects, delivery methods, and important topics to create a framework for information security culture in organisations.

Table 1.1 shows the scope of the research and how the secondary objectives are linked to it.

<b>Scope of Research</b>
1. Define acceptable information security culture.
1.1 Identify important aspects.
1.1.1 Rate the importance of each aspect in organisations.
2. How to achieve it.
2.1 Identify delivery methods.
2.1.1 Investigate ideal delivery method for each identified important aspect.
2.2 Identify important topics.
2.2.1 Rate the importance of each topic in organisations.
3. Construction of the framework for information security culture in organisations

**Table 1.1: Research scope**

As shown in the above table, numbers 1, 2 and 3 describe the primary research objective of this study, with their sub-categories describing how they will be achieved.

#### Delineation

This research only includes important aspects of information security culture and delivery methods found in literature and as identified by respondents. There may be different views from other organizations. This study is conducted in a South-African context.

### 1.3 Research Methods

This study mainly uses a positivistic approach (data is derived from surveys); however, some interpretive work is also conducted in analysing qualitative data. Data acquisition is done using literature and by conducting an empirical study. By using literature, aspects of information security culture as well as awareness and training methods are identified. A questionnaire was created with the aim of learning what organisations see as the minimum acceptable baseline for each identified aspect, as well as what training methods they would prefer to use to improve the identified aspect. The questionnaire was distributed electronically to organisations using Google forms. See Chapter 3 section 3.2 for more details on the distribution of the questionnaire. The questionnaire was handled anonymously. The design of the questionnaire allows for qualitative and quantitative analysis using a Likert-scale and open-ended questions. Statistical analyses were done on the responses and open-ended questions are analysed interpretatively to create a final framework. This framework describes an acceptable baseline/standard of information security culture that can be achieved by training and educating people regarding information security issues. The framework also recommends methods for achieving this baseline. The design and create approach was used to develop a mobile application to apply the findings of the study in a practical way. Table 1.2 describes how each objective was met and methods used:

Scope of Research	Method used
1. Define acceptable information security culture.	Literature review
1.1 Identify important aspects.	Literature review
1.1.1 Rate the importance of each aspect in organisations.	Questionnaire
2. How to achieve it.	Literature review and questionnaire
2.1 Identify delivery methods.	Literature review
2.1.1 Investigate ideal delivery method for each identified important aspect.	Literature review and questionnaire
2.2 Identify important topics.	Literature review
2.2.1 Rate the importance of each topic in organisations.	Questionnaire
3. Construction of the framework for information security culture in organisations	Create; using literature and the survey results

**Table 1.2: Research scope and methods used**

How the scope was achieved is described in chapter 6 section 1.

## **1.4 Chapter Division**

This study is divided into the following chapters:

Chapter 1: Introduction – This chapter provides the problem statement and research rationale describing what research will be done and why it is important to conduct this research.

Chapter 2: Literature review – This chapter describes current literature relevant to this study. Topics include organisational culture, information security, information security culture, awareness and training methods.

Chapter 3: Research method – This chapter presents an overall description of the empirical study and a description of how it has been undertaken. Important topics include the research paradigm, data sources, participants and an ethical review, data collection methods, data analysis method(s) and ethical considerations.

Chapter 4: Empirical study and results – This chapter presents the discussion and interpretation of results from data collection and analysis.

Chapter 5: Framework and mobile application – This chapter presents a framework for achieving identified levels of information security culture by using awareness and training methods. Results from the study will be structured into a useable framework.

Chapter 6: Conclusions and recommendations – This chapter presents final recommendations based on the entire study describing how objectives have been met and possible future research possibilities.

## **1.5 Summary**

This chapter described the purpose of the research, why it is valuable and what the aims and objectives are. It provides a brief introduction to the rest of the study.

The next chapter is the literature review, which provides background information on the topics of information security and organisational culture. The next chapter also looks into information security culture aspects and security and awareness training delivery elements.

## 2 CHAPTER 2: LITERATURE REVIEW

This chapter is divided into four subsections as seen in Figure 2.1. The first subsection is a descriptive introduction of organisational culture and is mainly for background purposes. The second subsection gives more detail and describes information security. The third subsection brings these two domains together into information security culture and is the main part of this study. The fourth subsection describes awareness and training aspects within information security.

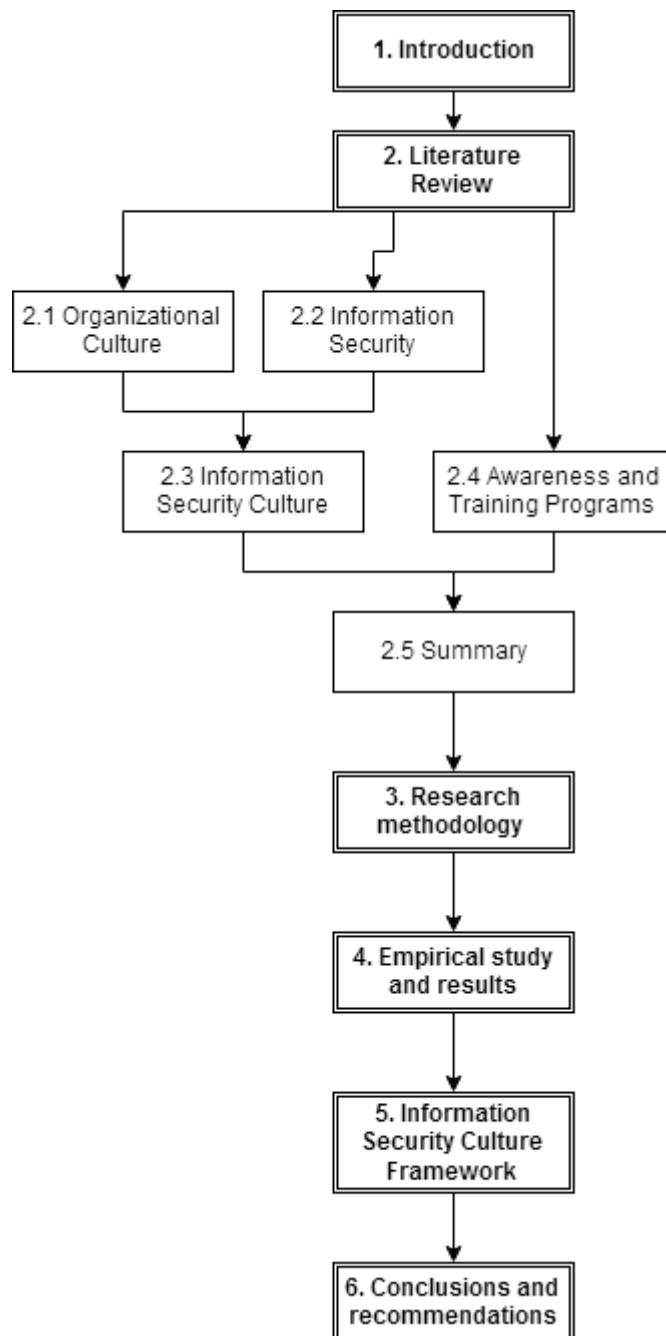


Figure 2.1: Introduction Chapter 2

The purpose of this chapter is to create a list of information security culture aspects. These aspects must be measurable and specific. A similar list of awareness and training methods is presented in Part 4. These two lists will be used to design the questionnaire. This chapter concludes with a summary.

## **2.1 Part One: Organisational Culture**

This section of the literature describes organisational culture and describes the characteristics and different types of organisational culture.

### **2.1.1 Introduction**

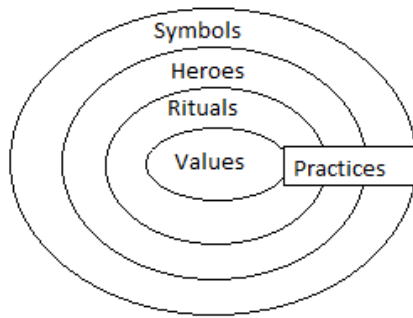
Organisational culture can be described as the “feel” of the organisation to its members that directs and motivates employee efforts. It is what the employees believe and their perception on what is valued by their organisation (Schneider, Brief & Guzzo, 1996).

This section provides a descriptive definition and brief overview of organisational culture, with the purpose of giving background to later topics. According to Da Veiga and Eloff (2010), organisational culture is the social glue that binds the members of an organisation together and can be perceived as the individual personality of the organisation. Organisational culture comprises four characteristics (Pfleeger, Pfleeger & Margulies, 2015):

- Symbols – words, gestures, pictures and objects that carry specific meaning to the people in an organisation, for example specific jargon.
- Heroes – individuals who can be regarded as role models and whose behaviour is highly prized; they are often recipients of awards or are speakers at events.
- Rituals – activities that are not crucial to the business, but that are performed by the entire group’s members; team building exercises are an example of rituals in an organisation’s culture.
- Values – the core of an organisation’s culture and the predisposition to favour certain states of affairs over others.

Figure 2.2 depicts the four characteristics of organisational culture where all of them influence the practices in an organisation.



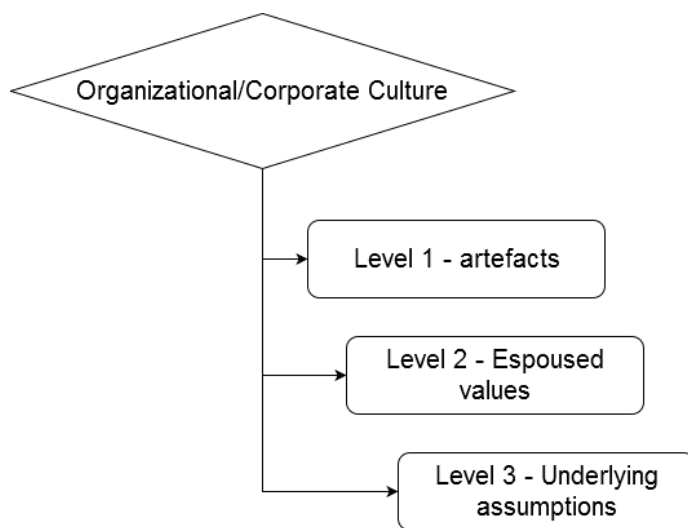


**Figure 2.2: Organisational Culture (Adopted from Pfleeger et al. 2015)**

### **2.1.2 Description of Organisational Culture**

It is noted that a stranger that enters a business might realise that the employees in the organisation seem to act and think alike, but act and think differently from people in other similar organisations. Each organisation has its own 'personality' that remains constant over time even if employees come and go. According to Burns and Stalker (cited by Van Den Steen, 2003), the concept of corporate culture dates back to at least 1961. They defined it as 'a dependable constant system of shared beliefs.' Large organisations even have subcultures shared by specific subgroups (Van Den Steen, 2003).

Schein (1999) defines three levels of culture, each having a direct influence on the level above/below it. Level one is artefacts: visible organisational structures and processes. These can be hard to decipher as it is what is observed, seen, heard and felt in an organisation. Level two is espoused values: strategies, goals and philosophies. It is the reason an employee would give to explain an artefact. Level three is underlying assumptions: unconscious, taken for granted beliefs, thoughts and feelings. It is the ultimate source of values and actions. These three together make up an organisation's culture (Schein, 1999) and is depicted in Figure 2.3.



**Figure 2.3: Levels of Organisational Culture**

Four types of organisational culture are defined: the autocratic power culture, the bureaucratic role culture, the anarchic individualistic culture and the matrix task-based culture (Da Veiga & Eloff, 2010).

Sponsorship for information security culture in autocratic organisations is crucial to ensure employee participation in security changes and comply with policies. Leaders are vital in implementing security procedures and changes (Da Veiga & Eloff, 2010). Every organisation has its own culture and might require its own approaches. It cannot always be measured or perceived but every organisation has its own culture.

Typically, employees are expected to have a job description and conform to the rules of the organisation in a bureaucratic culture. In information security, roles will be formally defined and security procedures will be documented and followed by employees. Characteristic examples are public sector organisations and banks.

In individualistic organisations, individuals have to be involved in order to acquire their commitment when information system security controls are implemented. This type of culture is mostly found in professional organisations like a lawyer's practice.

A task-based culture tends to obtain user buy-in and motivate users to comply with the security policy. They see planning, control and team responsibilities as crucial and usually include manufacturing companies. Projects are implemented using well-established project management disciplines.

The next section presents the topic of information security with a detailed description of aspects of managing information security.

## **2.2 Part Two: Information Security**

This part defines information security and provides a deep insight into the many aspects of information security management.

### **2.2.1 Introduction**

According to the United States' legal code (Title 44 › Chapter 35 › Subchapter III), the term information security is defined as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction...”. It addresses three important characteristics of a computer system. These three are (Pfleeger et al., 2015):

- Confidentiality – Information assets are accessible (not only readable, but also writable, viewable or just knowing that the information exists) only to those who are authorised to do so. Confidentiality is frequently called privacy or secrecy.
- Integrity – Information assets can only be changed, deleted, modified or created by authorised parties.
- Availability – Authorised parties must be able to access information assets at appropriate times.

An effective countermeasure to information security threats is to apply a range of both technical and non-technical controls. These controls should include good technical infrastructure, dependable internal processes and proper corporate governance (Da Veiga & Eloff, 2010).

The fast pace in which computers and information technology are advancing initiates new risk of possible security threats to information assets. This creates a great need in organisations to enhance their information security capabilities in order to respond to new challenges and risks. Organisations that fail to adapt to these needs are in danger of not surviving in a highly competitive environment (AlHogail, 2015).

The next section describes information security management (ISM) and the different building blocks that an information security system consists of. It does not focus on the technical aspects, but rather on the human related aspects as this study focuses on security culture.

### **2.2.2 Information Security Management**

To implement a security project, communication, coordination, time and a great deal of effort is required. Employees are often not positive about change and can consciously or unconsciously resist change. It is ideal to develop an organisational culture that supports change (Whitman & Mattord, 2016). Singh et al. (2014) identified 10 fields that represent all ISM activities. These activities are discussed next.

### **2.2.2.1 Top Management Support**

Top management plays a guiding part during the planning, design, development, deployment and post-deployment of an information security system. They also have to encourage positive user attitude towards the ISM in the organisation. Key issues that the top management are responsible for include:

- Information security policy compliance.
- Perception of management vs. security specialists and employees.
- Security culture and risk management.
- ISM as a corporate government responsibility.
- Information system security effectiveness.
- Resource provision to information security efforts.
- Set up of an information security infrastructure.

Important factors to ensure proper top management support are: “senior executives understand the significance of information security; senior executives attend information security related meetings; senior executives are involved in information security related decisions; and senior executives allocate budget and manpower for information security functions” (Singh et al., 2014). Ensuring employees comply with the security policy is influenced by: benefit of compliance (inherent benefits, safety and rewards), cost of noncompliance (inherent cost, vulnerability and sanctions), and cost of compliance (work impediment) that together form an overall attitude towards information security policy compliance (Bulgurcu et al., 2010). It is seen that managerial support is crucial in security planning.

The next section presents information security policy.

### **2.2.2.2 Information Security Policy**

A security policy is a document that states in writing how an organisation plans to protect its physical and information technology assets. It provides direction and support for all security aspects. The policy usually includes general statements of goals, objectives, beliefs, ethics and responsibilities and frequently describes the procedures to achieve them (Saint-Germain, 2005). Key issues of an information security policy include:

- Policy framework.
- Policy elements, characteristics and coverage.
- Formulation, implementation and adoption.
- Information security incident reporting.

- Aligning information security policy with strategic information system plan.
- Employees' behaviour toward policy compliance.
- Role of awareness in policy compliance.
- Policy communication.
- Policy effectiveness.
- Policy violations.

Important factors in an information security policy are: "The organisation has a documented information security policy; the information security policy clearly defines information security objectives of the organisation; the information security policy clearly defines roles and responsibilities of employees; the information security policy clearly defines roles and responsibilities of contractors/third party vendors; the information security policy is reviewed regularly (or when the environment changes); and procedures for implementing information security policy are clearly defined and documented" (Singh et al., 2014). This section indicates the importance of an information security policy, its contents and key issues.

The next section presents information security training.

### **2.2.2.3 Information Security Training**

The process of information security training aims at building knowledge in employees in order to produce relevant and needed skills and competencies in practitioners of fields other than information system security. Employees in all disciplines should be competent with information security. Training can take a while (longer than awareness) and requires learners to take an active role in the process. The longer time period ensures that employees are thoroughly trained and able to handle any security situation. It is expected that employees should be able to solve previously unmet problems after they have followed a well-designed training course. Individuals who specialise in information system security need more than just training. They require education in information system security. It is a longer and more thorough process that integrates all security skills and competencies of various security specialties into a common body of knowledge (Katsikas, 2000). Key elements of information security training include:

- Training needs of personnel.
- Training vs. awareness vs. education.
- Information security training tool.
- Usefulness of training programmes.
- E-learning training module.
- Information security policy compliance.

Important factors for information security training for employees are: The organisation conducts regular information security training for employees; information security training programmes offered by the organisation are useful; and that there is an information security advisor to coordinate information security functions in the organisation (Singh et al., 2014).

The next section introduces information security awareness.

#### **2.2.2.4 Information Security Awareness**

Awareness should not be seen as informal training. It attracts the attention of employees to the subject of security and teaches basic countermeasures. The main purpose of information security awareness is to allow employees to recognise the concern for information security and teach them to respond accordingly. Awareness teaches short-term, immediate and specific knowledge that have to be repeated regularly to ensure constant vigilance (Katsikas, 2000). In short, it is a blended solution of activities that encourages security, ensures responsibility and keeps employees updated on applicable security news.

Key elements of information culture awareness are:

- Requirements, challenges and potential.
- All personnel get the message.
- Dynamic and on-going process.
- Knowledge and attitude of employees.
- Gap between talk and action.
- Information security behaviour.
- Information security policy compliance.

Important factors for information security awareness are: “employees are aware of information security policy and guidelines of the organisation; the organisation conducts programs to make employees aware of the importance of information security; employees’ roles and responsibilities for information security are properly communicated; employees are aware that information security incidents must be reported to management immediately; employees are well informed about acceptable and unacceptable usage of information systems and assets; and employees are aware of the punishments/disciplinary actions for violating information security guidelines” (Singh et al., 2014).

This section indicates the focus of information security awareness while the previous section was on the training and highlighted that employees’ skills need to be developed in this area.

### **2.2.2.5 Information Security Culture**

This topic is the main focus of this study. Information security culture is the guiding factor for how things are done in an organisation concerning information security. Its aim is to protect the information assets by influencing employees' security behaviour (AlHogail & Mirza, 2014). A healthy information security culture exists when all employees are aware of their role and any potential risks and preventative measures, understand the results of non-compliance, and take steps to improve the information security within the organisation.

Information security culture is described in more detail in Section 2.3 and 4.1.2. Key elements of information security culture include:

- Employees' information security behaviour.
- Attitudes, assumptions, beliefs, values and knowledge of employees and stakeholders.
- Organisational information security culture dimensions.
- Information security policy compliance.
- Organisational culture.

Important factors in an information security culture include: "The organisation creates an information security focus among all employees; the organisation makes sure that information security is the first thing on the mind of all employees; the organisation makes information security the norm for all employees; the organisation dedicates efforts to create an information security focused workforce; the organisation makes sure that all employees are vigilant toward information security; and the organisation has an information security forum to give management direction and support" (Singh et al., 2014).

The next aspect of a security system (of ISM) is information security audit which is described in the following section.

### **2.2.2.6 Information Security Audit**

Information security audit is conducted when an independent individual/organisation examines and tests the security of an organisation's information systems. It assesses the quality of system controls; tests employee compliance with security protocols and recommends changes to improve the overall information security. In many cases, it is necessary to have a yearly audit and get certified according to certain standards (Saint-Germain, 2005). Key elements that should be included in an information security audit are:

- The human factor.
- Information systems risk planning.

- Internal audits.
- External (third party) audits.
- Monitor compliance to rules and guidelines.

Important factors for an information security audit are: the organisation has a team/committee for conducting information security; the organisation routinely conducts internal information security audits; and the organisation conducts external (third party) information security audits (Singh et al., 2014). Apart from audits, it is also necessary to have best practices in place. This is described in the following section.

#### **2.2.2.7 Information Security Management Best Practices**

Best practices are guidelines with the aim of helping an organisation to assess possible security risks, implement the appropriate security controls and countermeasures, and comply with organisational regulations and legal requirements. Best practices are often based on standards, for example, the ISO/IEC 17799 that is highly flexible and can be adapted to various organisations (Saint-Germain, 2005).

Key issues of ISM best practices include:

- Best practices framework.
- Compliance to ISM standards.
- Competitive advantage.
- Business continuity.

Some important factors of best practices are: “The organisation has a clean desk policy; the anti-virus systems used are up-to-date and are capable to safeguard against viruses; proper authentication is required for external connections; the organisation follows risk assessment and risk management processes to determine acceptable controls; systems are updated/upgraded according to a structured plan and not in an ad hoc manner; and every information security incident is reviewed and a report is submitted to the higher management” (Singh et al., 2014).

According to Saint-Germain (2005), the ISO 17799/BS 7799 information security standard provides guidelines on the following security domains: “Security policy, organisational security (management and responsibility), asset classification and control, personal security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance.” It is clear that the importance of ISM best practices is that it improves all/most of the other ISM activities.

The next activity of ISM is asset management.



### 2.2.2.8 Asset Management

There are three valuable parts/assets in a computer-based system: hardware, software and data. Each of these parts has different vulnerabilities that need to be considered when doing information security planning.

Figure 2.4 presents the three valuable parts/assets mentioned, as well as the possible dangers/threats to each part/asset. Interruption is when an asset of the system becomes unusable, unavailable or lost. Interception is when an unauthorised party gains access to an asset. If the unauthorised party tampers with an asset, it becomes modification; when the unauthorised party creates counterfeit objects on the system it is fabrication.

In order to properly manage an organisation's assets, the organisation has to identify all assets, consider associated risks and have controls in place to prevent the risks from taking place (Pfleeger et al., 2015).

Key issues of asset management include:

- Risk assessment.
- Asset classification and control.
- Ownership.
- Threats and protection.
- Physical access control.
- Access control to IT systems/services.

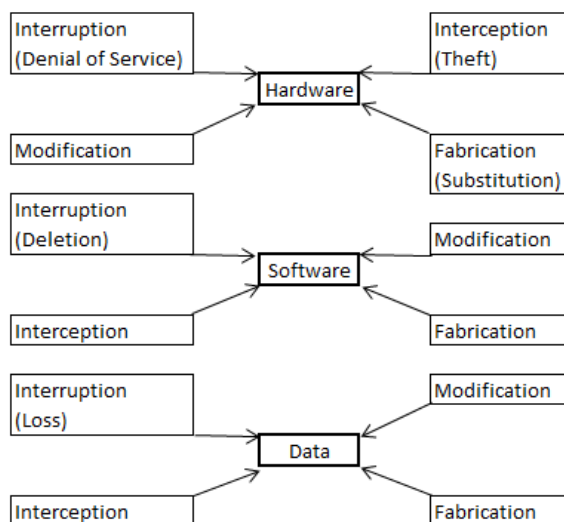


Figure 2.4: Possible Vulnerabilities of Assets (Adopted from Pfleeger et al. 2015)

Important factors of asset management are: “The organisation makes an inventory record of all the information assets (hardware and software); different departments/business units of the organisation maintain register of critical information assets; information assets are classified on the basis of confidentiality, accountability, usage, etc.; the organisation protects its information assets adequately (e.g. systems and information); the organisation has an access control policy that specifies which users have access to what data; and the organisation has policies requiring compliance with software licenses and prohibiting the use of unauthorized software” (Singh et al., 2014). It is seen that asset management is a crucial part in obtaining a secure system.

The next section discusses information security incident management.

### **2.2.2.9 Information Security Incident Management**

In the event of a security incident, a document called the incident response plan will be used to determine how to deal with the incident. An incident can be a single event, a series of events, or an on-going problem. The procedures described should define what constitutes an incident, identify the responsible party in case of an incident, and describe the action to be taken (Pfleeger et al., 2015).

Key issues of Information Security Incident Management include:

- Risk management.
- Incident management and response.
- Incident information management system.
- Incident response team.
- Business impact.
- Business continuity.

Important factors of information security incident management are: “The organisation has a documented disaster recovery and business continuity plan; in the event of a security incident, procedures clearly define what to do and who to call for assistance; the organisation takes disciplinary action against employees for violating information security rules/norms; disaster recovery and business continuity plan is discussed and communicated to all employees; the organisation has a backup and recovery process to maintain the integrity and availability of essential information processing and communication services; the organisation can survive a disaster that may result in the loss of systems, premises; historical records/data of information misuse/intrusion attempts/data theft are being maintained; and information security measures have been reviewed regularly - at least once a year” (Singh et al., 2014). It is shown that both

asset management and information security incident management are related aspects within ISM.

The next section is the last activity of ISM and discusses information security regulations compliance.

#### **2.2.2.10 Information Security Regulations Compliance**

Regular security audits are necessary to ensure that the information system complies with standards and guidelines as described in the security policy and other security documents. In some cases, there has to be punishment for noncompliance as failure to adhere by the security practices often lead to inadequate information security. Information security regulations compliance can be done by an independent team or by the organisation itself, often both (Pfleege et al., 2015).

Key issues include:

- ISM standards.
- Information security laws and regulations.
- Compliance to information security laws/regulations/standards.
- Adherence to organisational information security policies/guidelines.

Important factors of regulation compliance include: “The organisation has a data privacy and protection policy; employees have to sign a data privacy and protection agreement; contractors/third party vendors have to sign a data privacy and protection agreement while working with the organisation; there is a team/committee for monitoring organisation’s compliance to data protection law/legislation; the organisation adheres to the industry standards of information security management” (Singh et al., 2014). Information security regulations compliance is an important aspect of ISM.

The next section concludes the discussion of ISM and information security.

#### **2.2.3 Conclusion of Information Security**

There are many aspects of a good information security system. Thomson et al. (2006) state that employees without any training have unconscious incompetence. They do not know that they lack information security knowledge. They have to be made aware of that through awareness and training and will move to conscious incompetence as a result. Only then will they be aware of the security issues. Next they learn the security protocols and they become conscious competent. They follow security protocols, but have to remember it the whole time. If this is

done repeatedly and for long enough periods of time, it becomes a daily habit and they become unconsciously competent. The information security protocols are being followed without even thinking about it. It is part of their corporate culture.

The next section gives a discussion of information security culture and describes the different aspects thereof as described by different researchers.

### **2.3 Part Three: Information Security Culture**

In a security context, 'security culture' can be thought of as the awareness and understanding of security issues and policies (Pfleege et al., 2015). It can be assumed that information security culture is part of an organisation's culture as information security has become an organisational function. Information security culture can be regarded as a subculture that focuses on information security, concentrating on making information security a natural aspect in the daily lives of employees (AlHogail & Mirza, 2014).

Apart from the three aspects of corporate culture as defined by Schein (1999) and described in Section 2.1.2 (artefacts, espoused values and underlying assumptions), there is one more aspect to be added in an information security culture - knowledge. Knowledge is not part of normal culture as it is assumed that employees already possess the knowledge to perform their tasks. Security is not their primary or normal job, so it cannot be assumed that the average employee has the knowledge to perform his/her job in a manner that can be regarded information security aware. Employees need knowledge of information security in order to perform each and every task of their everyday activities in a secure manner. Therefore, information security knowledge can be included as the fourth level of information security culture and will affect all three other layers (Van Niekerk & Von Solms, 2010).

While information security is tied to technology, risk perception is a human characteristic. Not all systems are predictable, even when using mathematic tools, so it is not always possible to make predictive statements about a system (Munteanu & Fotache, 2015). When an unforeseen system flaw occurs, employees have to be able to handle the situation to ensure that the flaw does minimal, if any, damage to the organisation's information systems. A good information security culture ensures that employees are adequately aware of how they are expected to behave during these situations.

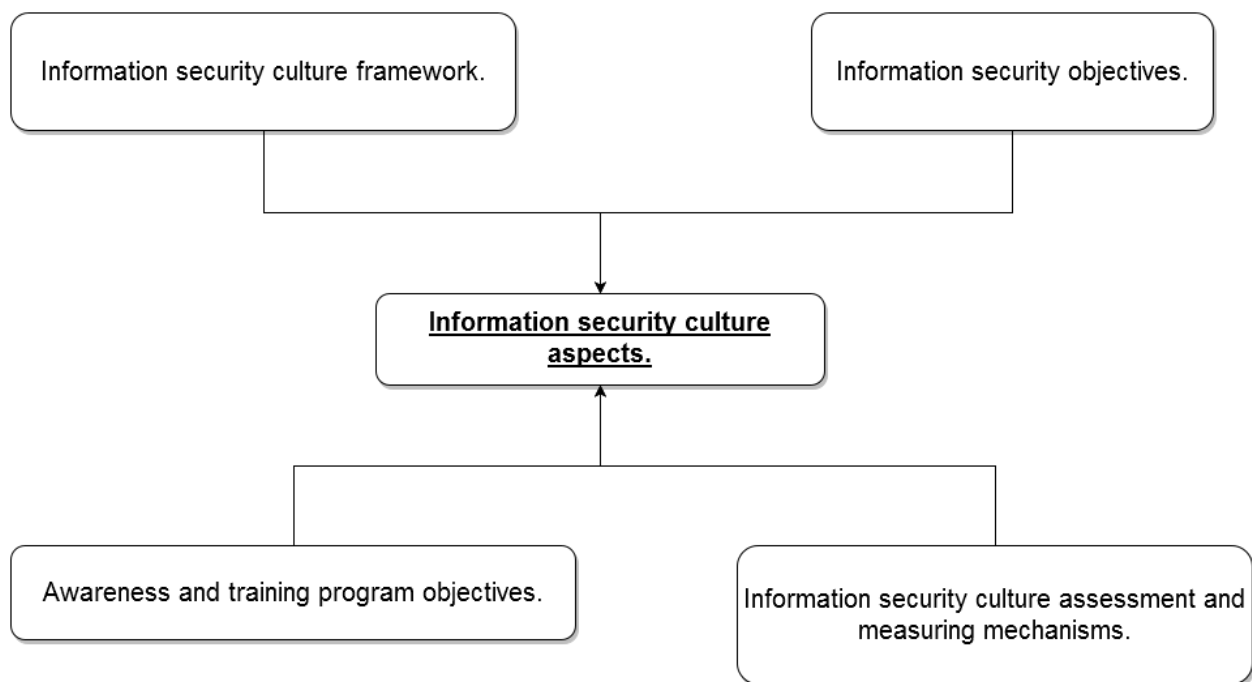
An information security culture, also called security aware culture, is developed when employees interact with information security procedures and controls. It can be defined as the attitudes, assumptions, beliefs values and knowledge of the employees used to interact with the organisations' systems (Da Veiga & Eloff, 2010). By establishing an information security culture,

an organisation can influence the security behaviour of its employees in order to guard against a wide variety of security threats (AlHogail, 2015). When an organisation has a culture that is security aware, the risk of employee misbehaviour and possible destructive contact with information assets is reduced. It is assumed that organisations already have technical controls in place.

Organisations have to place more focus on creating and growing a security aware culture as well as understanding the diverse range of possible security threats (O'Brien et al., 2013). AlHogail and Mirza (2014) define information security culture as: "The collection of perceptions, attitudes, values, assumptions and knowledge that guides how things are done in an organisation in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behaviour in a way that preserving the information security becomes second nature."

Employees need to understand the risk to the information they process, protect it using the required tools when processing it and be accountable for their actions. A culture should be maintained where it is evident that compliance behaviour for all sensitive and confidential information is maintained (Da Veiga & Martins, 2015). The organisational culture should be considered when cultivating an information security culture to ensure that the most appropriate controls are identified and deployed in a successful manner (Da Veiga & Eloff, 2010).

The next part of the literature review defines information security culture and investigates its various elements. It also investigates the different information security culture measuring mechanisms. By exploring these, it should be possible to categorise the key aspects found in any strong information system security culture. As seen in Figure 2.5, various articles used different definitions. These are combined and can be seen in Table 2.1.



**Figure 2.5: Various Definitions Combined into Information Security Culture Aspects**

### **2.3.1 Important Aspects of Information Security Culture**

The core of this study is to construct a list of aspects that describe organisational culture by studying various sources discussing it. Van Niekerk and Von Solms (2010) describe the basic aspects of information security as a culture whose net effect would meet the minimum requirements for some industry standard. The aim of this study is to determine what those minimum requirements are by reviewing different information security studies and frameworks.

#### **2.3.1.1 First Framework**

The first framework reviewed is from Da Veiga and Eloff (2010), and considers technical, procedural and human behavioural components. This is presented in Table 2.1. The table is one of the most comprehensive descriptions of an information system security culture and will be used as one of the primary sources when identifying all aspects.

Table 2.1 shows how information security components influence behaviour in employees, which in turn cultivates a strong information security culture. Different information security component categories can result in specific levels of information security culture (organisational, group, or individual) while others, like change management, is always necessary. In Table 2.1, the information security culture aspects are sorted into categories (first column) and are further sorted into organisational, group and individual tiers.

A (categories)	B (Information security culture aspects)			C
Information Security Component Categories	→ Influences	→ Information Security Behavior	→ Cultivates	→ Information Security Culture
	Organizational Tier	Group Tier	Individual Tier	
Leadership and governance	Sponsorship			Organizational artifacts and creations
	Strategy			
	Governance			Organizational values
	Risk management			Organizational assumptions
	ROI			
Security management and operations		Program organization		
	Legal and regulatory			
Security Policies	Policies			
	Procedures			
	Standards			
	Guidelines			
	Certifications			
	Best Practices			
Security program management		Monitor and audit		Group artifacts and creations
		Compliance		
User Security Management		Trust		Group values
		Education and training		Group assumptions
			Employee awareness	
			Ethical Conduct	
			Privacy	
Technology protection and operations		Asset Management		Individual artifacts and creations
		System Development		
		Incident management		Individual values
		Technical Operations		
		Physical and environmental		Individual assumptions
	Business Continuity Management			
Change	Change Management	Change Management	Change Management	

**Table 2.1: Information Security Culture Framework (Adapted from Da Veiga & Eloff, 2010)**

### 2.3.1.2 Second Framework

A second framework is adapted from Bulgurcu et al. (2010). This framework was used to measure employee compliance with information security policies. The following measurement items were included:

- Intention to comply with the information security policy – Intent to comply with the policy requirements, protect technology resources according to the policy, and use information and technology as described by the information security policy.
- General information security awareness – Being aware of security threats and their negative consequences, and knowledge of the cost of security failures.
- Information security policy awareness – Knowledge of the rules and regulations described in the information security policy, knowledge and understanding of the information security policy in order to enhance the overall security of the organisation.
- Attitude towards policy compliance – Belief of employees regarding the policy.

- Normative beliefs – Perception of fellow colleagues, executives and managers regarding the importance of policy compliance.
- Self-efficacy to comply – Possession of the skills, knowledge, and competencies to fulfil the requirements of the information security policy.
- Perceived cost of compliance – Perception of time and effort spent on policy compliance.
- Work impediment – Perception of how policy compliance hinders/impedes employee productivity or holds employees back from actual work.
- Intrinsic benefit – Contentment/fulfilment felt by employees for complying with the policy.
- Rewards – Concepts of tangible or intangible rewards based on policy compliance.
- Safety of resources – Perceptions of how policy compliance affects potential security risks and security related problems of resources.
- Perceived benefits of compliance – Perceptions of advantages/benefits gained from policy compliance.
- Sanctions – Penalties and reprimands caused by noncompliance.
- Vulnerability of resources – Perceptions that personal resources are at risk due to noncompliance.
- Perceived cost of noncompliance – Perception of possible personal negative impacts caused by noncompliance.

Motivational factors towards proper information security have a very big effect on employees' compliance behaviour and this in turn ensures a better information secure culture. As a result, it is advised that security awareness programmes should place some focus on influencing outcome beliefs positively (Bulgurcu et al., 2010). All of these identified aspects will be combined in Table 2.2.

### **2.3.1.3 Third Framework**

A third view is provided by Da Veiga, Martins and Eloff (2007), describing different dimensions of information security culture awareness. This view presents six different dimensions, each with certain concepts attached. They are:

- Management of information security – Accepting ownership, accepting change, necessity of resources, understanding threats.
- Performance management – Accepting necessity of monitoring and compliance, understanding of requirements.
- Performance accountability – Accepting accountability.
- Governance – Perception of visible leadership, protection of assets.
- Communication – Effectiveness of communication.



- Capability development – Capability enforcement, Implementation commitment, capability implementation effectiveness.

Each of these dimensions describes a general aspect of information security culture and can be divided into specific subcategories. By just being aware of the general aspects, an organisation can greatly improve its security culture.

#### **2.3.1.4 Fourth Framework**

After an extensive study, Dhillon and Torkzadeh (2006) identified 16 objectives that relate to information system security. While these are not by definition mentioned as part of information system culture, they share similarities with already identified aspects of security culture and will be used as aspects. The objectives are listed as follows:

- Increase trust – Maximise loyalty, display employer trust in employees, and create an environment that promotes organisational responsibility.
- Provide open communication – Ensure open communication between the IT department and other employees, minimise lack of information.
- Maximise awareness – Ensure that the environment promotes awareness, balances technical and social aspects of information system security, and promotes an understanding of the organisational culture.
- Optimise work allocation practices – Distribute the workload in a fair and optimal way; monitor and adjust free time.
- Establish ownership of information – Teach employees about ownership in the organisation and the importance of confidentiality; create a contract of confidentiality.
- Clarify centralisation/decentralisation issues – Make sure that there is a good balance between centralisation and decentralisation.
- Ensure legal and procedural compliance – Combat the indifference towards laws; minimise the tolerance of information misuse; provide employees with an understanding of legal and regulation issues; create a process that enables an information audit trail.
- Improve authority structures – Define the delegation of authority to all employees; ensure that there is no need for excessive control; limit the information access for different positions.
- Ensure availability of information – Create procedures to ensure that the correct information is available to all employees.
- Promote responsibility and accountability – Delegate responsibilities clearly; strive for the maximum level of commitment from employees; promote accountability.

- Understand the work situation – Create an environment with a minimum need to have leverage or seek revenge on other employees and where there is a minimum amount of disgruntled employees.
- Maximise fulfilment of personal needs – Provide options to employees for job enhancement; enable the achievement of self-actualisation needs.
- Understand individual characteristics – Understand individual characteristics and individual lifestyles of employees.
- Enhance understanding of personal financial situation – Ensure that there are no financial benefits in providing competitors with information.
- Ensure censure – Create a fear of negative responses triggered by noncompliance, including job loss, employees being exposed or ridiculed.
- Understand personal beliefs – Create an environment in which individuals are celebrated and understood; instil moral values and ethics into the organisational culture.

By following these objectives, an organisation will not only improve the information system security culture of its employees, but also improve on the overall morale of all employees because their individual needs are understood and fulfilled.

#### **2.3.1.5 Fifth Framework**

When creating an awareness programme, it is important to look at the business objectives and ensure that the employees understand the importance of the programme. To do this, the programme should be explained in a language that is easily understood and can be respected (Peltier, 2005).

The business objectives or mission requirements that an awareness programme should meet are as follows (Peltier, 2005):

- Risk analysis – Identify and assess factors that might potentially become problems in the future.
- Risk assessment – Determine the possible threats to each asset of the organisation and prioritise the possible risks to best implement appropriate security measures.
- Policies – Describe the goals and objectives for protecting the organisation's assets, as well as what is expected from all employees when using the organisation's assets.
- Procedures – Describe the step-by-step process used to complete a task, assist in the prevention of asset misuse and fraud, and explain return on investment; it provides users with all the necessary information needed to complete a task, and ensures management that the task is done.

- Standards – A norm or limit on how things are done; for example, data storage and hardware used.
- Business continuity planning – A description of procedures to follow during an incident or after an incident has occurred.
- Effective communication – Clear communication lines between employees, management and the security officer.
- Compliance – Monitor employee compliance to the security objective.

The value of business objectives in an awareness programme is extremely important as it is one of the best ways to ensure that those in managerial positions take it seriously. When comparing it to the previous study, refer to the description on Dhillon and Torkzadeh,'s (2006) 16 objectives, these business objectives appear to be harsh and formal. The reason is that the nature of the organisational culture will define which areas of information security culture to emphasise. The more formal aspects are probably for a bureaucratic or individualistic culture.

Section 2.3.1 looked at important aspects required to describe an information security culture. The security culture aspects from five studies were investigated and will be used in combination with information from Section 2.3.2 in constructing a list of all information security culture aspects. Some of these aspects can be considered as obvious; others are specifically considering the feelings and beliefs of employees.

The next section presents information security culture assessment methods to combine the identified aspects with the methods used in information security assessments in order to identify as many information security culture aspects as possible. Once all the aspects are identified, they are used in a questionnaire to create the planned framework.

### **2.3.2 Assessing Information Security Culture**

An information security culture assessment instrument can help to determine whether the level of information security culture within an organisation is enhancing the security of information assets. The results derived from using this instrument provide a roadmap to positively influence developmental areas concerning employee behaviour and attitude. These measures need to measure and report on the state of information security culture in the organisation (Da Veiga & Eloff, 2010).

According to Bulgurcu et al. (2010), employees' attitudes towards information security are greatly affected by three aspects: benefit of compliance, cost of compliance and cost of noncompliance. Benefit of compliance is shaped by intrinsic benefit, safety of resources and

rewards, while cost of compliance is shaped by work impediment. Cost of noncompliance is shaped by intrinsic cost, vulnerability of resources, and sanctions.

One method of testing an information security culture within an organisation is by presenting the following statements to employees in Likert scale questions where respondents had to choose from a low number (disagree strongly) to a higher number, indicating that they strongly agree (Da Veiga et al., 2007):

- The organisation protects its information assets adequately (for example, systems and information).
- It is important to understand the threats to the information assets (for example, systems and information) in my department.
- Threats to security of information assets (for example, information and systems) are controlled adequately in my department.
- Information security is necessary in my department.
- The information assets (for example, systems and information) I work with need to be secured, either physically or electronically.
- I believe my business unit will survive if there is a disaster resulting in the loss of systems, people and/or premises.
- I feel safe in the environment I work in.
- I believe that the information I work with is adequately protected.

Using a Yes/No scale, the following questions can be used to test the knowledge of employees:

- The organisation has a written information security policy.
- I have read the information security policy sections that are applicable to my job.
- I know where to get a copy of the information security policy.
- I know what information security is.
- I know what an information security incident is.

Additional questions regarding job level or demography can be added in order to group the respondents better (Da Veiga et al., 2007).

### **2.3.2.1 Sixth Framework**

The study by Da Veiga and Martins (2015) used 55 culture-related questions to measure security culture using Likert scale questions. These questions measure information system security culture in 10 constructs:

- Information asset management – How a user perceives the protection of information assets.
- Information security management – How management perceives ISM.
- Change management – How users perceive change and their willingness to change in order to protect information.
- User management – The level of users' training and awareness.
- Information security policy – How effective the information security policy was communicated to and understood by users.
- Information security programme – How effective investments into information security resources were.
- Trust – How users perceive the safekeeping of private information and whether they trust the organisational communications.
- Information security leadership – How users perceive information security governance with the aim of minimising information risks.
- Training and awareness – How employees perceive the need for additional security training.
- Privacy perceptions – How employees perceive privacy principles (organisational directives on how to protect confidential information).

Some aspects can already be identified as very important early on in this study. For example, the security policy is identified as an important aspect in nearly every study reviewed. Therefore, an organisation must have a clear security policy, ensure employees are aware of security procedures and there must be an obvious effort to improve security. This example is carried over to the framework created in this study.

The next section combines the identified aspects within a new framework.

### **2.3.3 Identified Aspects**

This section uses all the aspects of an information system security culture identified and discussed in previous sections and combines them to acquire a comprehensive list that is used in a questionnaire. This questionnaire was used to determine the acceptable baseline for information security culture aspects. Table 2.2 compares the aspects based on the source that represents the study, followed by an explanation of how the final column in the table was defined. The terms and groups are further defined in the next section.

Six studies were investigated for different information security culture aspects in the literature. These are sorted in Table 2.2 according to date. It is evident that some studies identified a wide

variety of aspects, while others identified fewer relevant aspects. Some aspects are grouped in the table; for example, policy was listed as a single entry in one study, while it could potentially be divided into six different aspects in another study; both instances comprise a policy.

The last column in the table is the final list of identified information security culture aspects that were used in the questionnaire to measure the importance of each identified aspect. This column shows the combined aspects as they are sorted and the number of times that they are found in the reviewed literature. There are six aspects that were dropped because they can be fitted into other aspects; for example, proper work situation can easily fit together with fulfilment of personal needs of employees. The list of identified aspects will be discussed next.

The aspects identified can be divided into three groups. The first group are aspects that were discussed in at least four of the six data sources. These aspects are very important, but are sometimes vague. Each aspect can be broken into more specific parts that are relevant to different organisations. These aspects are:

- Policy – There is a clear data policy describing all procedures, standards, guidelines and best practices; all employees are aware of the policy, its content and where to find it.
- Compliance – There are clear costs to noncompliance of security protocols; employees are aware of the possible repercussions if they do not adhere to the policy.
- Managerial trust/Information security leadership – It is clear to all employees that managers adhere to the policies and can be disciplined if they do not comply.
- Information security awareness – Awareness programmes are continuously run to keep employees up to date on security threats.
- Information asset management – Employees understand the value of information in the organisation and how vulnerable an information resource can be.

Peltier (2005)	Dhillon & Torkzadeh (2006)	Da Veiga et al (2007)	Da Veiga & Eloff (2010)	Bulgurcu et al (2010)	Da Veiga & Martins (2015)	Final & Count
			Sponsorship		Management's perceptions	Management's perspective: 1
			Strategy			Strategy: 1
	Delegation of responsibility		Governance			Delegation of responsibility: 1
Risk Analysis/Risk Assessment			Risk Management			Risk analysis: 1
			ROI (Return on Investment)			ROI: 1
			Program Organization			Dropped
	Understanding legal and regulatory issues		Legal and regulatory			Legal and regulatory: 1
Policies		Understanding of Requirements/Knowledge of Policy/Access to Policy	Policies	Information Security Policy Awareness	Information Security Policy/Privacy Perceptions	Policy: 5
Procedures			Procedures			
Standards			Standards			
			Guidelines			
			Certification			
			Best practices			
	Information audit trail	Necessity of monitoring and compliance	Monitor and Audit Security Program			Monitor and audit: 3
Compliance		Performance Management	Security Compliance	Intention to Comply with the Policy		Compliance: 5
				Attitude Towards Policy Compliance		
				Normative beliefs		
				Perceived Cost of compliance		
				Work Impediment		
				Intrinsic Benefit		
				Rewards		
				Safety of Resources		
				Perceived Benefits of Compliance		
				Sanctions		
	Negative responses to noncompliance			Perceived cost of Noncompliance		
	Increase Trust	Governance perception	Trust (Management)		Trust/Information Security Leadership	Trust/Leadership: 4
		Capability development	Education and Training	Self efficacy to comply	User training and awareness	Security awareness: 5
	Maximize awareness	Understanding Possible Threats & need for Information Security	Employee awareness	General information security awareness		
			Ethical Conduct			Ethical Conduct: 1
			Privacy			Dropped
		Protection of Assets	Asset Management	Vulnerability of resources	Information Asset Management	Asset management: 4
			System Development			Dropped
Business Continuity Planning		Incident Controls	Incident Management			Continuity/Incident Management: 3
		Post-Incident Controls				
		Electronic Asset Protection	Technical Operations			Information security program: 3
		Physical Asset Protection	Physical and Environmental		Information security programme	
			Business Continuity Management			Dropped
		Accepting Change	Change Management		Change Management	Change Management: 3
	Ownership of information/contract of confidentiality	Accountability/Accepting ownership				Accountability: 2
Effective Communication	Open Communication	Communication				Communication: 3
	Fairness towards employees (work allocation)					Fairness towards employees: 1
	Limit information access					Dropped
	Proper work situation					Dropped
	Fulfillment of personal needs of employees					Personal needs of employees: 1

**Table 2.2: Information System Security Culture Aspects**

The second group of aspects were discussed in at least three of the six data sources, and excludes aspects from the first group. These aspects are of a moderate importance and are more specific than the first group. Information security culture aspects in the second group include:

- Information monitoring and audit – It should be possible for an external individual/organisation to test the security procedures of the organisation. All work done and information used should be properly documented to ensure that all work done can be traced.
- Business continuity plan/Incident management – Procedures regarding incidents are normally incorporated into the organisation's policy, but are important enough to be mentioned so often that it is identified as an aspect on its own. These procedures describe actions to be taken in the event of an incident that can potentially cause harm to the organisation's assets, or procedures to take after such an event has occurred. Examples include fires, hacking attempts or server crashes.
- Information security programme – Technical and physical aspects used to protect assets. Employees should be aware of the technical and physical safeguards and know how to use them where applicable.
- Change management – Employees should be encouraged to be open to change in the organisation. Management could play a big part in change management by showing lower level employees that they embrace change. This is especially important in organisations where employees reject security measures because it is "too new" for them.
- Communication – Clear lines of communication between employees, management and security officers should be in place. Employees should know who to ask concerning security, where to report possible security threats, and know who to contact regarding ideas/complaints about security protocols.

Aspects in the third group can be seen as subcategories and can be grouped with aspects in any of the first two groups if necessary. These aspects are mentioned once or twice in all the sources. Some of these aspects were dropped as a result of their similarity to other identified aspects. These aspects are still important for any information system security culture and include:

- Management's perspective – It is important that those in managerial positions do not see a training and awareness programme as a waste of time and are willing to contribute time, effort and money into the programme.



- Strategy – Leaders should have a clear strategy on implementing awareness and training programme.
- Delegation of responsibility – Specific tasks are delegated to employees in such a way that all employees are sure of their roles. This does not apply only to information security.
- Risk analysis – All potential risks to information assets are analysed and managed in such a way that security protocols are set according to the value of assets and the potential security threats to each of them.
- ROI (return on investment) – Leaders in the organisation should see how investing in information security training returns a financial gain to the organisation.
- Legal and regulatory – Employees should be aware of the legal consequences of security breaches and how it can affect them.
- Ethical conduct – Employees should be encouraged to behave in an ethical manner towards each other and all organisational assets.
- Accountability – Employees should be encouraged to take accountability for their own actions without constant managerial supervision.
- Fairness towards employees – Managers and employees in leadership positions should focus on being fair to lower level employees in terms of work allocation and rewards for good services. This encourages employees to have stronger loyalty to the organisation and reduces the risk of intentional harm from employees.
- Fulfilment of personal needs of employees – By spending some resources on the personal needs of employees, an organisation can improve the employees' loyalty and reduce the risk of intentional harm from employees.

These identified aspects and descriptions are the final aspects of information security culture identified from the reviewed literature. The aspects with a higher count can be regarded as more important than those aspects with lower counts.

### **2.3.4 Conclusion of Information Security Culture**

These identified aspects derived from the six frameworks of information security culture were used to design a questionnaire that was sent to organisations in order to get feedback, comments and amendments from the respondents. The design of the questionnaire is further discussed in Chapter 3.

The next section investigates awareness and training programmes, their content and the important delivery methods of information security training.

## **2.4 Part Four: Information Security Awareness and Training Programmes**

Any IT organisation that intends to survive the various information security threats of the modern world should educate its employees on the importance of information security. The purpose of a security awareness programme is to change the way in which people think and act where information security is concerned; develop mechanisms to measure the knowledge of the participants and the success of a programme; and to continually address the importance of information security (McCoy & Fowler, 2004). This is true for IT organisations as well as any other information intensive organisation (Herath & Rao, 2009).

When focusing on knowledge, there are three levels of learning to consider. The first level of learning is awareness. This should not be seen as training, since awareness simply attracts the mindfulness of employees to the subject of information security. It demonstrates to them the concern for information security and basic responses. Awareness activities are usually directed towards broad audiences and tend to be short term, immediate and specific. These activities have to be repeated regularly in order to be effective. All employees in an organisation should at least be security aware. The next level of learning aims at building knowledge and producing relevant security skills and competencies. Training takes longer than awareness and is more formal, requiring learners to take a more active role in the process. After a training course, employees are expected to have developed specific information security skills. The level of training needed for each employee is different based on his/her specific job description. The final level of learning is education and is meant only for those who become information security experts. It strives to produce information security specialists and professionals (Katsikas, 2000). Training is the most frequently suggested method for improving policy compliance (Puhakainen & Siponen, 2010).

There are various options for adding an awareness and training programme into organisations. Some organisations hire external parties to plan and execute the entire programme or buy a pre-planned programme and execute it themselves. There are many guidelines and tips on how to establish a new awareness and training programme (Wilson & Hash, 2003). It is noted that using different methods/media will result in better performance in different fields (Shaw, Chen, Harris & Hui-Jou, 2009).

It is often found that employees of all levels in an organisation are negative towards the security officer, including the security officer him-/herself. The security officer may find it difficult to express how he/she is adding to the business objectives. Users often do not understand the technical and security terms in which the security officer expresses himself/herself. Therefore, it is very important to use the same terms that management use to ensure employees are more

positive towards awareness and training sessions (Peltier, 2005). This is another reason why management support is essential to a successful programme.

The next section presents different topics that need to be addressed during an information security awareness and training programme.

#### **2.4.1 Awareness and Training Topics**

Wilson and Hash (2003) provide a detailed description of how to set up a well-planned information security awareness and training programme. The topics they encourage organisations to discuss are:

- Password usage and management – including creation, frequency of changes and protection.
- Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating anti-virus definitions.
- Policy – what the security policy says and the implications of noncompliance.
- Unknown e-mail/attachments and how to handle them.
- Web usage – allowed versus prohibited websites; monitoring of user activity.
- Spam. – What it is and how to avoid it.
- Data backup and storage – centralised or decentralised approach.
- Social engineering– what it is and how to avoid it.
- Incident response – Whom to contact in case of an incident; procedures to follow.
- Shoulder surfing – What it is and how to avoid others from viewing your screen.
- Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access).
- Inventory and property transfer – identify responsible organisation and user responsibilities (e.g., media sanitisation).
- Personal use and gain issues – systems at work and home.
- Handheld device security issues – address both physical and wireless security issues.
- Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance.
- Laptop security while on travel – address both physical and information security issues.
- Personal owned systems and software at work – state whether allowed or not (e.g., copyrights).
- Timely application of system patches – part of configuration management.
- Software license restriction issues – address when copies are allowed or not allowed.

- Supported/allowed software on organisation systems – part of configuration management.
- Access control issues – address least privilege and separation of duties.
- Individual accountability – explain what this means in the organisation.
- Use of acknowledgement statements – passwords, access to systems and data, personal use and gain.
- Visitor control and physical access to spaces – discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
- Desktop security – discuss use of screensavers, restricting visitors' view of information on screen.
- Protect information subject to confidentiality concerns – in systems, archived, on backup media, in hardcopy form, and until destroyed.
- E-mail list etiquette – attached files and other rules.

Of the above topics, 18 were chosen by Kim (2014) as the most important information security awareness topics that should always be discussed during an information security awareness and training programme. These 18 are:

- To understand the need of an anti-virus program.
- To understand the need of updating virus definitions.
- To regularly scan a computer and storage devices.
- To use a personal firewall.
- To install software patches.
- To use pop-up blockers.
- To understand the risk of downloading programs or files.
- To understand the risks of peer-to-peer (P2P) file sharing.
- To understand the risk of clicking on e-mail links.
- To understand the risk of e-mailing passwords.
- To understand the risk of e-mail attachments.
- To regularly backup important files.
- To understand the risk of smartphone viruses.
- To understand the need of anti-virus program for a smart phone.
- To know the characteristics of a strong password.
- To use different passwords for different systems.
- To change passwords regularly.

McCoy and Fowler (2004) add that legal, regulatory and ethical issues should also be added in an information security awareness and training programme. This includes accountability and

possible responses to security breaches. After the topics have been identified, it is necessary to reflect on the methods to deliver them.

#### **2.4.2 Delivery Methods**

The question of how employees learn is important when creating awareness and training programmes. Different topics are best conveyed using different delivery methods. The three basic training methods are reading about a subject, watching a video, or asking someone to demonstrate the process. The third delivery method is regarded as effective for most employees (Peltier, 2005). Awareness topics can be introduced in an informal setting. It has a limited influence, and must be short term and subject specific.

Wilson and Hash (2003) provide the following awareness delivery methods:

- Messages on awareness tools (e.g., pens, key fobs, post-it notes).
- Posters, “do and don’t lists,” or checklists.
- Screensavers and warning banners/messages.
- Newsletters.
- Desk-to-desk alerts (e.g., a hardcopy, bright-coloured, one-page bulletin).
- Agency wide e-mail messages.
- Videotapes.
- Web-based sessions.
- Computer-based sessions.
- Teleconferencing sessions.
- In-person, instructor-led sessions.
- IT security days or similar events.
- “Brown bag” seminars.
- Pop-up calendar with security contact information, monthly security tips, etc.
- Mascots.
- Crossword puzzles.
- Awards programme (e.g., plaques, mugs, letters of appreciation).

Training should be presented in a more formal manner than awareness, since it has the purpose of building knowledge or developing specific skills. Wilson and Hash (2003) provide the following training delivery methods:

- Interactive video training (IVT).
- Web-based training.

- Non-web, computer-based training.
- Onsite, instructor-led training (including peer presentations and mentoring).

The following is a list of methods to improve awareness of information security (Banerjee & Pandey, 2010):

- Training and education.
- Campaigns.
- Interviews and questionnaires.
- Surveys.
- Industry / Academia interaction.
- Tests and experiments.
- Games and simulation.
- Industry / Academia tools.
- Online community advice.
- Media and related areas.

It is also an option to buy a pre-packaged awareness programme from the private sector. Some firms offer security awareness curricula as fully formalised product lines with live seminars (Valentine, 2006). The benefit of such a pre-packaged programme is that it has already been evaluated.

The identified delivery methods were shortened into a concise list, as it was seen that a long list of delivery methods could potentially confuse respondents. Another consideration was that the questionnaire could become too long if too many delivery methods were included. This may cause respondents to be confused or to stop completing the questionnaire. The identified delivery methods were shortened into the following five groups:

1. Formal training sessions – instructor led sessions and seminars.
2. Informal training – “brown bag seminars” (a quick meeting usually held over lunch where everyone can eat their food during the seminar), web-based instructor-led training or teleconferences.
3. Short messages around the office – posters, “do and don’t lists”, checklists or desk-to-desk alerts.
4. Employee sitting in front of computer – introductory course on security, games and simulations, puzzles, screensavers, mass emails, or a pop-up calendar with security details.

5. Other – Mascots, award programmes for good security practice, videotapes, security related events, or newsletters.

### **2.4.3 Conclusion of Awareness and Training**

There are many aspects to an information security awareness and training programme. The five key aspects are: a process to deliver and reinforce the importance of information security, identifying those that are responsible for implementing the security programme, determining the sensitivity of information, the business reason describing the need for security, and senior management support (Peltier, 2005). A variety of delivery methods was presented in this section. The identified delivery methods in this study will be used as part of the questionnaire to identify how organisations prefer to improve the security awareness of their employees.

## **2.5 Summary**

There are many ways for an organisation to measure and improve its information security culture. Using the six studies that were investigated, a list of 21 unique and specific information security culture aspects was created. These are: policy; compliance; managerial trust/Information security leadership; education and training; information security awareness; information asset management; information monitoring and audit; business continuity plan/incident management; information security programme; change management; communication; management's perspective; strategy; delegation of responsibility; risk analysis; ROI; legal and regulatory; ethical conduct; accountability; fairness towards employees; and fulfilment of personal needs of employee. The delivery methods were shortened to a list of five methods: formal training; informal training, short messages around the office; employee sitting in front of computer; and other.

This study uses the identified aspects and awareness and training delivery methods, with the aid of a questionnaire, to investigate what organisations define as a norm for the level of information security culture aspects. The study further uses the identified delivery methods as a measurement for identifying respondents' preference to achieve the identified norms. The data regarding information security culture and awareness and training programmes (refer to Sections 2.3 and 2.4) are used in the construction of a questionnaire (refer to Chapter 3).

In the next chapter, the research paradigm, data sources, participants, data collection method(s) and analysis are discussed. The design of the questionnaire is also shown.

### 3 CHAPTER 3: RESEARCH METHODOLOGY

Research can be defined as a process of systematic enquiry with the purpose of collecting, analysing, interpreting and using data. It has many purposes, including understanding, describing, or controlling phenomenon or to empower individuals (Mertens, 2014). Figure 3.1 shows that this chapter briefly describes research paradigms as well as an appropriate paradigm for this study, before it describes the research approach used, how the data is collected and analysed, as well as possible ethical considerations in this study. It further presents the process following in the study, before concluding this chapter.

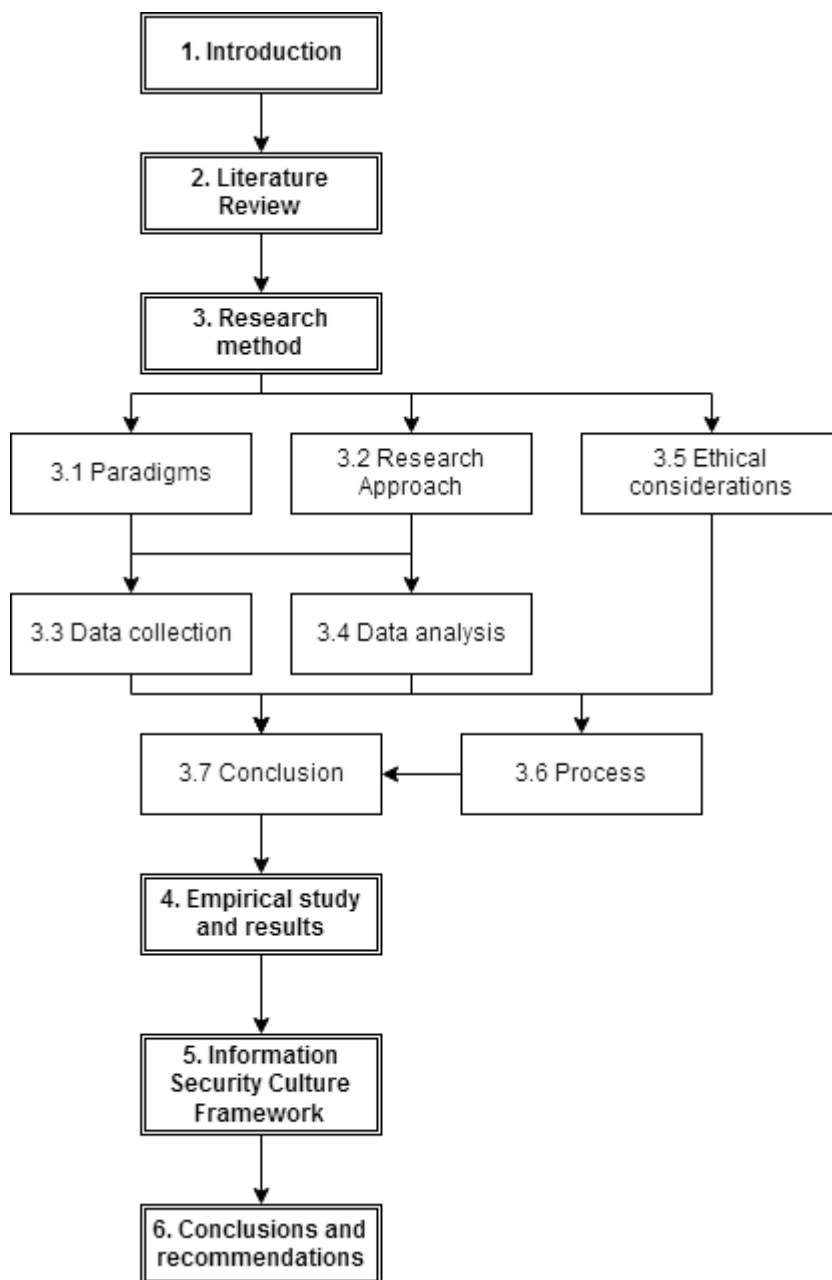


Figure 3.1: Introduction Chapter 3



### **3.1 Paradigms**

A paradigm can be defined as “a set of shared assumptions or ways of thinking about some aspect of the world”. Each research paradigm has its own ontology (views and perceptions of the ‘real’ world/the world being researched), and epistemology (the reasoning process or manner in which it can be obtained) that defines it (Oates, 2006).

Three research paradigms are discussed: the Positivistic, Interpretive/Constructivist, and Critical Social paradigms. This discussion is followed by a brief section regarding the appropriateness of each paradigm for this research study.

#### **3.1.1 Positivistic Paradigm**

The positivistic philosophy reflects much of Western science and is dominant in information systems research (Orlikowski & Baroudi, 1991). It is based on the belief that everything is driven by unchallengeable natural laws and that the purpose of science is to calculate and control natural occurrences (Guba, 1990). Methods used in the positivistic paradigm are usually questionnaires, hypotheses and statistical analysis.

A positivistic paradigm means that data is derived from experiments and observations. “In the positivistic paradigm, the inquirer’s perspective is imposed on organisational members’ contextual spheres in a highly structured, often contrived and controlled, manner in order to facilitate clear isolation of cause and effect in tests of hypotheses deduced from a specific theory” (Henning, 2004).

Positivism is based on the following assumptions (Orlikowski & Baroudi, 1991):

- The research subject/phenomenon single, palpable and fragmental.
- The researcher is independent from the object of enquiry and there is a clear separation between observations and theory statements.
- Scientific concepts are precise and have permanent and invariant meanings.
- Using logic and analysis, it is possible to identify and test cause and effect relationships.
- Enquiry is value free.

The following words are commonly associated with positivism (Mackenzie & Knipe, 2006):

- Experimental.
- Quasi-experimental.
- Correlational.
- Reductionism.

- Theory verification.
- Causal comparative.
- Determination.
- Normative.

For this study, the positivistic paradigm seems appropriate in that data collection and analysis were done in the more traditional scientific way. This paradigm allows for repeatability.

### **3.1.2 Interpretive/Constructivist Paradigm**

The interpretive/constructivist paradigm differs from the positivistic paradigm where the social world is objectified by the researching subject. The interpretive paradigm perceives the social world as subjective; something that cannot be treated by researchers as natural objects (Tribe, 2001).

In the field of computer science, the interpretive paradigm offers a way of understanding computing as a practice constructed and developed by humans. It focuses on understanding the social part of an information system: which social influences played a part in the creation of the system and how it influences people (Oates, 2005). The fundamental assumption in interpretive research is that knowledge of reality can only be gained through social constructions such as consciousness, tools and other artefacts, and a shared language (Klein & Myers, 2001).

There are three basic principles of interpretive research (Cooper & Schindler, 2014):

- The world is constructed and meaning is provided by the people.
- The researcher is never neutral and is part of what is being observed.
- Research is driven by the interest of people conducting the research.

The following words are commonly associated with interpretivism (Mackenzie & Knipe, 2006):

- Naturalistic.
- Phenomenological.
- Hermeneutic.
- Ethnographic.
- Multiple participant meanings.
- Social and historical construction.
- Theory generation.
- Symbolic interaction.

Although interpretation and analysis of data sources was done in order to get a framework for the design of the questionnaire, this paradigm was not the main underlying philosophy.

### **3.1.3 Critical Social Paradigm**

The general outcome expected from the critical social paradigm is liberation. According to Tribe (2001), there are three interests that motivate human enquiry. These are a technical interest seeking to dominate and control an environment, a practical interest seeking to understand the environment/world, and an emancipatory interest seeking emancipation and freedom from falsehood and dogma. The critical social paradigm is served by the emancipatory interest.

In information systems, the critical social paradigm concerns itself with the identification of power relations, conflicts and contradictions, and eliminating people as sources of alienation and domination, therefore empowering them. Researchers in the critical social paradigm believe that social reality is created and re-created by people and that social reality possesses objective properties that tend to dominate our ways of seeing the world.

The following words are commonly associated with critical social theory (Mackenzie & Knipe, 2006):

- Neo-Marxist.
- Feminist.
- Critical race theory.
- Freirean.
- Participatory.
- Emancipatory.
- Advocacy.
- Grand narrative.
- Empowerment issue oriented.
- Change-oriented.
- Interventionist.
- Queer theory.
- Race specific.
- Political.

The aim in this study was not to liberate employees, although this may be a side effect in the long term. As such, this paradigm is not appropriate for this study.

### **3.1.4 Appropriate Paradigm**

The underlying paradigm for this study is positivism. This paradigm is regarded as the most appropriate for this study because it is objective, has been proven to be reliable, and the study should be repeatable. The researcher will not take part in the study and will remain objective. The research is based on generalisations.

The next section describes the research approach used.

## **3.2 Research Approach**

There are three typical approaches when conducting research: quantitative, qualitative and mixed methods. These approaches are described for the different types of data used in research (numeral, textual or combination numeral and textual). The quantitative approach is typically selected when numerical data is used, and the qualitative when textual data is used. A mixed method is selected when both numerical and textual data are required (Williams, 2007).

Some authors call positivism 'quantitative research' and interpretivism 'qualitative research'. According to Oates (2005), this is not true. Both qualitative and quantitative approaches can be used in any paradigm, although quantitative data tend to dominate positivism and qualitative data tends to dominate the other two paradigms. The three typical approaches will be discussed next.

### **3.2.1 Quantitative Research**

Quantitative research is driven by the need to quantify data. The research design is created with a numerical or statistical approach. The research is independent of the researcher and data is measured objectively. Using this approach creates meaning through objectivity collected in the data. Typically, quantitative research starts with a problem statement, followed by a hypothesis, a literature review and a quantitative data analysis (Williams, 2007).

### **3.2.2 Qualitative Research**

Many researchers using the qualitative approach believe that the best way to understand a phenomenon is to view it in its context. Quantifications are perceived as limited in nature, viewing just a small part of reality that cannot be fragmented or united without losing the importance of complete phenomenon. It is believed that the best way to understand a situation is to immerse oneself into the culture or organisation being studied and experience it from the inside. Instead of measuring with a fixed instrument, qualitative researchers become familiar with the study content in order to shape their questions (Krauss, 2005).

### **3.2.3 Mixed Methods**

Research that involves the integration of qualitative and quantitative approaches has become more common in recent years. Combining quantitative and qualitative approaches can be done to optimise the data collection process. This is called a mixed method research approach (Krauss, 2005).

There are many reasons for researchers applying mixed methods. Some of these reasons are (Bryman, 2006):

1. Triangulation: Convergence, corroboration, correspondence of results from different methods; seeking corroboration between quantitative and qualitative data.
2. Complementary: Seeking elaboration, illustration or clarification of the result of one approach with that of the other.
3. Development: Use the result from one approach to help develop the other approach.
4. Initiation: Seeking paradoxes and contradictions when comparing frameworks made from different approaches.
5. Expansion: Expand the breadth and range of an enquiry by using different approaches and approach components.

### **3.2.4 Approach Used in This Study**

This study uses mostly quantitative data; statistical analyses were done as is discussed in the next section. There are, however, some aspects of qualitative data analysis (in the form of open-ended questions) that were used to expand the range of enquiry. The result is that a mixed method approach is used. The design and create approach was used to plan and develop a mobile application for Android devices (refer to Chapter 5). This approach falls under the extreme programming where the planning, analysis, and design is done throughout development.

The next section describes the data collection method.

## **3.3 Data Collection**

### **3.3.1 Survey design**

A survey was done using a questionnaire to collect data for this research. Results from the questionnaire were used to draw conclusions regarding the whole population or a specific aspect of a population. This research targets any organisation or person within an organisation that has regular access to a computer in their work environment.

The questionnaire was developed based on the literature review conducted. The questionnaire uses the identified culture aspects, delivery methods, and important topics from the literature. It comprises six sections:

- **Key terms and aims of this study.** This section included a short consent form with relevant information as seen in Figure 3.2. A respondent could not proceed with the questionnaire without confirming that he/she has read and understood the general principles.

## Key terms and aims of this study

**Key terms:**  
Organizational culture is described as the “feel” of the organization to its members that directs and motivates employee efforts. It is what the employees believe and their perception on what is valued by their organization.  
Information security culture is part of an organization’s culture as information security has become an organizational function. It can be seen as a subculture that focuses on information security that emphasizes on making information security a natural aspect in the daily lives of employees.

**Aims of this study**  
To learn what organizations see as the minimum acceptable baseline of each information security culture aspect.  
Learn which training and awareness delivery methods are preferred to improve each information security culture aspect.  
And rate the importance of awareness and training topics as seen by modern organizations.

Please read the following general principles as it is important that you understand what you are agreeing to:

1. Your participation in this research project is completely voluntary, and no pressure, however subtle, may be placed on you to take part.
2. It is possible that you may not gain any benefit personally from your participation in the research project, although the knowledge that you provide may benefit other persons or communities.
3. You are free to withdraw from the research project at any time, without giving reasons for your decision. You will in no way be harmed in doing so. You may also request that your information provided, no longer be used in the research project. However, you are kindly requested not to withdraw from the project without careful consideration, since it may have a negative effect on the reliability of the project.
4. By agreeing to take part in the research project, you are also giving consent for the data that will be generated to be used by the researchers for scientific purposes as they see fit, with the agreement that it will be confidential and that your name will not be linked to any of the data without your consent.

By completing the accompanying questionnaire, you agree that you have read the previous information in connection with the research project and that you understand it. You also declare that you are taking part in the project voluntarily.

---

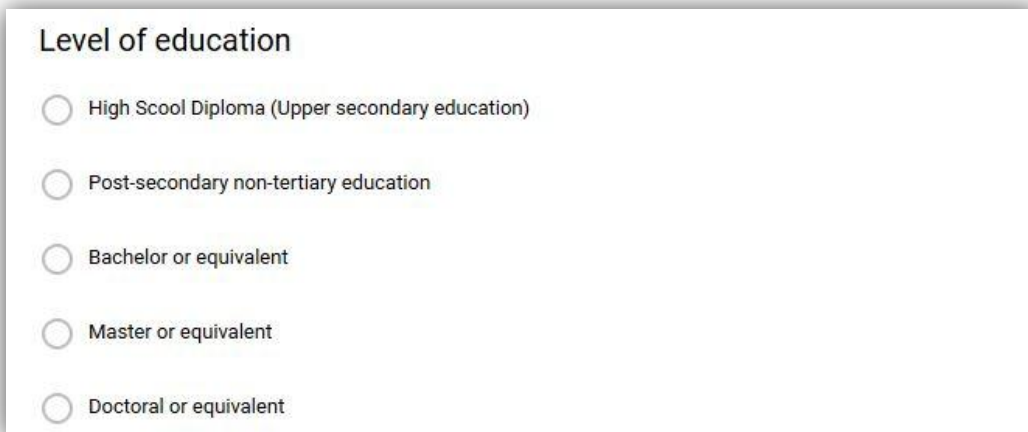
Untitled Question \*

☐ I have read and understand the general principles

**Figure 3.2: Key Terms, Aim and Consent Form in Questionnaire**

- **Demographical details.** This section asked respondents for their age, gender, level of education, level of employment; years of computer experience, urban/rural housing, type of organisation, and number of employees in their organisation (see Figure 3.3). This

does not relate directly to any of the aims of this study, but is used to find underlying trends in the data using statistical analysis.



**Level of education**

☐ High School Diploma (Upper secondary education)

☐ Post-secondary non-tertiary education

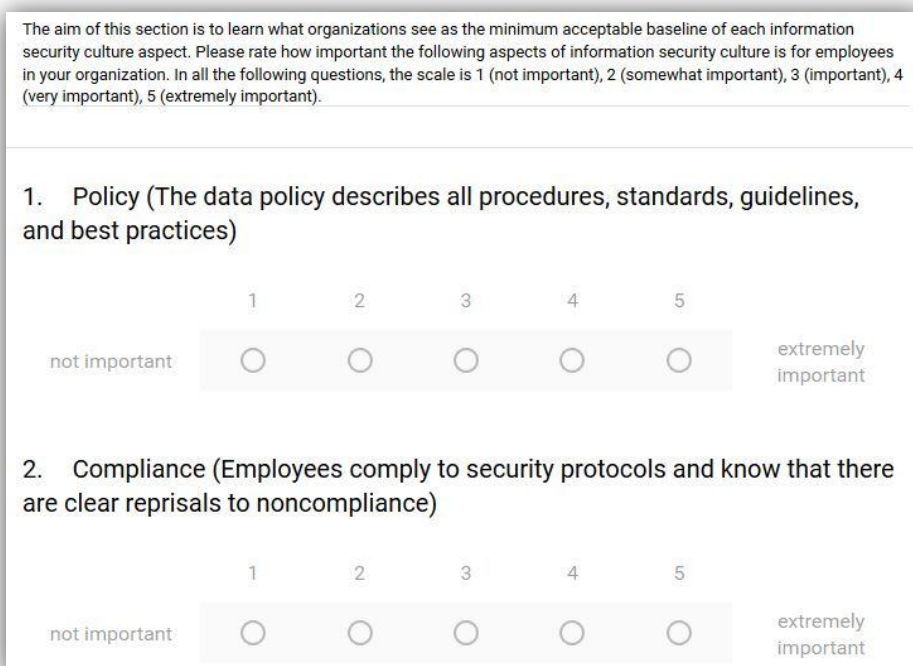
☐ Bachelor or equivalent

☐ Master or equivalent

☐ Doctoral or equivalent

**Figure 3.3: Example of Questions Related to Demographical Details in Questionnaire**

- **Information security culture aspects.** Figure 3.4 shows an example of how the information security culture aspects identified in the literature review was presented in the questionnaire. Each of the 21 aspects was presented with a short description and options to rate the aspects from 1 (not important) to 5 (extremely important). This fulfils the second aim of this study which is to use the aspects identified in the literature within different organisations to determine an acceptable baseline/standard.



The aim of this section is to learn what organizations see as the minimum acceptable baseline of each information security culture aspect. Please rate how important the following aspects of information security culture is for employees in your organization. In all the following questions, the scale is 1 (not important), 2 (somewhat important), 3 (important), 4 (very important), 5 (extremely important).

1. Policy (The data policy describes all procedures, standards, guidelines, and best practices)

1 2 3 4 5

not important ☐ ☐ ☐ ☐ ☐ extremely important

2. Compliance (Employees comply to security protocols and know that there are clear reprisals to noncompliance)

1 2 3 4 5

not important ☐ ☐ ☐ ☐ ☐ extremely important

**Figure 3.4: Example of Questions Related to Information Security Culture Aspects in Questionnaire**

- **Awareness and training delivery methods.** Figure 4.4 is an example of the delivery methods as asked in the questionnaire. For each identified information security culture aspect, the respondent is given five options. Each of these five options is composed of the delivery methods identified in the literature and grouped in such a manner that the respondents are not confronted with too many options. This provides the second part of the framework where each information security culture aspect is shown next to the preferred delivery methods that can be used to improve that aspect. This part of the questionnaire used multiple choice questions to rate the topics identified in the literature review. These topics are:
  1. Formal training sessions
  2. Informal training
  3. Short messages around the office
  4. Employee sitting in front of computer
  5. Other

This section is to learn which training and awareness delivery methods are preferred to improve each information security culture aspect. Please mark your preferred delivery method that you would choose to use to improve each information security aspect. The definitions of each security aspect term are the same as in part 2.

## 1. Policy

1. Formal training sessions (examples include instructor led sessions and seminars etc.)
2. Informal training ("brown bag" seminars, web-based instructor-led training etc.)
3. Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
4. Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
5. Other (award programs, security related events, videos etc.)

**Figure 3.5: Example of Questions Related to Awareness and Training Delivery Methods in Questionnaire**

- Figure 3.6 presents important topics pertaining to awareness and training programmes. This supports the aim of investigating which training/awareness delivery methods can be used to improve each identified information security culture aspect in order to reach the identified standard/baseline. Two open-ended questions are included at the end of this section. These open-ended questions are also at the end of the sections regarding information security culture aspects and important topics.



This section aims to rate the importance of awareness and training topics as seen by modern organizations. In all the following questions, the scale is 1 (not important), 2 (somewhat important), 3 (important), 4 (very important), 5 (extremely important). Please rate how important it is for employees to:

understand the need of an anti-virus program

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

understand the need of updating virus definitions

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

Are there any aspects not mentioned here that you believe is important? If yes, please name these aspects and give a rating to each of 1 (not important) to 5 (extremely important).

Long-answer text

Please give any comments or feedback that you might have regarding this aspect of your company.

Long-answer text

**Figure 3.6: Important Topics of Awareness and Training Programmes in Questionnaire**

- A final questionnaire page is presented to the respondent to ascertain his/her confidence regarding the information security culture in his/her organisation, as well as his/her knowledge/insight about the topics addressed in the questionnaire. Both these questions were compulsory to complete in order to submit a response. The final questionnaire page is shown in Figure 3.7.

# Thank you

I thank you for your participation, time, and valuable contribution to this project. Your participation is greatly appreciated.

Frans Nel (MSc Student)

Email: snarfnel@gmail.com

Supervisor: Dr L Drevin

Email: lynette.drevin@nwu.ac.za

Please fill in the last 2 questions

I am confident that my company has a strong information security culture. \*

	1	2	3	4	5	
severely pessimistic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	very confident

I am confident that I have a strong knowledge/insight on these topics. \*

	1	2	3	4	5	
severely pessimistic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	very confident

Figure 3.7: Final Page of Questionnaire

## 3.3.2 Participants

The questionnaire was created using Google forms and circulated by various means. These included:

- LinkedIn: A post with a link to the online questionnaire was posted on this social media site requesting anyone interested to fill in the questionnaire.
- A short article in the Institute of Information Technology Professionals South Africa IITPSA June/July 2016 newsletter was posted with a similar request.
- And personal emails were sent to IT related companies.

Emails were sent to employees of all ages, with various levels of education and years of computer experience, working for different types of organisations and employed at different levels (management, technical, etc.). Respondents from different sized organisations were

targeted. As information security is a topic relevant in almost all fields, the only criteria necessary for a respondent was that he/she must use a computer regularly in his/her work environment.

The electronic questionnaire ensured the anonymity of the respondents and made it easy to circulate the questionnaire. Data analysis of each part of the questionnaire is discussed in more detail in the following section.

### **3.4 Data Analysis**

The data collected from the electronic questionnaire was analysed statistically using different techniques. The techniques used are discussed in Chapter 4. Some open questions are included in order to expand the range of enquiry and ensure that there are no gaps in the questionnaire. The statistical consulting service of the North-West University was consulted in this regard.

As introduction to the questionnaire, the key terms and aims of this study, as well as a consent form with relevant information were presented to each respondent. This section does not return any information relevant to data collection. It serves as basic necessary information for all respondents and ensures that respondents know the principles behind the questionnaire. Each respondent was required to click on the checkbox indicating that he/she understood the consent form before he/she was able to continue with the completion of the form. With the exception of the last two questions, none of the remaining questions were compulsory to complete (a respondent could leave questions unanswered). The respondent was allowed to cancel the questionnaire at any point. This is further discussed in the next section.

The demographical data was not part of the original study aim, but was included to determine whether there were any interesting trends among respondents. For example, whether the level of employment has an influence on how information security culture is perceived, etc.

The section on information security culture aspects was the first part of the questionnaire that gathered actual data for statistical analysis. The questions were in the form of a Likert-type scale where each aspect was rated: 1 (not important), 2 (somewhat important), 3 (important), 4 (very important), 5 (extremely important). Based on the number of answers, each aspect was given a total score that could be compared to other aspects. This assisted in determining the importance of each aspect relevant to the other aspects.

This data could be interpreted in two ways: an average importance (in percentage) of each aspect, and a count of each of the numbers on the Likert-type questions. After the Likert-type

question, there were two open-ended questions asking if the respondent would like to add an aspect not mentioned in the questionnaire or has any comments or feedback. These open-ended questions were used to better understand how the respondents felt about the questions and ensured that there were no information security culture aspects missing from this study.

The next section in the questionnaire addressed awareness and training delivery methods. Originally, a much longer list was identified from the literature review. These were shortened to the following five options for delivery method:

1. Formal training sessions - instructor led sessions and seminars.
2. Informal training – “brown bag seminars” (this is a quick meeting usually held over lunch where everyone can eat their food during the seminar), web-based instructor-led training, or teleconferences.
3. Short messages around the office – posters, “do and don’t lists”, checklists, or desk-to-desk alerts.
4. Employee sitting in front of computer – Introductory course on security, games and simulations, puzzles, screensavers, mass emails, or a pop-up calendar with security details.
5. Other – Mascots, award programmes for good security practice, videotapes, security related events, or newsletters.

Respondents were asked to select one delivery method for each information security culture aspect. For each aspect, it was then possible to calculate the percentage of times that each delivery method was selected. The delivery method with the highest percentage is the obvious choice for each aspect, although all percentages are shown. These questions were followed by two open-ended questions to ensure that no preferred delivery methods were omitted from the study.

The next section discusses important topics of awareness and training programmes. Each topic identified in the literature review is presented and respondents were asked to rate its importance on a Likert-type question where each aspect was rated: 1 (not important), 2 (somewhat important), 3 (important), 4 (very important), 5 (extremely important). The responses were analysed in the same way as the information security culture aspects. There were two open-ended questions at the end of this section to determine if there are topics not mentioned and to provide respondents with the opportunity to state any other comments or feedback.

The last section briefly thanks participants and asked two important questions:

- Is the respondent confident that his/her organisation has a strong information security culture?

- Is the respondent confident that he/she has a strong knowledge regarding information security culture?

These two questions were of similar value as the demographical details and were used to determine how respondents rated themselves and their organisations.

### **3.5 Ethical Considerations**

This section briefly describes the ethical considerations in this study, mainly focusing on the questionnaire. All respondents were treated anonymously and the questionnaire was done on a voluntary basis. Respondents had the option of leaving the questionnaire at any time without any repercussions and could request that their responses be removed from the study. These ethical considerations were included in the questionnaire – respondents had to click on a button to indicate that they have read and understood the general principles of the questionnaire. These aspects were part of the study proposal and a committee on ethical matters has given permission for this study.

### **3.6 Data Analysis Process**

The data gathered with the electronic questionnaire was statistically analysed and described (this is presented in Chapter 4). The results were used to construct the standard/baseline for information security culture aspects and the appropriate delivery methods. This was used to create the framework (refer to Chapter 5). In order to apply the results in a practical way, a mobile application was developed (refer to Chapter 5).

### **3.7 Summary**

The research paradigm, research approach, data collection and analysis, as well as the ethical considerations of the study are discussed in this chapter. This study used a single questionnaire derived from literature sources as a data collection tool. Statistical analysis was done on the data collected from the electronically completed questionnaires. The next chapter presents the empirical study and results describing the data collected and how it was analysed.

## 4 CHAPTER 4: EMPIRICAL STUDY AND RESULTS

Figure 4.1 provides an overview of the structure of this chapter. This chapter describes the results from the questionnaire, shows the data analysis and results and explains how the framework (refer to Chapter 5) was developed using the data. The only data used in this chapter are the results from the questionnaire.

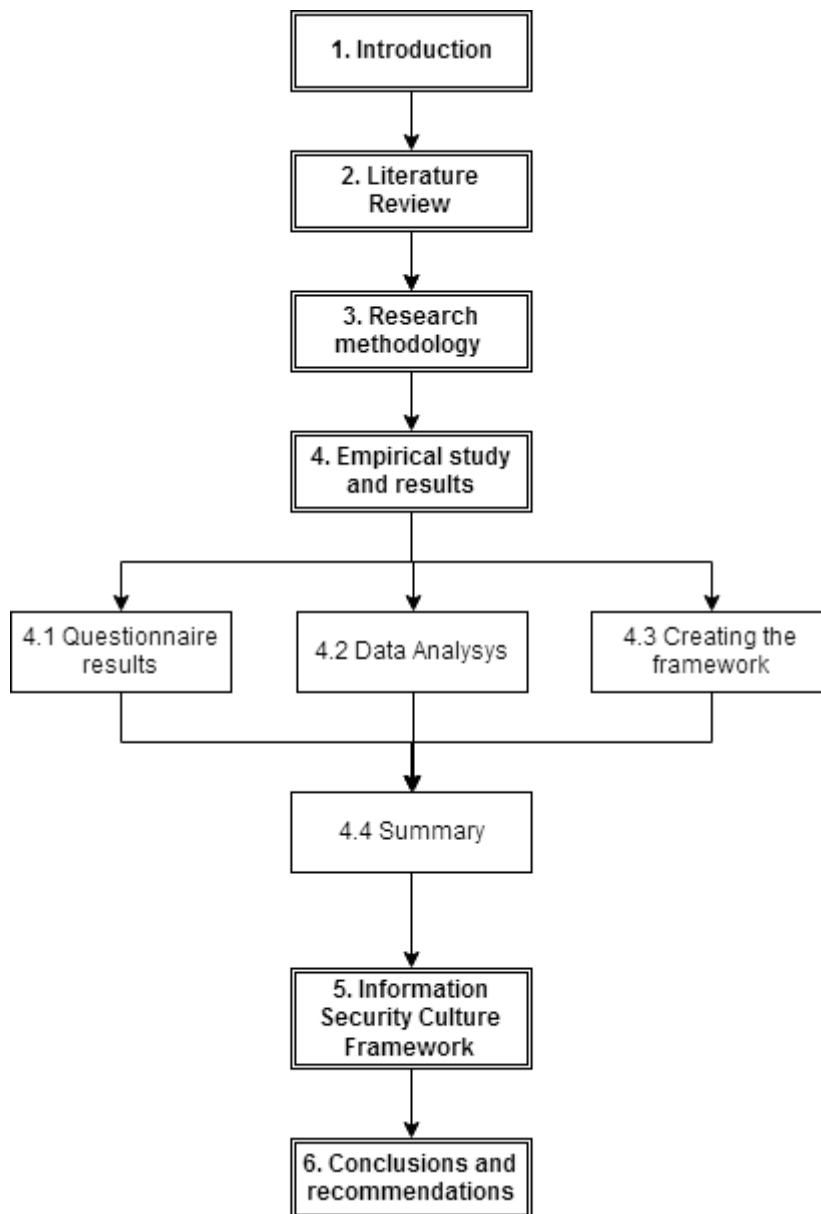


Figure 4.1: Introduction Chapter 4

### 4.1 Questionnaire Results

An electronic questionnaire was created to determine a norm/minimum acceptable baseline for the identified information security culture aspects. This questionnaire measured which delivery

methods are preferred by respondents for each information security culture aspect, as well as which topics in awareness and training programmes are seen as most important. The questionnaire consists of five sections, each with its own purpose. The sections are *Demographical details*, *Information security culture aspects*, *Awareness and training delivery methods*, *Important topics*, and *Confidence*. The last section determines the confidence of the respondent in his/her organisation's information security culture and his/her knowledge on the topic of information security culture.

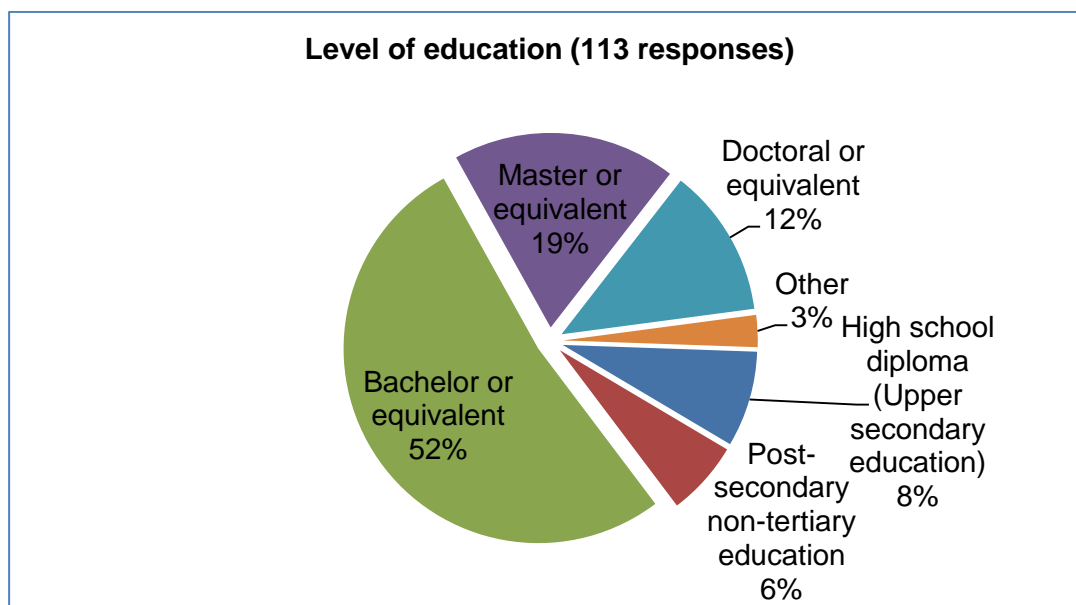
This chapter first describes the data received from each section of the questionnaire, followed by a description of the data analysis tools used and the results from the statistical analysis. The next section describes the demographical details.

#### **4.1.1 Demographical Details**

The online questionnaire was completed by 113 respondents. Apart from the button stating that respondents have read and understand the general principles, none of the questions were compulsory. This questionnaire design decision was made to prevent respondents from reacting negatively if they were compelled to answer each question (for example, if respondents fail to complete one or two questions and the questionnaire does not allow the respondent to continue) and decide to stop doing the questionnaire without completing it. As a result of this design, some questions were not completed by all respondents. The demographical details of respondents were the least answered section with only 89 people providing their age. The respondent age range is from 22 to 71 with an average age of 36.8 years. The majority of respondents were male with 78 (68.1%) male and 36 (31.9%) female. More than half of the respondents have achieved at least a bachelor's degree or equivalent, as seen in Figure 4.2.

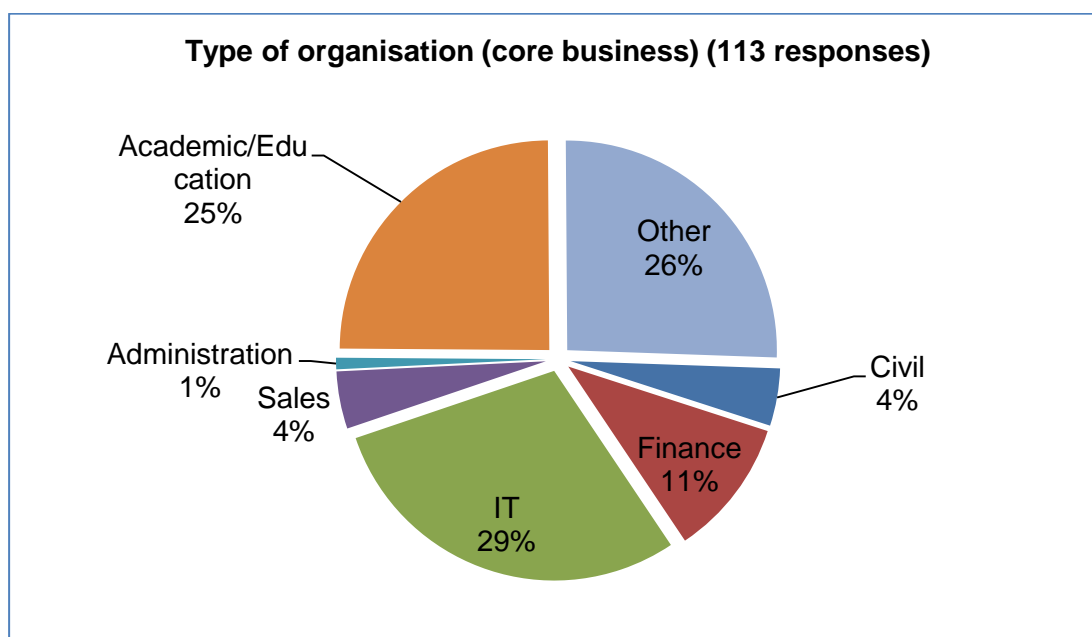
The level of employment amongst respondents was mostly technical 41 (38.3%) and middle management 36 (32.7%), followed by top level management 14 (13.1%), other 13 (12.1%), and administration 4 (3.7%). The 'Other' field includes intern, self-employed/business owners, start-up management and consulting.

Years of computer experience reported by respondents was mostly more than 8 years with 79 (69.9%) of respondents, followed by 3 to 5 years' experience 16 (14.2%), 6 to 8 years' experience 10 (8%), and 0 to 2 years' experience 9 (8%). 69 (61.4%) of the 113 respondents lives in urban areas, while 44 (38.6%) respondents live in rural areas.



**Figure 4.2: Respondents' Level of Education**

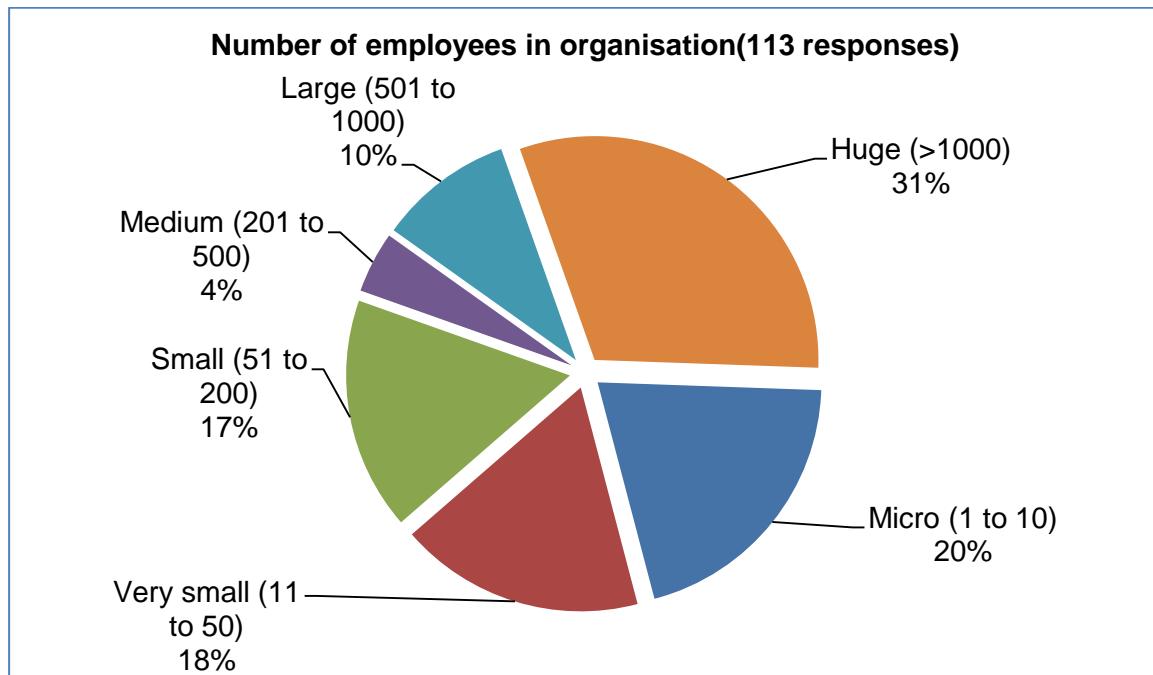
There is a wide variety of organisation types amongst the respondents. These are IT 33 (29.2%), other 29 (25.7%), academic/education 28 (24.8%), finance 12 (10.6%), civil 6 (4.4%), sales 5 (4.4%), and administration 1 (0.9%), and. The other category includes: consulting, research and development, pharmacy, nursing, logistics, architecture, production, power generation, transport, electronic warfare, engineering, fitness and health, legal, mining, petrochemical, and power generation. The questionnaire was sent to a wide variety of individuals and was made available to any and all organisation types possible. Due to privacy issues, respondents were not asked to identify their organisation. This is presented in Figure 4.3.



**Figure 4.3: Respondents' Type of Organisation**



The number of employees in an organisation was answered by all respondents. Data analysis shows that almost a third of respondent organisations have more than 1000 employees (31%). The statistics for number of employees can be seen in Figure 4.4.



**Figure 4.4: Number of Employees in Organisation According to Respondents**

More than 55% of respondents belong to organisation with between 1 and 200 employees. A very small number of respondents are from a medium-sized organisation, while more than 40% of respondents are from large or huge organisations. The demographical details are summarised in Table 4.1 and Table 4.2. Table 4.1 presents the age, gender, location (rural vs. urban), and level of education of respondents, while Table 4.2 provides the level of employment, years of computer experience, and type of organisation:

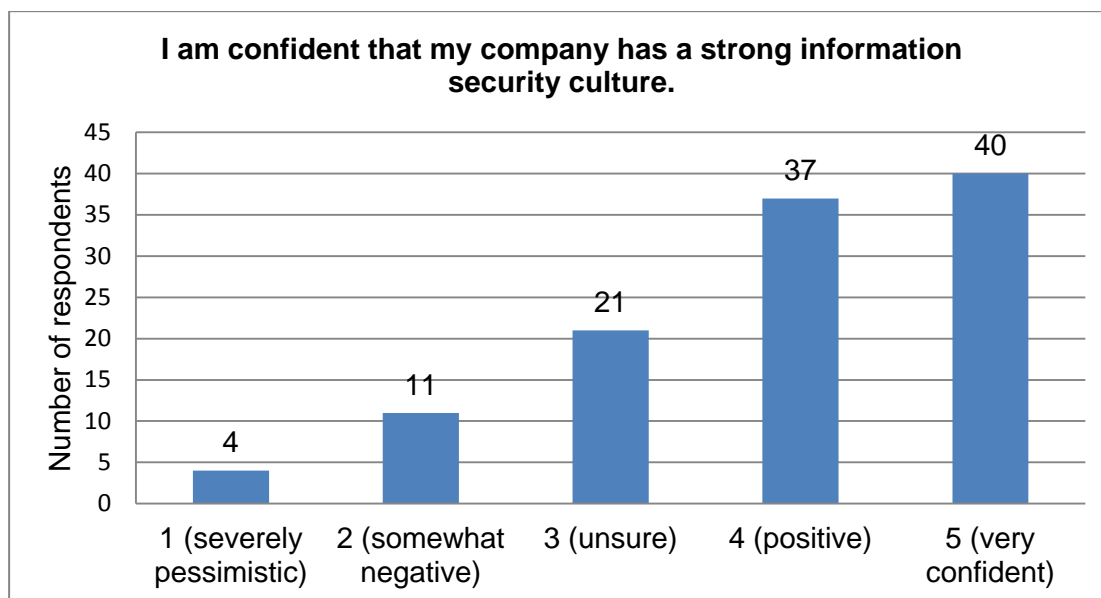
Age (89)		Gender (114)		Level of education (114)	
<25	11%	Female	32%	High school diploma (Upper secondary)	8%
25-27	25%	Male	68%	Post-secondary non-tertiary education	6%
28-34	15%			Bachelor or equivalent	52%
35-44	17%	<b>Rural vs. urban (114)</b>		Master or equivalent	19%
45-49	13%	Urban	61%	Doctoral or equivalent	12%
>50	19%	Rural	39%	Other	3%

**Table 4.1: Demographical Details - Part 1**

Level of employment (108)		Years of computer experience (114)		Type of organisation (core business) (114)	
Top Level Management	13%	0 - 2 years	8%	Civil	4%
Middle Management	33%	3 -5 years	14%	Finance	11%
Admin	4%	6 - 8 years	8%	I.T.	29%
Technical	38%	>8 years	70%	Sales	4%
Other	12%			Admin	1%
				Academic/Education	25%
				Other	26%

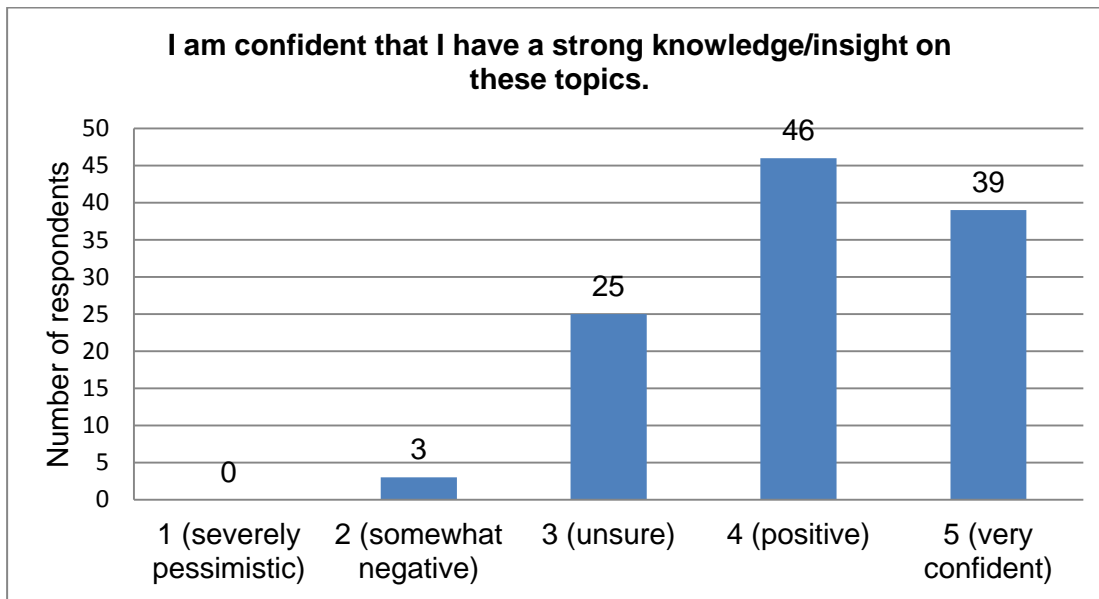
**Table 4.2: Demographical Details - Part 2**

At the end of the questionnaire, respondents were asked to rate two statements: I am confident that my company has a strong information security culture; and I am confident that I have a strong knowledge/insight on these topics. The results for these statements are shown in Figure 4.5 and Figure 4.6.



**Figure 4.5: Respondent Confidence 1**

Overall, most respondents believe that their organisations have a strong information security culture and that they themselves have a reasonable knowledge regarding security culture. It is however alarming to see that 36/113 (32%) of respondents are somewhat negative or unsure about their companies' information security culture (unsure/somewhat negative/severely pessimistic). There are also 28 respondents (25%) that do not have a strong knowledge about the information security culture topics discussed (unsure or worse). This demonstrates that there is scope for awareness raising programmes in organisations. Only 39 (34%) of respondents felt very confident about their knowledge level on the topics discussed. This confirms that this type of study is indeed necessary.



**Figure 4.6: Respondent Confidence 2**

This section described the demographical details of the respondents. Next the information security culture aspects will be discussed.

#### **4.1.2 Information Security Culture Aspects**

This section describes the responses for the questionnaire on the section pertaining to information security culture aspects and how important each aspect is. Most respondents completed all questions in this section. The data is summarised into paragraphs that display the number of responses for each identified aspect, the number of each importance rating (1 to 5, with 1 being not important and 5 being extremely important), as well as the average noted importance of each aspect. Bar graphs are used to display some of the results.

The results are split across four tables (Table 4.3 to table 4.6) to facilitate easier display of the data. The aspects in the tables are not sorted according to any values, but are presented according to the question number as they were included in the questionnaire. The rating that most respondents selected is highlighted and underlined for emphasis. After each table, there is a short discussion and a bar graph that supplements the data analysis presented in the tables.

Table 4.3 provides a summary of the first five information security culture aspects (Policy, Compliance, Managerial trust/Information security leadership, Education and training, and Information security awareness). Note that only the most responded to importance ratings have percentage shown. This is done for all aspect results.

Importance	1. Policy	2. Compliance	3. Managerial trust/ Information security leadership	4. Education and training	5. Information security awareness
1 (not important)	2	1	1	8	5
2 (somewhat important)	6	8	4	18	16
3 (important)	12	15	11	22	17
4 (very important)	39	41	41	<b><u>35 (31%)</u></b>	<b><u>42 (37%)</u></b>
5 (extremely important)	<b><u>54 (48%)</u></b>	<b><u>47 (42%)</u></b>	<b><u>55 (49%)</u></b>	30	33
Number of responses	113	112	112	113	113
<b>Average /5</b>	<b>4.21</b>	<b>4.12</b>	<b>4.29</b>	<b>3.54</b>	<b>3.73</b>

Table 4.3: Information Security Culture Aspects 1 to 5

From the table it is clear that Managerial trust/Information security leadership is regarded as the most important aspect by respondents - most respondents rated this aspect as very important and the aspect has a high average. A question raised by these results pertains to the lower rating of the Education and training aspect. Education and training is marked by 35 respondents as very important and by 30 respondents as extremely important. This may show towards the ignorance of the importance of awareness and training issues that are needed. Figure 4.7 shows the results for the Managerial trust/Information security leadership aspect.

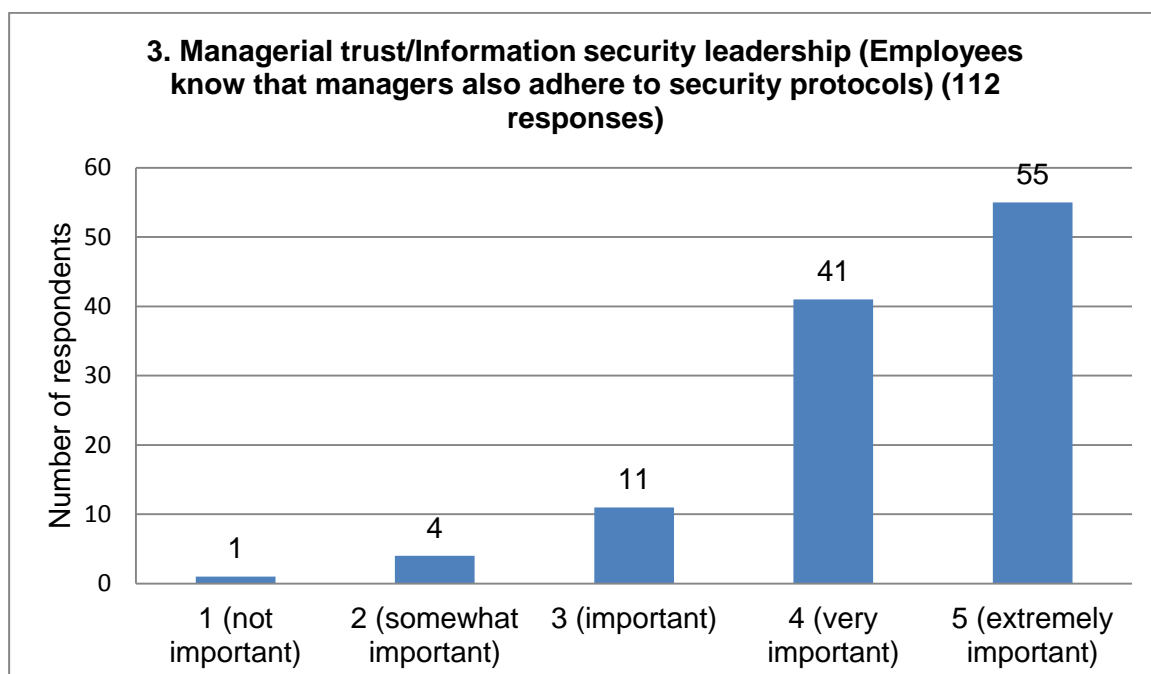


Figure 4.7: Managerial Trust/Information Security Leadership Responses

Figure 4.7 presents the responses for the question pertaining to the importance of managerial trust/information security leadership. Of the 112 respondents, 96 (86%) rated this aspect as either very important or extremely important. This indicates the necessity of leadership.

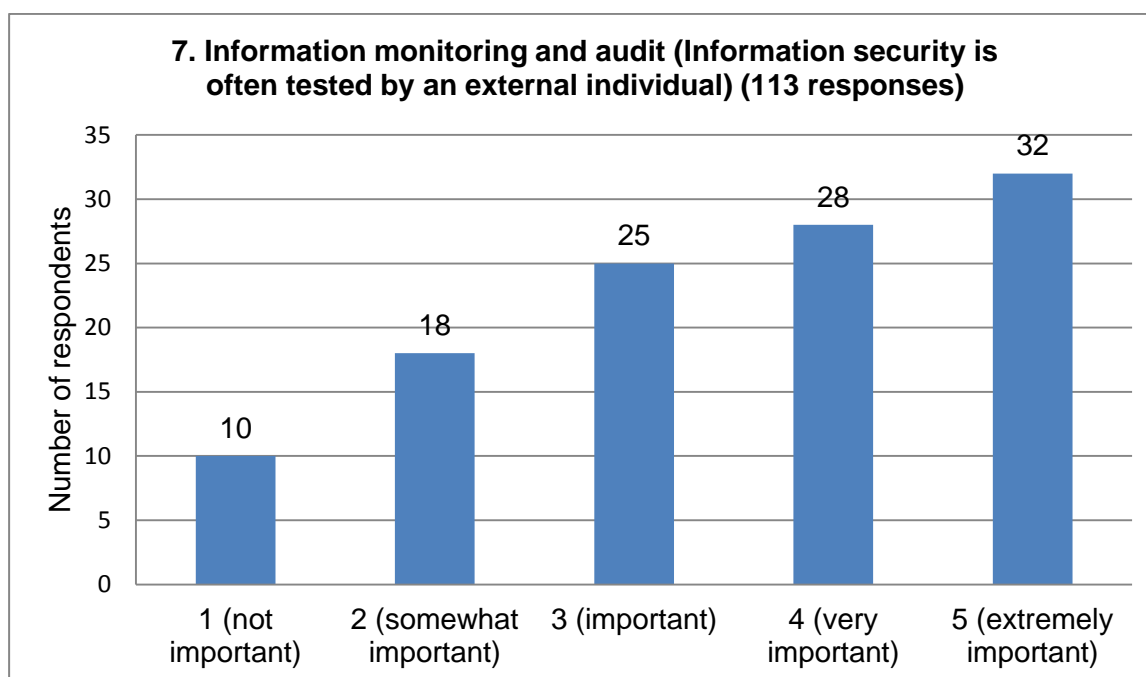
Table 4.4 presents the importance of the next five information security culture aspects.

Importance	6. Information asset management	7. Information monitoring and audit	8. Business continuity plan/ Incident management	9. Information security programme	10. Change management
1 (not important)	0	10	3	2	6
2 (somewhat important)	9	18	14	5	8
3 (important)	19	25	24	20	20
4 (very important)	40	28	<b><u>45 (40%)</u></b>	<b><u>43 (38%)</u></b>	<b><u>48 (42%)</u></b>
5 (extremely important)	<b><u>45 (40%)</u></b>	<b><u>32 (28%)</u></b>	27	42	31
Number of responses	113	113	113	112	113
Average /5	<b>4.07</b>	<b>3.48</b>	<b>3.70</b>	<b>4.05</b>	<b>3.8</b>

Table 4.4: Information Security Culture Aspects 6 to 10

According to the respondents, information monitoring and audit is the least important of all the aspects. The average of this aspect is 3.48 or 69.6%. Although monitoring and audit has one of the lowest average importance ratings, it still has the most (32 of 113) respondents providing it an importance rating of 5 (extremely important). Figure 4.8 displays the results for the Information monitoring and audit aspect.

It is interesting to note that the Information monitoring and audit aspect has the lowest average importance rating, although 54% of respondents rated it very or extremely important. When comparing it to the Managerial trust/Information security leadership aspect, it is obvious that respondents did not view monitoring and audit as significant. This does not indicate that it should be disregarded, but merely that other aspects are valued higher. Table 4.5 presents the information security culture aspects 11 to 16.

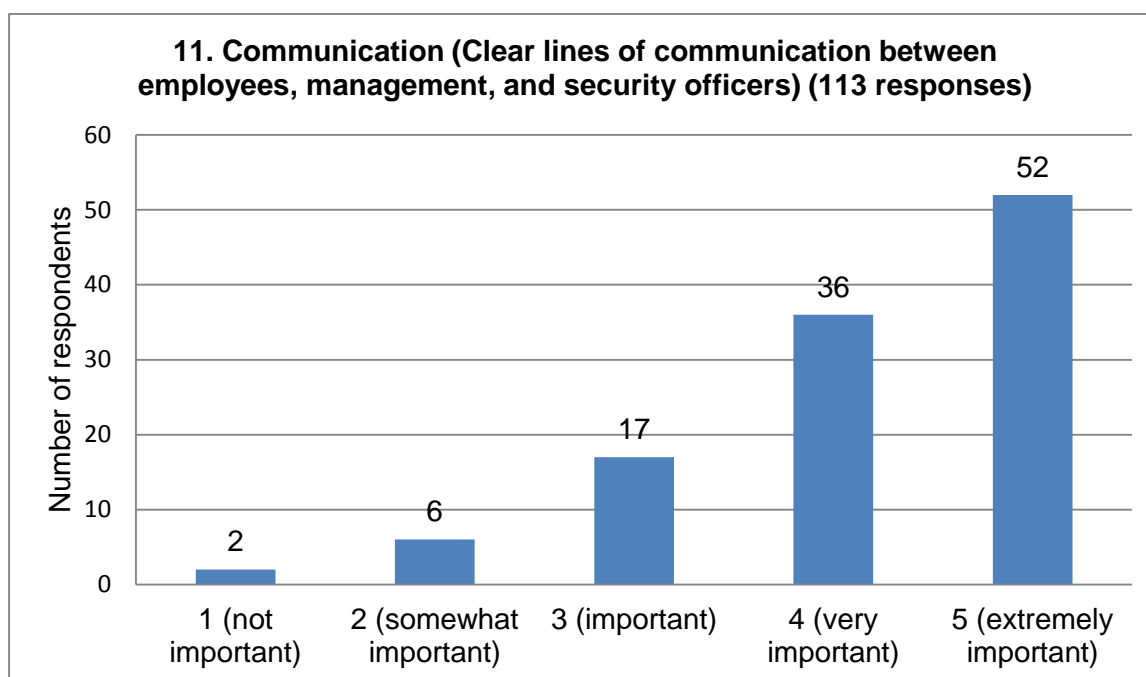


**Figure 4.8: Information Monitoring and Audit Responses**

Importance	11. Communication	12. Management's perspective	13. Strategy	14. Delegation of responsibility	15. Risk analysis	16. ROI
1 (not important)	2	5	1	1	2	8
2 (somewhat important)	6	7	10	8	11	18
3 (important)	17	17	27	13	18	25
4 (very important)	36	<b><u>47 (42%)</u></b>	<b><u>42 (37%)</u></b>	<b><u>51 (45%)</u></b>	<b><u>51 (45%)</u></b>	<b><u>34 (30%)</u></b>
5 (extremely important)	<b><u>52 (46%)</u></b>	36	33	40	31	28
Number of responses	113	112	113	113	113	113
<b>Average</b>	<b>4.15</b>	<b>3.91</b>	<b>3.85</b>	<b>4.07</b>	<b>3.87</b>	<b>3.5</b>

**Table 4.5: Information Security Culture Aspects 11 to 16**

The aspects depicted in Table 4.5 range from a relatively low importance (ROI) to somewhat high importance (Communication). Most of these aspects were rated as 4 (very important) by respondents, except for Communication which received mostly 5 (extremely important) ratings. The responses for the Communication aspect can be seen in Figure 4.9.



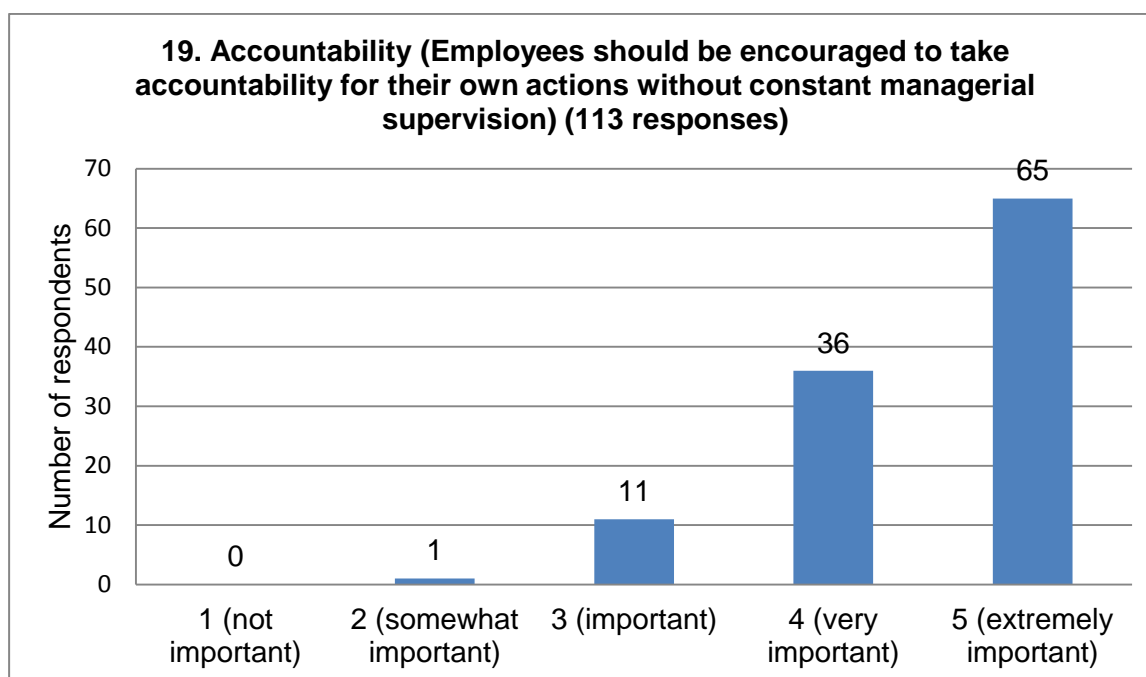
**Figure 4.9: Communication Responses**

The responses for the final five information security culture aspects can be seen in Table 4.6.

Importance	17. Legal and regulatory	18. Ethical conduct	19. Accountabili ty	20. Fairness towards employees	21. Fulfilment of personal needs of employees
1 (not important)	2	1	0	2	2
2 (somewhat important)	8	2	1	4	8
3 (important)	16	12	11	9	22
4 (very important)	36	32	36	51	<b><u>43 (38%)</u></b>
5 (extremely important)	<b><u>51 (45%)</u></b>	<b><u>66 (58%)</u></b>	<b><u>65 (58%)</u></b>	<b><u>47 (42%)</u></b>	38
Number of responses	113	113	113	113	113
<b>Average</b>	<b>4.12</b>	<b>4.42</b>	<b>4.46</b>	<b>4.21</b>	<b>3.95</b>

**Table 4.6: Information Security Culture Aspects 17 to 21**

The Accountability aspect was rated as the most important of all aspects in this grouping, with an average rating of 4.46 (89.2%). It is closely followed by the Ethical conduct aspect, with an average rating of 4.42 (88.4%). Both of these aspects had an overwhelming number of respondents rating them as extremely important. Figure 4.10 depicts the responses for accountability.



**Figure 4.10: Accountability Responses**

Not a single respondent rated the importance of accountability as 1 (not important). This is the only aspect where no respondent gave a rating of 1. Additionally, more than half of the respondents rated accountability as extremely important, with most the remaining respondents rating it as very important. From Figure 4.10 it is clear that the Accountability aspect is of utmost significance in an organisation's information security culture.

After the Likert-type questions, respondents were given the opportunity to add any aspects that they felt were missing from the questionnaire by responding to an open-ended question. This was not a compulsory field and only 18 respondents chose to answer the question. The responses can be seen in Table 4.7 along with the relevant interpretation of the responses.

Respondent Number	Are there any aspects not mentioned here that you believe is important? If yes, please name these aspects and give a rating to each of 1 (not important) to 5 (extremely important). *	Interpretation
R24	Management is generally too busy to properly focus on these aspects 5	Management's perspective (already in list)
R31	Everything that I can think of is covered.	List complete
R40	no	List complete
R42	IT audit performed by government (government to audit IT companies if they do abide to law of the land) extremely Important Software License (Do companies have software scan to identify unwanted and unlicensed software) extremely Important	Governmental audit 5 - information monitoring and audit Software licence 5 - legal and regulatory (both already in list)
R48	Your company's security policy can be the best in the industry, but employees also need to be aware of a	Social engineering (no number)



Respondent Number	Are there any aspects not mentioned here that you believe is important? If yes, please name these aspects and give a rating to each of 1 (not important) to 5 (extremely important). *	Interpretation
	form of hacking called 'Social Engineering'	
R53	No	List complete
R56	N/A	List complete
R66	Impact of recent breaches of data security 3	Impact of recent breaches 3
R70	productivity (4 very important) - information security measures, especially for access to shared resources electronically, should not be counterproductive. Research and other work methodologies are trending towards interdisciplinary and information security checks and balances should allow for secured ease of data flow without constant disruption during a work session. The use of repositories and other shared resources should be 'secured' within the system architecture before the end-user interface, and the continual scanning for IoT-threats should not negatively impact the workflow for the engaging employee	Productivity impediment 4 Technical background security (no number)
R84	Alignment of information management with local culture (5)	Local Culture 5
R85	none	List complete
R91	Trust between employees and managers = 2	Managerial trust/Information security leadership 2 (already in list)
R97	No	List complete
R98	no	List complete
R100	none	List complete
R102	Organisational security structure for civil departments (rating of 5)	Organisation type specific 5
R107	None	List complete
R110	no	List complete

**Table 4.7: Additional Information Security Culture Aspects**

\* Exact responses as given by questionnaire participants.

Most respondents chose not to complete this question. The interpretation for the non-completion of this question is that respondents could not think of additional aspects to add to the list of aspects presented to them. Of those that provided an answer to the open-ended question, 10 of the 18 respondents wrote “No”, “None” or “N/A” or indicated in some way that they are of the opinion that the list is complete. Three respondents named aspects that fit in with other aspects that are already in the list. The remaining comments are discussed below:

- R66: Impact of recent breaches 3 – This aspect can be included in a number of other aspects, but would be of little importance there.

- R70: Productivity impediment 4 – Losing productivity because of strict security procedures. This respondent believes that most security procedures should be a technical aspect and run without the knowledge of the employees.
- R84: Local culture 5 – The respondent that provided this feedback mentioned local culture in other comments as well. He believes that the identified aspects do not fit an organisation with an African culture and that an organisation creating a security culture should take into consideration the local culture.
- R102: Organisation type specific 5 - This is similar to the previous comment in that the security culture can depend on the local culture or, in this case, the type of organisation.

At the end of each section of the questionnaire, respondents were asked to provide feedback and comments. The feedback and comments are discussed in the next section of this chapter. The final list of information security culture aspects is sorted according to importance from the most important to the least important (according to the respondent ratings) in Table 4.8.

Information security culture aspect	Average /5	Importance (%)
19. Accountability	4.46	89.2%
18. Ethical Conduct	4.42	88.3%
3. Managerial trust/Information security leadership	4.29	85.8%
1. Policy	4.21	84.2%
20. Fairness towards employees	4.21	84.2%
11. Communication	4.15	83.0%
2. Compliance	4.12	82.3%
17. Legal and Regulatory	4.12	82.3%
6. Information asset management	4.07	81.4%
14. Delegation of responsibility	4.07	81.4%
9. Information security programme	4.05	81.0%
21. Fulfilment of personal needs of employee	3.95	78.9%
12. Managements perspective	3.91	78.2%
15. Risk analysis	3.87	77.3%
13. Strategy	3.85	76.9%
10. Change management	3.80	75.9%
5. Information security awareness	3.73	74.5%
8. Business continuity plan/Incident management	3.70	73.9%
4. Education and training	3.54	70.8%
16. ROI	3.50	69.9%
7. Information monitoring and audit	3.48	69.5%
Added comments: <ul style="list-style-type: none"> <li>• Impact of recent breaches</li> <li>• Productivity impediment</li> <li>• Local culture</li> <li>• Organisation type</li> </ul>		

**Table 4.8: Culture Aspects Rated According to Importance**

Although some aspects are rated as more significant than others, it is important to note that all information security culture aspects are vital. This study aims to determine how important each aspect is, but even the least important aspects should never be absent in any information security culture. The importance of the identified aspects ranges from 69.6% to 89.2%. Organisations can use this data to compare how strong their information security culture is based on this information. The data is analysed further in Section 4.2.

This section described the results of the information security culture aspects. The next section presents the awareness and training delivery methods.

#### 4.1.3 Awareness and Training Delivery Methods

This section of the questionnaire asked respondents to select one of five delivery methods presented for each identified information security culture aspect. The results of the responses to this section will be summarised in table format, with supporting figures describing the data. Table 4.9 provides a short key for each of the awareness and training delivery methods presented to the respondents. The same key is used throughout the section on delivery methods in order to display the information more efficiently and neatly.

Awareness and training delivery methods	Key
Formal training sessions (examples include instructor led sessions and seminars etc.)	1 - Formal
Informal training ("brown bag" seminars, web-based instructor-led training etc.)	2 - Informal
Short messages around the office (posters, desk-to-desk alerts, checklists etc.)	3 - Short
Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)	4 - Computer
Other (award programmes, security related events, videos etc.)	5 - Other

**Table 4.9: Delivery Methods Key**

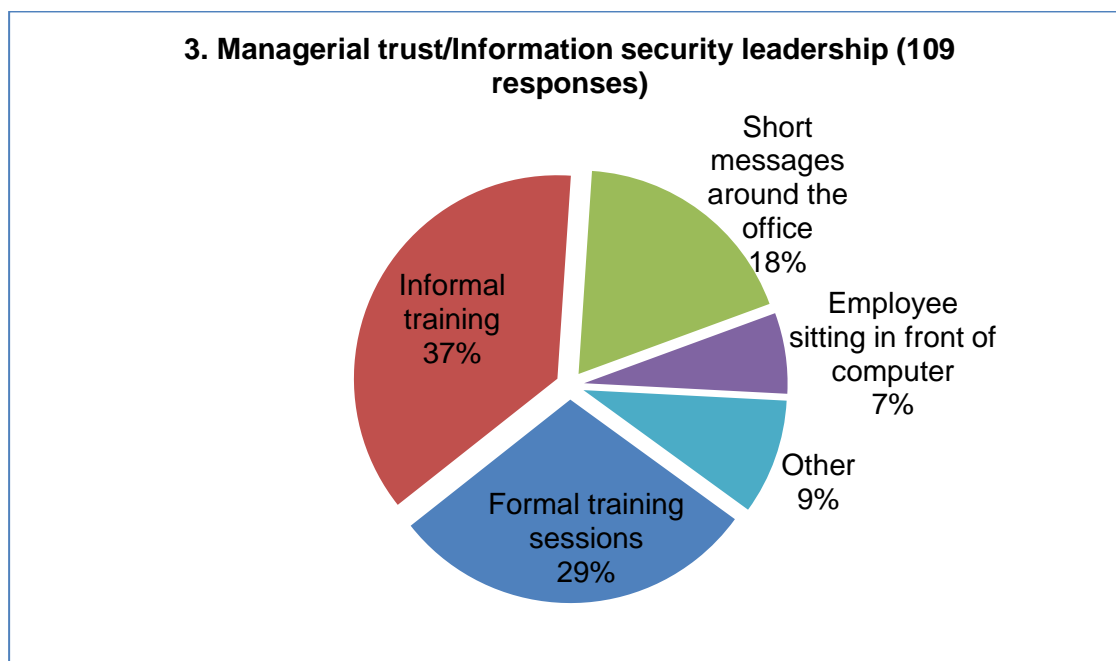
Data is displayed in a similar fashion to the previous section. The data is split across four tables (Table 4.10 to Table 4.13) to facilitate easier display of the data. The aspects in the tables are not sorted according to any values, but are presented according to the question number as they were included in the questionnaire. The rating that most respondents selected is highlighted and underlined for emphasis. After each table, there is a short discussion and a pie graph that supplements the data analysis presented in the tables. Not all questions were answered by all respondents.

Table 4.10 provides the preferred delivery methods for the first five aspects.

Delivery Method Number	1. Policy	2. Compliance	3. Managerial trust/ Information security leadership	4. Education and training	5. Information security awareness
1 - Formal	<b><u>41 (37%)</u></b>	33	32	<b><u>53 (48%)</u></b>	22
2 - Informal	29	<b><u>41 (36%)</u></b>	<b><u>40 (37%)</u></b>	30	<b><u>42 (38%)</u></b>
3 - Short	25	20	20	5	33
4 - Computer	12	14	7	18	10
5 - Other	6	5	10	5	4

**Table 4.10: Awareness and Training Delivery Methods for Aspects 1 to 5**

Delivery method 1 (Formal training sessions) and 2 (Informal training) received a lot more responses than the other delivery methods. This trend is seen throughout the responses, with delivery method 5 (Other) the least preferred. Figure 4.11 presents the data in graph-format for the third information security culture aspect.



**Figure 4.11: Delivery Methods for Managerial Trust/Information Security Leadership**

Table 4.11 presents the results regarding the preferred delivery methods for the next five information security culture aspects.

For this aspect grouping, delivery methods 1 and 2 are again most favoured by the respondent, with the remaining delivery methods sharing lower values. Delivery method 5 (Other) is especially unpopular. Respondents indicated a major preference towards formal training (49.5%) in terms of the Business continuity plan/Incident management aspect. The detailed results for information monitoring and audit can be seen in Figure 4.12.

Delivery Method Number	6. Information asset management	7. Information monitoring and audit	8. Business continuity plan/Incident management	9. Information security programme	10. Change management
1 - Formal	26	<u>40 (37%)</u>	<u>54 (49%)</u>	<u>42 (38%)</u>	27
2 - Informal	<u>40 (38%)</u>	31	24	35	<u>46 (42%)</u>
3 - Short	23	15	15	12	18
4 - Computer	10	13	8	17	10
5 - Other	7	7	8	5	10

Table 4.11: Awareness and Training Delivery Methods for Aspects 6 to 10

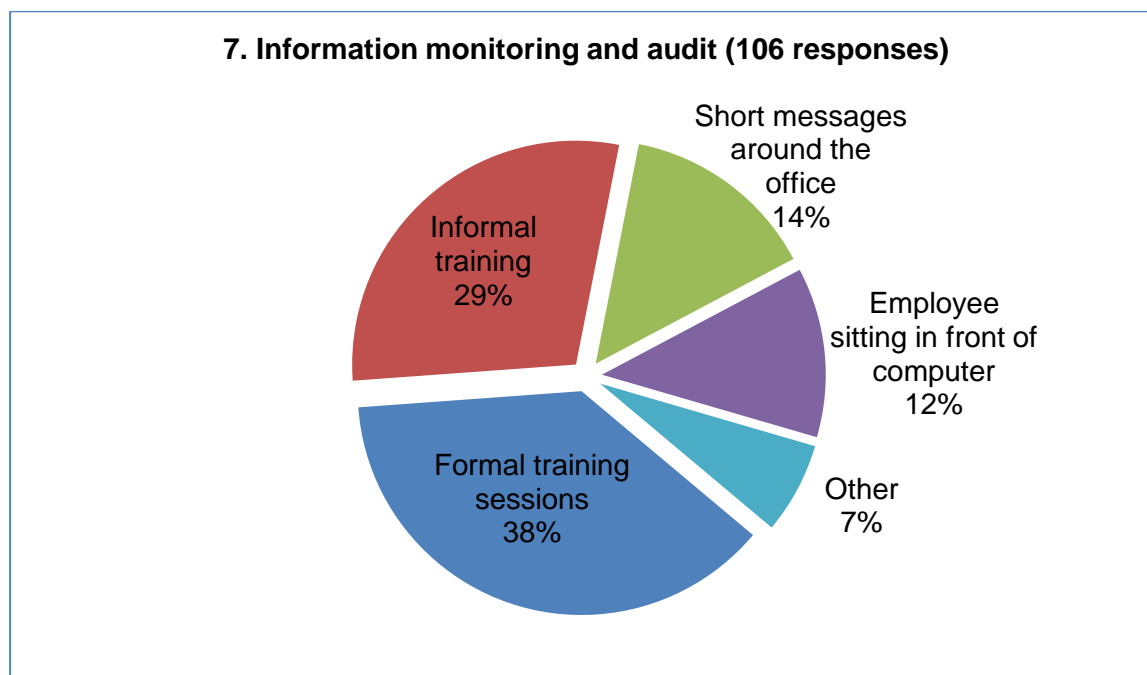


Figure 4.12: Delivery Methods for Information Monitoring and Audit

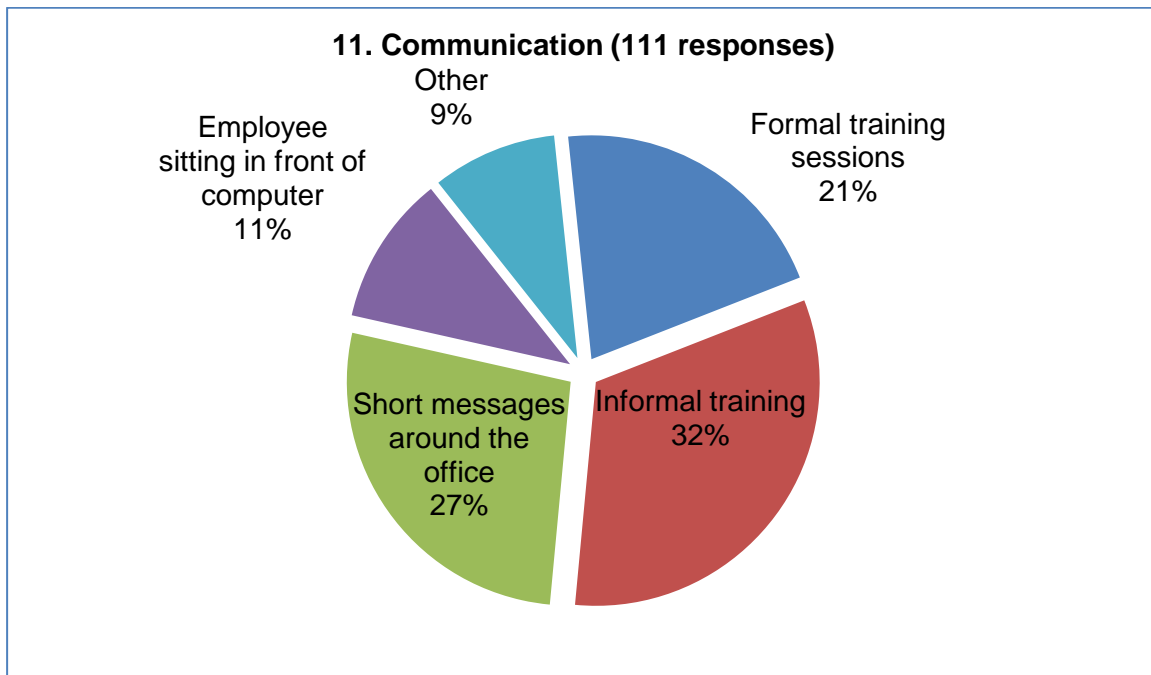
The delivery methods for the next six information security culture aspects are shown in Table 4.12.

Delivery Method Number	11. Communication	12. Management's perspective	13. Strategy	14. Delegation of responsibility	15. Risk analysis	16. ROI
1 - Formal	23	28	<u>45 (41%)</u>	<u>44 (42%)</u>	<u>49 (45%)</u>	<u>39 (36%)</u>
2 - Informal	<u>36 (32%)</u>	<u>39 (36%)</u>	34	31	37	35
3 - Short	30	23	16	17	13	13
4 - Computer	12	9	7	6	8	6
5 - Other	10	9	6	9	2	17

Table 4.12: Awareness and Training Delivery Methods for Aspects 11 to 16

These aspects follow the pattern where either delivery method 1 (Formal training) or delivery method 2 (Informal training) are selected most by respondents. Delivery method 5 (Other) is

generally selected the least number of times, although respondents selected this delivery method 17 times in relation to ROI – this reflects the most responses for this delivery method. The preferred delivery methods for the communication aspect can be seen in Figure 4.13.



**Figure 4.13: Delivery Methods for Communication**

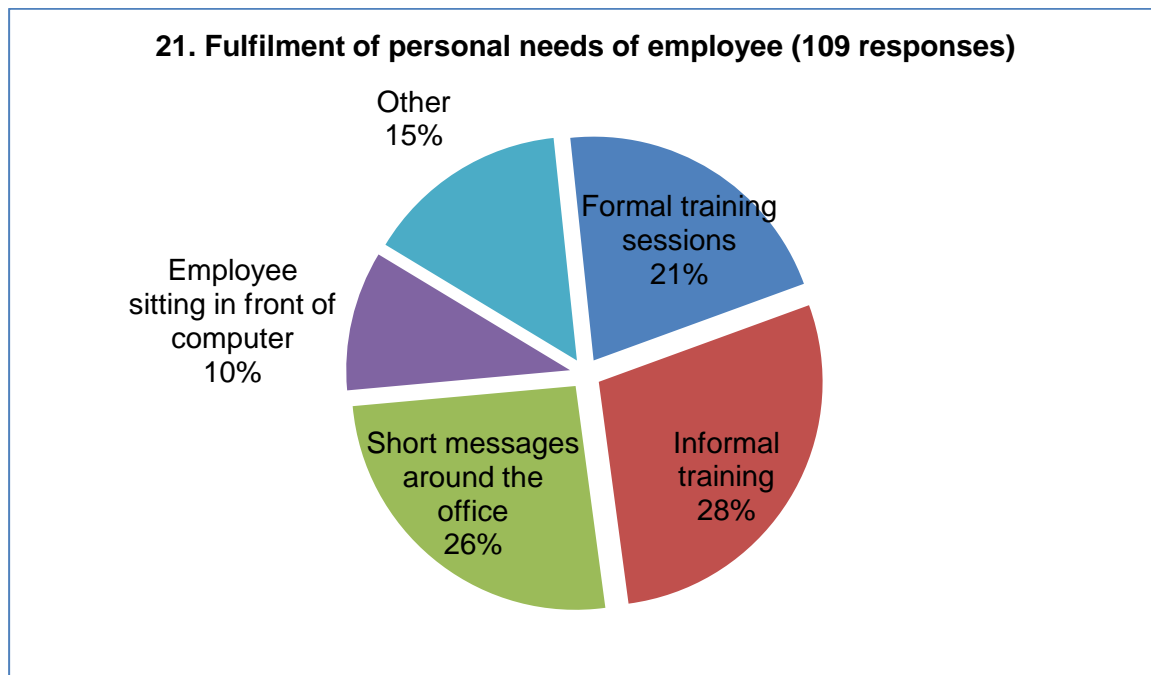
Communication requires a balance between the delivery methods, with special emphasis on informal training and short messages around the office. There are a few information security culture aspects where formal training is not selected as one of the two most preferred delivery methods. In this regard, the Communication (aspect 11) and Fulfilment of personal needs of employee (aspect 21) are unique in sharing this characteristic.

Table 4.13 presents the result for the delivery methods for the remaining five information security culture aspects.

Delivery Method Number	17. Legal and regulatory	18. Ethical Conduct	19. Accountability	20. Fairness towards employees	21. Fulfilment of personal needs of employee
1 - Formal	<b><u>49 (44%)</u></b>	<b><u>38 (35%)</u></b>	<b><u>41 (39%)</u></b>	26	23
2 - Informal	30	<b><u>38</u></b>	30	<b><u>40 (37%)</u></b>	<b><u>31 (29%)</u></b>
3 - Short	15	20	24	22	28
4 - Computer	10	9	7	12	11
5 - Other	6	7	5	11	16

**Table 4.13: Awareness and Training Delivery Methods for Aspects 16 to 21**

Fulfilment of personal needs of employee is one of the aspects that are balanced in terms of preferred delivery methods selected by respondents. A mixed method would be ideal in providing awareness and training for this aspect. It is recommended that the final method selected to address this aspect would depend on the size of organisation, type of organisation, location, personal preferences of management/employees, and a number of other factors. This study can only indicate the preferred delivery methods in general and does not have enough data for specific organisation types, sizes etc. Figure 4.14 provides the detailed responses for the fulfilment of personal needs of employee aspect.



**Figure 4.14: Delivery Methods for Fulfilment of Personal Needs of Employee**

Throughout the section on delivery methods, most questions were not answered by all respondents. Possible reasons for this include respondents accidentally skipping a question, respondents being uncertain on their delivery method preference, or respondents not understanding the question.

The data presented in this section shows that, although there are preferred delivery methods for specific information security culture aspects, using a mixed method based on the organisation type and other preferences would be suggested.

Respondents were also asked to identify delivery methods that were not already listed by the questionnaire. This is similar to the previous open-ended question used for the identification of additional information security culture aspects. Table 4.14 presents the responses to this question, as well as the interpretations thereof.

<b>Respondent Number</b>	<b>Are there any delivery methods not mentioned here that you believe is important? If yes, please name them and supply the number of the aspects (1-21) you would improve using them.</b>	<b>Interpretation</b>
R8	face to face 2 21	Face-to-face 2,21
R19	No	List complete
R24	One can have a combination of formal training and short regular eye-catching messages/popups as reminders for critical aspects, with a rewards system thrown into it for conformance to the requirements.	Combination
R40	Yes. Mass emails can be very helpful and informative in an organisation. 3,11,12,16,20	Mass emails 3,11,12,16,20
R43	Email alerts help reinforce training and create awareness around various issues	Email alerts
R53	NO	List complete
R56	N/A	List complete
R66	No	List complete
R70	A combination of delivery methods	Combination
R76	Some of the answers for some of the questions were difficult to relate	
R77	x	List complete
R81	One on one conversations, building the culture. 2,3,5,10,11,18,19,21	Face-to-face 2,3,5,10,11,18,19,21
R83	In a small start-up company none of your options really exist -there is no capacity. Information security is something that appears in all team sessions, it is an inherent part of the culture and because of such a small group, formal training & reward is not required. Info security is the lifeblood of a small org - employees buy in to that concept and guard it. Also the level of employee in a small company is typically less diverse - most of the employees are hired because they can work independently and has a deep understanding of and responsibility towards making the company work.	Group discussion (small companies)
R84	None of the delivery methods is applicable in a rural area. The way to discuss issues is to sit together, discuss together, and come to 'ways ahead' together. Any aspect of any activity can only flourish when all are involved (the Ubuntu way).	Group discussion (rural)
R85	none	List complete
R86	personal coaching	Face-to-face
R91	Stakeholder involvement	Stakeholder involvement
R93	Sometimes multiple methods are used - selecting just one answer has made me pick the most prevalent.	Combination
R100	none	List complete
R110	no	List complete

**Table 4.14: Additional Awareness and Training Delivery Methods**

\* Exact responses as given by questionnaire participants.



There were 20 respondents who answered this question. Of those respondents, eight responded with “No”, “None”, “x” or “N/A”. One respondent stated that some questions are difficult to relate to. A summary of the other mentioned methods and comments are:

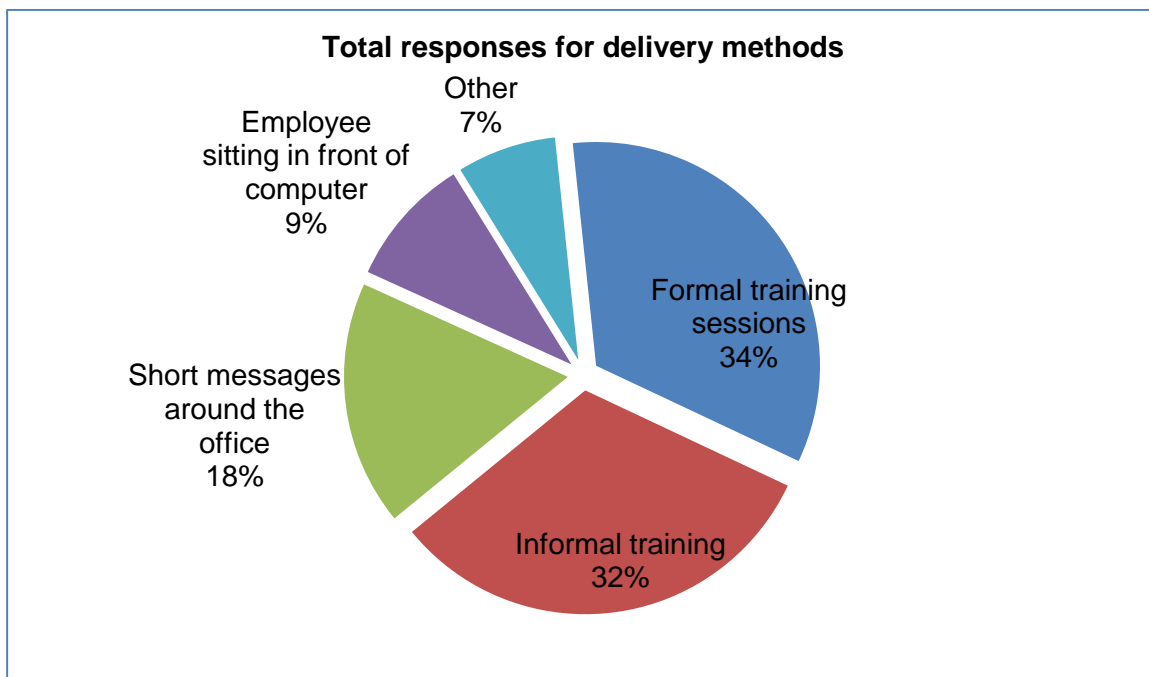
- R8, R81, R86: Face-to-face. This is where an employee and trainer have a personal training session. This can be in a formal or informal setting. This can be used for the following information security culture aspects: 2,3,5,10,11,18,19,21.
- R24, R70, R93: A combination of delivery methods.
- R40, R43: Regular email alerts sent to employees in specific department or all employees in the organisation. The email can remind employees of standard security procedures or introduce new topics.
- R83, R84: Group discussion as a formal or informal event. Team sessions are regular in any case and can be a great opportunity to build and reinforce security culture.
- R91: Stakeholder involvement. It is not argued that stakeholder involvement is important; merely that it is not a delivery method. Stakeholder involvement can be seen as an additional information security culture aspect.

When comparing the total responses for each delivery method, it is clear that delivery methods 1 and 2 are most preferred by respondents. Table 4.15 presents the delivery methods and the total number of times each that each method was selected.

<b>Delivery method</b>	<b>Total number</b>
1. Formal training sessions (examples include instructor led sessions and seminars etc.)	775
2. Informal training ("brown bag" seminars, web-based instructor-led training etc.)	739
3. Short messages around the office (posters, desk-to-desk alerts, checklists etc.)	407
4. Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)	216
5. Other (award programmes, security related events, videos etc.)	165

**Table 4.15: Total Responses Regarding Delivery Method**

Based on the data in Table 4.15, it is obvious that both formal training and informal training are preferred (high preference) by respondents, with short messages having a medium preference and sitting in front of a computer and other methods having a low preference. This is also depicted in Figure 4.15.



**Figure 4.15: Total Responses for Delivery Methods**

The responses indicating that a combination of delivery methods could be used are very valuable. The above data can be used to determine how much of each delivery method should be included in the mixed method training. This section discussed the awareness and training delivery methods. The next section describes the import topics of awareness and training programmes. The data presented will be used to create the framework in Chapter 5.

#### **4.1.4 Important Topics of Information Security Awareness and Training Programmes**

This section describes the important topics that should be included in an information security awareness and training programme regarding information security culture. Respondents rated each topic between 1 (not important) and 5 (extremely important). The data is split across three tables (Table 4.16 to Table 4.18) to facilitate easier display of the data. After each table, there is a short discussion and a bar graph that supplements the data analysis presented in the tables. The topics were mostly rated by respondents at an importance of 4 or 5, and ranges from 3.73 to 4.63 out of 5. The first six responses are presented in Table 4.16.

Most respondents rated all topics as 5 (very important). Topics related to anti-virus programs were rated as most important for all employees to be aware of and understand, while the use of pop-up blockers is rated as less important by respondents. Figure 4.16 represents the responses for the need to understand an anti-virus program.

Importance	1. Understand the need of an anti-virus programme	2. Understand the need of updating virus definitions	3. Regularly scan a computer and storage devices	4. Use a personal firewall	5. Install software patches	6. Use pop- up blockers
1 (not important)	1	2	2	6	2	5
2 (somewhat important)	3	1	2	5	7	6
3 (important)	8	8	22	13	14	25
4 (very important)	25	27	24	32	35	30
5 (extremely important)	<b><u>76 (67%)</u></b>	<b><u>75 (66%)</u></b>	<b><u>63 (55%)</u></b>	<b><u>55 (49%)</u></b>	<b><u>55 (48%)</u></b>	<b><u>47 (42%)</u></b>
Number of responses	113	113	113	111	113	113
Average /5	<b>4.52</b>	<b>4.52</b>	<b>4.27</b>	<b>4.13</b>	<b>4.19</b>	<b>3.95</b>

Table 4.16: Responses for Important Topics 1 to 6

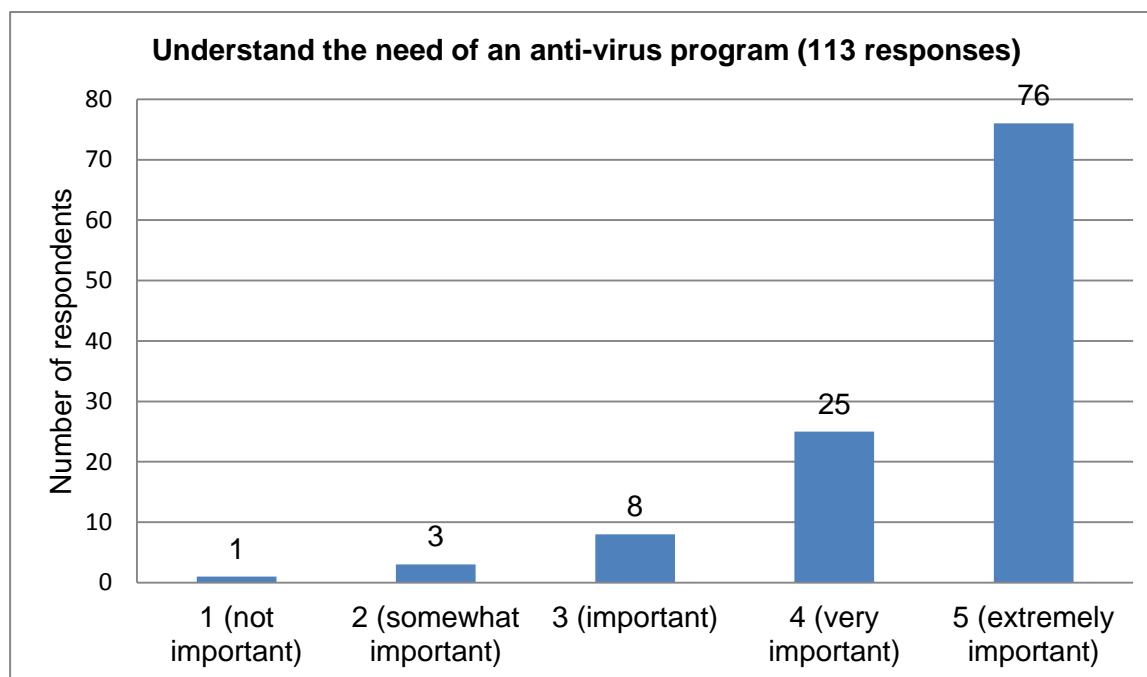


Figure 4.16: Response for Important Topic 1

A large majority of respondents (89%) rated the importance of understanding the need of an anti-virus program as very or extremely important. It is clear from Figure 29 that the topic pertaining to an anti-virus program is vital to information security culture. When comparing the average rating of each important topic, the resulting average importance rating for all important topics is 4.22/5 or 84.3%. Table 4.16 presents the next six delivery method responses.

Importance	7. Understand the risk of downloadin g programs or files	8. Understan d the risks of P2P file sharing	9. Understand the risk of clicking on e-mail links	10. Understand the risk of e-mailing passwords	11. Understand the risk of e- mail attachments	12. Regularly backup important files
1 (not important)	0	2	1	2	0	3
2 (somewhat important)	3	7	3	2	8	3
3 (important)	7	18	18	4	14	7
4 (very important)	35	37	23	20	30	24
5 (extremely important)	<b><u>66 (60%)</u></b>	<b><u>50(44%)</u></b>	<b><u>69 (61%)</u></b>	<b><u>86 (75%)</u></b>	<b><u>62 (54%)</u></b>	<b><u>77 (68%)</u></b>
Number of responses	111	113	113	113	113	113
<b>Average /5</b>	<b>4.48</b>	<b>4.10</b>	<b>4.36</b>	<b>4.63</b>	<b>4.27</b>	<b>4.48</b>

Table 4.17: Responses for Important Topics 7 to 12

Most respondents completed most answers for this topic grouping. Once again the majority of respondents rated each topic as extremely important. The risk of emailing passwords was the topic rated as most important of all topics provided in this grouping. The results for this topic can be seen in Figure 4.17.

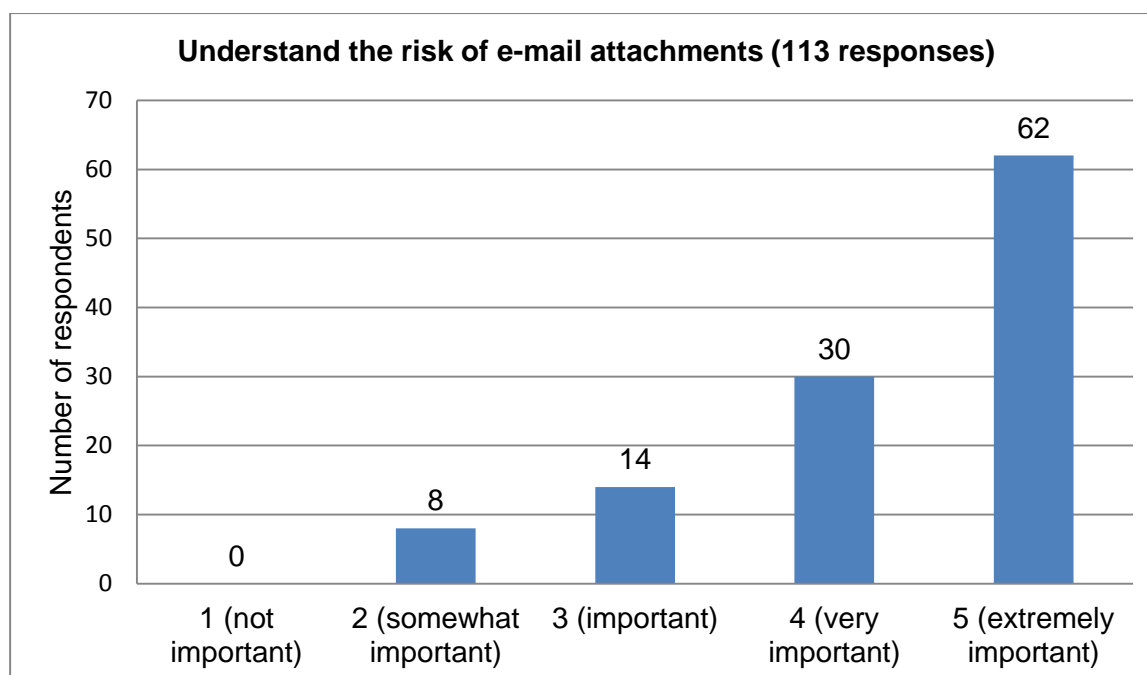


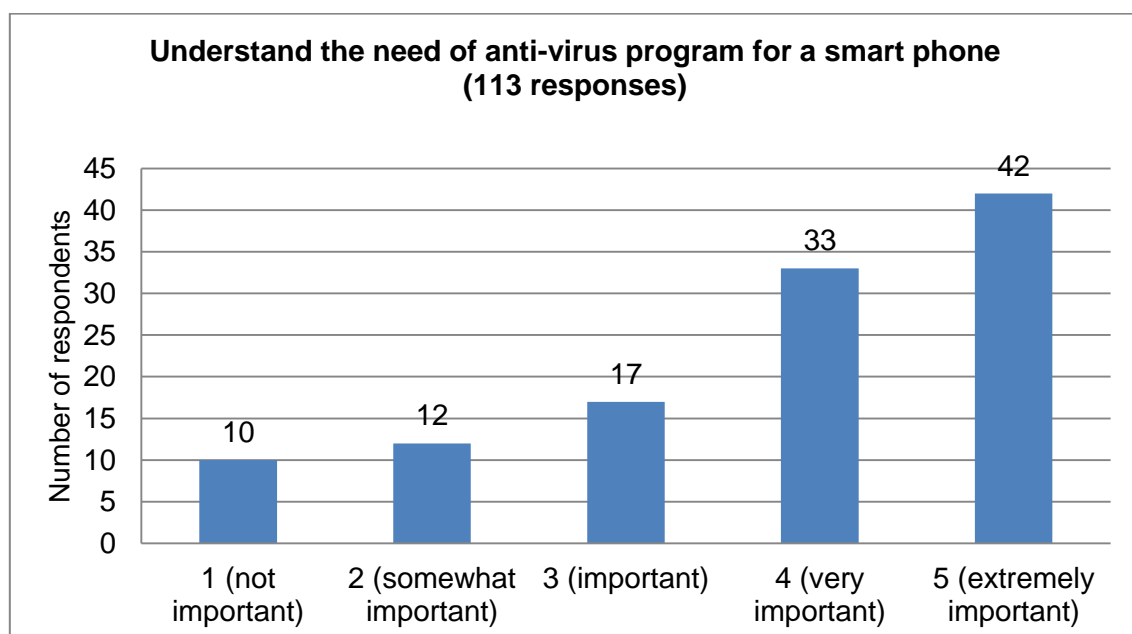
Figure 4.17: Response for Important Topic 11

From Figure 30 it is obvious that most respondents rated the risk of emailing passwords as extremely important, indicating that it is an essential topic. Majority of respondents (93%) rated this topic as very or extremely important. The last grouping of important topics on average is rated lower than the others. These topics are presented in Table 4.18.

Importance	13. Understand the risk of smartphone viruses	14. Understand the need of anti-virus program for a smart phone	15. Know the characteris tics of a strong password	16. Use different passwords for different systems	17. Change passwords regularly	18. Understand legal, regulatory and ethical issues of information security
1 (not important)	9	10	2	6	6	1
2 (somewhat important)	8	12	4	6	8	7
3 (important)	23	17	8	14	21	21
4 (very important)	31	33	33	35	30	36
5 (extremely important)	<b><u>42 (37%)</u></b>	<b><u>42 (37%)</u></b>	<b><u>66 (58%)</u></b>	<b><u>52 (46%)</u></b>	<b><u>47 (42%)</u></b>	<b><u>48 (42%)</u></b>
Number of responses	112	113	113	113	112	113
<b>Average /5</b>	<b>3.78</b>	<b>3.73</b>	<b>4.39</b>	<b>4.07</b>	<b>3.93</b>	<b>4.09</b>

**Table 4.18: Responses for Important Topics 13 to 18**

The topic pertaining to the importance for employees to understand the need of an anti-virus program for a smart phone was rated as the least important of all the identified topics. Other topics related to smartphone viruses were also rated very low. Despite this lower rating, the majority of respondents rated all topics identified as very important in terms of information security culture. The responses for understanding the need of an anti-virus program for a smart phone are presented in Figure 4.18.



**Figure 4.18: Response for Important Topic 14**

Topics related to smartphone viruses had the most 1 (not important) ratings. This might indicate that respondents are not aware of mobile threats. For this topic, the ratings provided by respondents were divided between all importance ratings, whereas results for most other topics

only presented ratings in a select number of importance ratings. This may indicate that a variety of perceptions exist among the respondents on this topic.

Respondents were asked if there are other topics that were not included in the questionnaire. Twelve respondents provided feedback on this open-ended question. The responses are presented in Table 4.19.

<b>Respondent Number</b>	<b>Are there any topics not mentioned here that you believe is important? If yes, please name these topics and give a rating to each of 1 (not important) to 5 (extremely important).</b>	<b>Interpretation</b>
R8	ransomware 5	Ransomware 5
R19	No	List complete
R24	None	List complete
R35	To know the vulnerability of smartphones in terms of security breaches. Smartphones are more easily accessible by 'criminals' than a desktop or laptop computer. Most smartphone users doesn't even have password protection on their lock screen, but mostly email accounts and documents can be accessed via someone's smartphone.	Mobile devices security
R40	No	List complete
R43	Physical security of mobile devices. Encryption as employed in the organisation. Clear desk policy. Use of cloud computing/file storage and USB.	Mobile devices Encryption Clear desk policy File storage
R53	No	List complete
R66	No	List complete
R81	My employees get trained on a different system and get exposed to dealing with better security out of principle, by being introduced to the Debian system, TOR, and related systems, rather than sticky tape over symptoms.	Has good security
R84	Knowing who to ask for mentoring and guidance in these aspects (5)	Mentoring and guidance 5
R93	Many workplaces do development (even where that is not the main role) and developers need security awareness of a different kind.	Security for developers
R103	All is important. As new attacks arise new aspects must be addressed.	New aspects with new attacks

**Table 4.19: Additional Important Awareness and Training Programme Topics**

\* Exact responses as given by questionnaire participants.

Of the 12 respondents who answered this question, five responded with “No” or “None”, indicating that they cannot think of other important topics that should be included in an awareness and training programme. Some of the other comments were not interpreted as additional topics, but rather as general comments. These responses are:

- R8: Ransomware 5 (very important) – This is a type of malware that restricts access to an information systems resources until a sum of money has been paid to “release” the resource.
- R35, R43: Mobile device security – Password protected lock screens, unsecure documents on phone, physical security of mobile devices etc. The inclusion of this comment is interesting considering topics pertaining to passwords for mobile devices were not rated as an extremely important topic. One possible reason for this is that some organisations/respondents often use smartphones for work-related tasks while others do not.
- R43: Encryption – Encrypting important documents throughout an entire organisation helps prevent unauthorised access.
- R43: Clear desk policy – This is another method to prevent unauthorised access; by keeping desks clear, stealing information becomes more difficult. It also creates a more professional and neat work environment.
- R43: File storage – There are various methods that can be utilised by employees to store important documents, including the use of personal USB drives, cloud storage or a company server. Each organisation must decide which method is best suited to the organisation and ensure that employees are trained to use the system and any relevant security protocols.
- R81: This respondent believes that employees should receive in-depth security training and that his organisation has a strong security culture.
- R84: Mentoring and guidance 5 (very important) – This is more of an information security culture aspect and fits in with Managerial trust/Information security leadership.
- R93: Security for developers – Programmers and developers have to be aware of more specific security issues and must be trained to integrate security measures into applications that they create. This is also not a specific topic, but rather an important comment.
- R103: New aspects with new attacks – This is another comment stating that with each new threat to the organisations information; new topics should be added to the training and awareness programme to fight these threats.

Each organisation must decide for itself which topics to add to this list. The important topics are sorted from most important to least important (according to the respondents) in Table 4.20.

Information security topic	Average /5	Importance (%)
10. Understand the risk of e-mailing passwords	4.63	92.57%
1. Understand the need of an anti-virus program	4.52	90.44%
2. Understand the need of updating virus definitions	4.52	90.44%
12. Regularly backup important files	4.48	89.56%
7. Understand the risk of downloading programs or files	4.48	89.55%
15. Know the characteristics of a strong password	4.39	87.79%
9. Understand the risk of clicking on e-mail links	4.36	87.26%
3. Regularly scan a computer and storage devices	4.27	85.49%
11. Understand the risk of e-mail attachments	4.27	85.49%
5. Install software patches	4.19	83.72%
4. Use a personal firewall	4.13	82.52%
8. Understand the risks of P2P file sharing	4.10	81.95%
18. Understand legal, regulatory and ethical issues of information security	4.09	81.77%
16. Use different passwords for different systems	4.07	81.42%
6. Use pop-up blockers	3.95	78.93%
17. Change passwords regularly	3.93	78.57%
13. Understand the risk of smartphone viruses	3.78	75.54%
14. Understand the need of anti-virus program for a smart phone	3.73	74.69%
Additional comments: <ul style="list-style-type: none"> <li>• Ransomware</li> <li>• Mobile devices security</li> <li>• Encryption</li> <li>• Clear desk policy</li> <li>• File storage</li> </ul>		

**Table 4.20: Important Topics Rated According to Importance**

Even the least important topic is still very important with a rating of 74.69% as rated by the respondents. Five additional topics were identified by respondents that could be included in an awareness and training programme.

This section discussed the data received from the respondents on important topics. The next section is the data analysis and describes how the data was analysed and which statistical methods were used.

## 4.2 Data Analysis

The previous section provided the results from the online questionnaire. This section describes how the data was analysed to find correlations and describes how the framework was created. It is divided into the same sections as the questionnaire results (demographical details, information security culture aspects, awareness and training delivery methods, and important topics of awareness and training programmes).



The first section describes the demographical data and how it was analysed.

#### 4.2.1 Demographics Inferential Statistics

Several statistical methods were used to find correlations and significant facts for the demographical details. These tests are described as subsections of this chapter. The first test used was the t-test.

##### 4.2.1.1 T-Test

The t-test is used to compare the difference between two population means to examine whether the two groups differ. The larger the difference between the two means, the clearer difference can be seen between the groups (Field, 2013). The test was run on several demographical details. The first test results are shown for all information security culture aspects in Table 4.21. The other results shown in later tables are only those with statistical significance.

Table 4.21 presents the t-test for information security culture aspects (ISCA) with regard to the **gender** of the respondents indicating effects sizes.

Information Security Culture aspect	Gender	N	Mean	Std. deviation	Std. error mean	Effect size
ISCA1 - Policy	Female	36	4.14	1.073	.179	0.10
	Male	77	4.25	.905	.103	
ISCA2 - Compliance	Female	35	4.14	.912	.154	0.04
	Male	77	4.10	.981	.112	
ISCA3 - Managerial trust/Information security leadership	Female	36	4.28	.944	.157	0.03
	Male	76	4.30	.817	.094	
ISCA4 - Education and training	Female	36	3.81	1.191	.198	0.31
	Male	77	3.42	1.250	.142	
ISCA5 - Information security awareness	Female	36	3.83	1.183	.197	0.13
	Male	77	3.68	1.152	.131	
ISCA6 - Information asset management	Female	36	4.14	.990	.165	0.10
	Male	77	4.04	.924	.105	
ISCA7 - Information monitoring and audit	Female	36	3.78	1.245	.207	0.34
	Male	77	3.34	1.304	.149	
ISCA8 - Business continuity plan/incident management	Female	36	3.72	1.137	.189	0.03
	Male	77	3.69	1.016	.116	
ISCA9 - Information security programme	Female	36	4.11	.950	.158	0.09
	Male	76	4.03	.952	.109	
ISCA10 - Change management	Female	36	3.83	1.134	.189	0.05
	Male	77	3.78	1.071	.122	
ISCA11 - Communication	Female	36	4.11	1.166	.194	0.05
	Male	77	4.17	.894	.102	

Information Security Culture aspect	Gender	N	Mean	Std. deviation	Std. error mean	Effect size
ISCA12 - Management's perspective	Female	35	3.86	1.061	.179	0.07
	Male	77	3.94	1.068	.122	
ISCA13 - Strategy	Female	36	4.08	.841	.140	0.34
	Male	77	3.74	1.018	.116	
ISCA14 - Delegation of responsibility	Female	36	4.17	1.000	.167	0.14
	Male	77	4.03	.873	.100	
ISCA15 - Risk analysis	Female	36	3.94	.984	.164	0.11
	Male	77	3.83	.992	.113	
ISCA16 - ROI	Female	36	3.47	1.276	.213	0.03
	Male	77	3.51	1.210	.138	
ISCA17 - Legal and regulatory	Female	36	4.17	.910	.152	0.07
	Male	77	4.09	1.066	.121	
ISCA18 - Ethical conduct	Female	36	4.47	.845	.141	0.10
	Male	77	4.39	.814	.093	
ISCA19 - Accountability	Female	36	4.44	.607	.101	0.03
	Male	77	4.47	.754	.086	
ISCA20 - Fairness towards employees	Female	36	4.22	1.045	.174	0.01
	Male	77	4.21	.784	.089	
ISCA21 - Fulfilment of personal needs of employee	Female	36	4.00	.956	.159	0.08
	Male	77	3.92	1.010	.115	

**Table 4.21: Effect sizes - Information Security Culture Aspects (Gender)**

The effect size (last column) indicates whether there is practical significance between the means for the two different genders. The effect size has the following significance:

- $\approx 0.2$  Small - No practically significant difference.
- $\approx 0.5$  Medium - Practically visible difference.
- $\approx 0.8$  Large - Practically significant difference.

Note that these effect size interpretations are the same across all demographic aspects.

Although females have set a higher norm for information security culture, the average difference is small enough to be negligible. The effect size is really low for all information security culture aspects, except for ISCA 4 (Education and training), 7 (Information monitoring and audit), and 13 (Strategy). Table 4.22 presents the t-test of the important topics with regard to gender.

The effect sizes from the T-test are shown in table 4.21 and 4.22 and a small part of the t-test is shown in table 2.23.

Important topics	Gender	N	Mean	Std. deviation	Std. error mean	Effect size
ITOAATP1 - Understand the need of an anti-virus program	Female	36	4.50	.737	.123	0.04
	Male	77	4.53	.852	.097	
ITOAATP2 - Understand the need of updating virus definitions	Female	36	4.47	.736	.123	0.09
	Male	77	4.55	.851	.097	
ITOAATP3 - Regularly scan a computer and storage devices	Female	36	4.42	.732	.122	0.20
	Male	77	4.21	1.043	.119	
ITOAATP4 - Use a personal firewall	Female	35	4.37	.973	.164	0.30
	Male	76	4.01	1.183	.136	
ITOAATP5 - Install software patches	Female	36	4.25	.906	.151	0.09
	Male	77	4.16	1.040	.118	
ITOAATP6 - Use pop-up blockers	Female	35	4.00	1.085	.183	0.07
	Male	77	3.92	1.144	.130	
ITOAATP7 - Understand the risk of downloading programs or files	Female	36	4.47	.736	.123	0.01
	Male	75	4.48	.742	.086	
ITOAATP8 - Understand the risks of P2P file sharing	Female	36	4.11	.919	.153	0.02
	Male	77	4.09	1.041	.119	
ITOAATP9 - Understand the risk of clicking on e-mail links	Female	36	4.31	.920	.153	0.09
	Male	77	4.39	.905	.103	
ITOAATP10 - Understand the risk of e-mailing passwords	Female	36	4.53	.941	.157	0.16
	Male	77	4.68	.715	.082	
ITOAATP11 - Understand the risk of e-mail attachments	Female	36	4.28	.944	.157	0.01
	Male	77	4.27	.941	.107	
ITOAATP12 - Regularly backup important files	Female	36	4.64	.593	.099	0.23
	Male	77	4.40	1.042	.119	
ITOAATP13 - Understand the risk of smartphone viruses	Female	35	3.97	1.294	.219	0.22
	Male	77	3.69	1.217	.139	
ITOAATP14 - Understand the need of anti-virus program for a smart phone	Female	36	3.94	1.264	.211	0.24
	Male	77	3.64	1.307	.149	
ITOAATP15 - Know the characteristics of a strong password	Female	36	4.33	.862	.144	0.09
	Male	77	4.42	.923	.105	
ITOAATP16 - Use different passwords for different systems	Female	36	4.11	1.090	.182	0.05
	Male	77	4.05	1.157	.132	
ITOAATP17 - Change passwords regularly	Female	36	4.19	.980	.163	0.31
	Male	76	3.80	1.244	.143	
ITOAATP18 - Understand legal, regulatory and ethical issues of information security	Female	36	4.28	.914	.152	0.28
	Male	77	4.00	.987	.112	

**Table 4.22: Effect sizes - Information Security Important Topics (Gender)**

Table 4.22 indicates that there are more notable effect sizes with performing the t-test on important topics with regard to gender. Of the identified 18 important topics, 7 topics have an effect size equal or bigger than 0.20, with 0.31 as the highest effect size. While these are small

values, it is large enough to show the difference between the two genders. The topics with notable effect size are:

- 3. Regularly scan a computer and storage devices. (0.2)
- 4. Use a personal firewall. (0.3)
- 12. Regularly backup important files. (0.23)
- 13. The risk of smartphone viruses. (0.22)
- 14. Understand the need of anti-virus program for a smart phone. (0.24)
- 17. Change passwords regularly. (0.31)
- 18. Legal, regulatory and ethical issues of information security. (0.28)

All of these topics had a higher mean for females than for males. However, an independent t-test was run, showing that the two groups (male and female) are not significantly different. Table 4.23 provides an extraction of the results from the independent t-test.

Independent Samples Test										
		Levene's Test for Equality		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
ISCA7 - Information monitoring and audit	Equal variances assumed	.299	.585	1.696	111	<b>.093</b>	.440	.260	-.074	.954
	Equal variances not assumed			1.725	71.468	<b>.089</b>	.440	.255	-.069	.949
ISCA11 - Communication	Equal variances assumed	1.699	.195	-.289	111	<b>.773</b>	-.058	.199	-.453	.338
	Equal variances not assumed			-.263	55.004	<b>.793</b>	-.058	.219	-.497	.382
ISCA13 - Strategy	Equal variances assumed	2.710	.103	1.759	111	<b>.081</b>	.343	.195	-.043	.730
	Equal variances not assumed			1.885	81.746	<b>.063</b>	.343	.182	-.019	.705
ITOAATP4 - use a personal firewall	Equal variances assumed	.196	.659	1.563	109	<b>.121</b>	.358	.229	-.096	.812
	Equal variances not assumed			1.680	79.402	<b>.097</b>	.358	.213	-.066	.783
ITOAATP11 - understand the risk of e-mail attachments	Equal variances assumed	.090	.765	.027	111	<b>.979</b>	.005	.190	-.372	.382
	Equal variances not assumed			.027	68.243	<b>.979</b>	.005	.190	-.375	.385
ITOAATP12 - regularly backup important files	Equal variances assumed	6.091	.015	1.266	111	<b>.208</b>	.236	.187	-.133	.606
	Equal variances not assumed			1.529	106.647	<b>.129</b>	.236	.154	-.070	.543

**Table 4.23: Independent T-Test (Gender)**

The Sig. (2-tailed) value has to be lower than 0.05 for the mean difference to be significant. Table 4.23 shows values ranging from 0.063 to 0.979, verifying that there is no significant difference to be found.

Note that the purpose of these analytical tests was to investigate possible similarities in the data with the idea of using it for possible future research. It is not part of the original scope of this study and is shown to prove that proper analysis was run.

The same test was run on **location (urban vs. rural)** and provided interesting results. There was one security culture aspect and three important topics that have statistical significance. Table 4.24 displays the t-test for these.

Aspects and Important topics	Urban_Rural	N	Mean	Deviation	Error Mean	Effect size
ISCA1 - Policy	1 (urban)	69	4.38	.842	.101	0.39
	2 (rural)	44	3.95	1.077	.162	
ITOAATP2 - understand the need of updating virus definitions	1 (urban)	69	4.65	.590	.071	0.32
	2 (rural)	44	4.32	1.052	.159	
ITOAATP5 - install software patches	1 (urban)	69	4.48	.851	.102	0.72
	2 (rural)	44	3.73	1.042	.157	
ITOAATP15 - know the characteristics of a strong	1 (urban)	69	4.55	.697	.084	0.37
	2 (rural)	44	4.14	1.112	.168	

**Table 4.24: T-Test for Significant Aspects and Topics (Location)**

All four of these aspects and topics had urban respondents desiring a higher baseline and assigning more importance on the topics. The effect size is between small and medium, except for ITOAATP5 (Install software patches) which has a large effect size. The security culture aspect in Table 26 is:

- Policy (small-medium effect size).

The important awareness and training topics are:

- 2. Understand the need of updating virus definitions (small-medium effect size).
- 5. Install software patches (medium-large effect size).
- 15. Know the characteristics of a strong password (small-medium effect size).

Table 4.25 presents the results from the independent t-test, showing the significance of the aspect and the three topics.

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
ISCA1 - Policy	Equal variances assumed	.173	.678	2.328	111	.022	.422	.181	.063	.782
	Equal variances not assumed			2.206	75.750	.030	.422	.191	.041	.804
ITOATP2 - understand the need of updating virus definitions	Equal variances assumed	11.240	.001	2.162	111	.033	.334	.155	.028	.640
	Equal variances not assumed			1.923	60.444	.059	.334	.174	-.013	.681
ITOATP5 - install software patches	Equal variances assumed	1.526	.219	4.187	111	.000	.751	.179	.396	1.106
	Equal variances not assumed			4.004	78.346	.000	.751	.188	.378	1.124
ITOATP15 - know the characteristics of a strong password	Equal variances assumed	5.189	.025	2.436	111	.016	.414	.170	.077	.751
	Equal variances not assumed			2.210	64.697	.031	.414	.188	.040	.789

**Table 4.25: Independent T-Test (Location)**

The topic of installing software patches is the only result that has a low enough Sig. value to have noteworthy significance (Sig. <0.05). It can be concluded that respondents in urban areas regard this topic as more important than those respondents in rural areas. The other aspect and topics have some significance: policy, virus definitions, and strong passwords are all seen as marginally more important in urban areas.

This section described the t-test which is a form of statistical analysis between two groups. The next section describes ANOVA which is used to analyse a model with more than two groups.

#### 4.2.1.2 Analysis of Variance (ANOVA)

The previous section described the t-test, which analysed a model with two groups. A t-test can only handle two groups and another model is necessary for more than two groups. The ANOVA test is used to describe these models.

ANOVA compares the differences between the means in a model with more than two groups using a linear model. Also known as the variance ratio method, ANOVA is well suited for simple designs and uses a multiple regression equation (Bryman, 2006).

The ANOVA test was run according to the level of employment of respondent. As all input groups had to contain at least 20 respondents, the respondents were grouped into top and middle management, technical, and other. All statistical analyses were done by the SKD (statistical consultation services) of the NWU Potchefstroom campus. Table 4.26 provides the descriptive ANOVA test for these groups. Only results with some significance are shown.

Important Topics	Level of employment	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum	Effect size	
						Lower Bound	Upper Bound			Top and Middle with ...	Technical with ....
ITOAATP12 - regularly backup important files	Top and Middle Management	51	4.63	.720	.101	4.42	4.83	2	5		
	Technical	41	4.17	1.202	.188	3.79	4.55	1	5	0.38	
	Other	15	4.73	.594	.153	4.40	5.06	3	5	0.15	0.47
	Total	107	4.47	.945	.091	4.29	4.65	1	5		
ITOAATP13 - understand the risk of smartphone viruses	Top and Middle Management	51	4.08	1.111	.156	3.77	4.39	1	5		
	Technical	40	3.43	1.299	.205	3.01	3.84	1	5	0.50	
	Other	15	3.47	1.457	.376	2.66	4.27	1	5	0.42	0.03
	Total	106	3.75	1.265	.123	3.50	3.99	1	5		
ITOAATP14 - understand the need of anti-virus program for a smart phone	Top and Middle Management	51	4.08	1.163	.163	3.75	4.41	1	5		
	Technical	41	3.39	1.394	.218	2.95	3.83	1	5	0.49	
	Other	15	3.40	1.404	.363	2.62	4.18	1	5	0.48	0.01
	Total	107	3.72	1.323	.128	3.47	3.97	1	5		

**Table 4.26: Significant Results Using ANOVA (Level of Employment)**

The effect size is similar to previous results with  $0.2 \approx$  Small,  $0.5 \approx$  Medium, and  $0.8 \approx$  Large. The only change is that for each important topic, multiple groups are compared to each other. The result from this test indicates that there is a small to medium sized effect for level of employment between:

- *Top and middle management and Technical* for:
  - 12. Regularly backup important files.
  - 13. Understand the risk of smartphone viruses.
  - 14. Understand the need of anti-virus program for a smart phone.
- *Top and middle management and Other* for:
  - 13. Understand the risk of smartphone viruses.
  - 14. Understand the need of anti-virus program for a smart phone.
- *Technical and Other* for:
  - 12. Regularly backup important files.

These results indicate a clear difference in mean value for the different levels of employment. For example, for ITOAATP12 – Regularly backup important files, the technical group generally has a lower value than the other group and top and middle management group. A large enough effect size indicates a clear difference in mean values.

A test was run to indicate if there is a statistical significance between the means of the different groups. This test aims to explain the experimental effect using either a linear or quadratic relationship in the data. This is shown in Table 4.27.

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
ITOAATP12 - regularly backup important files	Between Groups	5.976	2	2.988	3.505	.034
	Within Groups	88.660	104	.852		
	Total	94.636	106			
ITOAATP13 - understand the risk of smartphone viruses	Between Groups	10.928	2	5.464	3.580	.031
	Within Groups	157.195	103	1.526		
	Total	168.123	105			
ITOAATP14 - understand the need of anti-virus program for a smart	Between Groups	12.546	2	6.273	3.770	.026
	Within Groups	173.042	104	1.664		
	Total	185.589	106			

**Table 4.27: Trend Analysis (Level of Employment)**

The Sig. value indicates whether there are any statistical significance; it has to be lower than 0.05 to be significant. Table 4.27 indicates that only three important topics have statistical significance. No information security culture aspects have any statistical significance.

The same test was run on the levels of education of respondents. One aspect and one topic have statistical significant results. 'High school and post-secondary' have a high effect size with 'Masters and doctoral' and a medium effect size with 'Bachelors'. 'Bachelors' also has a small effect size with 'Masters and Doctoral' for both the aspect and the important topic. This is shown in Table 4.28.

Aspect and important topic	Level of education	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum	Effect size	
						Lower Bound	Upper Bound			High school and post s	Bachelor with ....
ISCA21 - Fulfillment of personal needs of employee	High school and post sec	16	4.50	.632	.158	4.16	4.84	3	5		
	Bachelor	59	3.76	1.150	.150	3.46	4.06	1	5	0.64	
	Masters and Doctoral	35	4.09	.702	.119	3.84	4.33	3	5	0.59	0.28
	Total	110	3.97	.990	.094	3.79	4.16	1	5		
ITOAATP11 - understand the risk of e-mail attachments	High school and post sec	16	3.75	1.183	.296	3.12	4.38	2	5		
	Bachelor	59	4.22	.966	.126	3.97	4.47	2	5	0.40	
	Masters and Doctoral	35	4.60	.604	.102	4.39	4.81	3	5	0.72	0.39
	Total	110	4.27	.938	.089	4.10	4.45	2	5		

**Table 4.28: Significant Results Using ANOVA (Level of Education)**

According to Table 4.28, the level of education determines the importance that can be ascribed to information security culture aspects. This can be seen with ISCA21 – Fulfillment of personal needs of employees in Table 4.28. People with high school and post-secondary levels of education see the information security culture aspect as very important (the mean is 4.5/5), while those with Masters and Doctoral degrees see it as important (the mean is 4.09/5); people with a Bachelor's degree only rate the aspect as 3.76/5. A large effect size indicates that there is a significant and universal difference between the means for a specific aspect/important topic.

Table 4.29 presents the aspect pertaining to fulfilment of personal needs of employee and the topic regarding the understanding of e-mail attachment risks. These aspects and topics have no related statistical value at this point in the analysis. The trend analysis for level of education can



be seen in Table 4.29. Both ISCA21 and ITOAATP11 have low Sig. values (<0.05), indicating that they have credible statistical significance.

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
ISCA21 - Fulfillment of personal needs of employee	Between	7.497	2	3.749	4.034	.020
	Within Groups	99.421	107	.929		
	Total	106.918	109			
ITOAATP11 - understand the risk of e-mail	Between	8.283	2	4.141	5.062	.008
	Within Groups	87.536	107	.818		
	Total	95.818	109			

**Table 4.29: Trend Analysis (Level of Education)**

The ANOVA test was run based on type of organisation that the respondents placed themselves in. This question has a high number of respondents in the 'Other' category. The significant results are shown in Table 4.30.

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum	Effect size		
						Lower Bound	Upper Bound			IT with ....	Academic / Education with ....	Sales, Admin with ....
ISCA9 - Information security program	I.T.	33	4.24	.751	.131	3.98	4.51	2	5			
	Academic /	28	3.61	.994	.188	3.22	3.99	1	5	0.64		
	Civil, Finance, Sales, Admin	24	3.96	1.160	.237	3.47	4.45	1	5	0.24	0.30	
	Other	27	4.37	.742	.143	4.08	4.66	3	5	0.17	0.77	0.36
	Total	112	4.05	.948	.090	3.88	4.23	1	5			
ISCA21 - Fulfillment of personal needs of employee	I.T.	33	4.30	1.015	.177	3.94	4.66	1	5			
	Academic /	28	3.57	1.034	.195	3.17	3.97	1	5	0.71		
	Civil, Finance, Sales, Admin	25	4.04	.935	.187	3.65	4.43	2	5	0.26	0.45	
	Other	27	3.81	.834	.160	3.48	4.14	2	5	0.48	0.24	0.24
	Total	113	3.95	.990	.093	3.76	4.13	1	5			
ITOAATP7 - understand the risk of downloading programs or files	I.T.	33	4.58	.614	.107	4.36	4.79	3	5			
	Academic /	28	4.36	.826	.156	4.04	4.68	2	5	0.26		
	Civil, Finance, Sales, Admin	24	4.17	.868	.177	3.80	4.53	2	5	0.47	0.22	
	Other	26	4.77	.514	.101	4.56	4.98	3	5	0.32	0.50	0.69
	Total	111	4.48	.737	.070	4.34	4.62	2	5			
ITOAATP15 - know the characteristics of a strong password	I.T.	33	4.58	.614	.107	4.36	4.79	3	5			
	Academic /	28	3.96	1.232	.233	3.49	4.44	1	5	0.50		
	Civil, Finance, Sales, Admin	25	4.52	.770	.154	4.20	4.84	2	5	0.07	0.45	
	Other	27	4.48	.802	.154	4.16	4.80	2	5	0.12	0.42	0.05
	Total	113	4.39	.901	.085	4.22	4.56	1	5			

**Table 4.30: Significant Results Using ANOVA (Organisation Type)**

The two aspects with significant results have a medium to large effect size for 'IT' with 'Academic/education' and a small effect size with 'Civil, finance, sales, and admin'. The second aspect also has a small effect size for 'IT' with 'Other'. There are several other effect sizes between small and medium with the exception of 'Academic/education' with 'Other' that has a large effect size. The important topics also have various degrees of effect sizes between small and medium. This indicates a clear difference between the mean value based on type of

organisation for each aspect/important topic. Table 4.31 presents the trend analysis for these aspects and topics.

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
ISCA9 - Information security program	Between	9.685	3	3.228	3.874	.011
	Within	89.994	108	.833		
	Total	99.679	111			
ISCA21 - Fulfillment of personal needs of employee	Between	8.821	3	2.940	3.177	.027
	Within	100.861	109	.925		
	Total	109.681	112			
ITOAATP7 - understand the risk of downloading programs or files	Between	5.256	3	1.752	3.443	.019
	Within	54.438	107	.509		
	Total	59.694	110			
ITOAATP15 - know the characteristics of a strong password	Between	6.862	3	2.287	2.968	.035
	Within	84.006	109	.771		
	Total	90.867	112			

**Table 4.31: Trend Analysis (Organisation Type)**

The Sig. values are less than 0.05, indicating that there is significant difference between the groups regarding the type of organisation. The security aspects mentioned in the table is:

- 9. Information security programme.
- 21. Fulfilment of personal needs of employee.

The important topics mentioned are:

- 7. Understand the risk of downloading programs or files.
- 15. Know the characteristics of a strong password.

This section described the inferential statistics that was used to analyse the demographic data. Although several statistical techniques were applied to the data, the main aim of the questionnaire was to test how respondents rated the information security culture aspects, delivery methods, and important topics. This was done with means and averages as shown in the final framework (refer to Chapter 5).

The next section describes the open questions of the questionnaire and how they were examined.

#### **4.2.2 Open-ended Questions**

This section describes the open-ended questions from the questionnaire. In total, there were four open-ended questions for comments or feedback (Sections 4 to 7). After each section,

respondents were invited to provide comments and feedback on the topic of information security culture as well as the specific topic of each section. The questions were not compulsory; so many respondents chose not to complete the questions. The responses are split across four tables.

The responses for the first open-ended question (included after the section regarding **information security culture aspects**) are presented in Table 4.32. This table describes which respondent made the comment, the exact comment, and how it was interpreted.

<b>Respondent Number</b>	<b>Please give any comments or feedback that you might have regarding this aspect of your company.*</b>	<b>Interpretation</b>
R3	I am unsure whether I understood the questions correctly. In my view all aspects mentioned are extremely important and should be present. This means that all aspects should be rated as 5? Unless someone don't understand the concept of security everybody is suppose to rate all questions as 5, in which case no deductions can be made from the questionnaire. This is also a compliment as it seems that you have already identified all the important aspects. As I said, maybe I misunderstood the questions.	All aspects important
R8	Geen (None**)	N/A
R10	I have not experienced a security issue at my company thus far, so have not seem security procedures in action. In general though taken as important and best practices followed, security is more a sideline aspect to companies I have worked at.	Security side line aspect
R19	Security needs to be taken more seriously	Security side line aspect
R24	Reality (daily life in the company) tends to shift the importance of each aspect downwards	Security side line aspect
R41	It is a concern that my company does not implement the necessary policies, processes, training etc. to adequately ensure information security.	Security side line aspect
R42	Policies and Compliance should always be observed in collaboration with security. Users should always be informed about the importance of IT threats and assets and trained accordingly and constantly reminded about cost and consequences in non-compliance situations.	Noncompliance consequences
R48	Disciplinary action when these security policies are violated	Non-compliance consequences
R53	N/A	N/A
R66	Complacency rules.	Non-compliance consequences
R67	As we are still a small, fast-growing organisation, these aspects are being taken up more seriously.	All aspects important
R70	There are too many disruptions during a work session to verify user accounts and password requests disrupts thought- and conversation patterns, negatively impacting productivity	Productivity impediment
R75	The company should listen to security experts and apply the recommendations they give and not get annoyed by them.	Listen to experts

Respondent Number	Please give any comments or feedback that you might have regarding this aspect of your company.*	Interpretation
R84	All these questions assume a Western way of organising, with an hierarchical organisation. What if the organisation is participative, governed by elders, people with authority, who call for indabas to discuss issues. Where information is freely shared? We have got an open organisation, where information is seen as a resource to share, not to keep...	Local culture, Information is sharable resource
R91	Employees not fully trained on information security, hence you will find too many information security breaches	Security side line aspect
R93	Change management should be split into organisational change and technical change. Nothing said about keeping software up to date or the degree of vendor interaction. I've marked some points 4 because from my low position in this organisation it's hard to be sure how good those points are. I've previously worked at another organisation in the same industry where most of the answers would have been at the low end.	Expand change management
R97	How can we improve the security awareness of the company from a employee standpoint	Employee standpoint
R103	All of this is important and do not get enough attention	All aspects important
R111	Being a financial insurance organisation that operate in International markets, we MUST have security measures in place. Most of the measures in place are there because fingers have been burned in the past. I can confirm that security has been tightened a lot in the 6 years that I have been in the organisation. - There has been a major increase in all aspects of security in this time. From what I hear this was a trend even before I joined the organisation. Sometimes I feel that there is a lack of communication on added security measures - we just suddenly notice that we need to justify sending emails to address outside of our organisation or when we copy data on it a removable storage.	All aspects important

**Table 4.32: Open-ended Question Results - Part 1**

\* Exact responses as given by questionnaire participants.

\*\* Edited to add English translation.

Nineteen respondents gave feedback on this question. Of these respondents, two indicated that they had no feedback. The other responses were interpreted as:

- R3, R67, R91, R103, R111: All aspects are considered as important. As R3 states, it would be ideal if all information security culture aspects could be perfect. R103 and R111 agree that security culture is extremely important and should receive more attention. They all feel that their respective organisations should give more attention to security training. R111 adds that new security measures/controls should be properly communicated to employees.

- R10, R19, R24, R41: Security side line aspect. These respondents feel that the organisations that they are part of do not give enough attention to information security and should take security more seriously.
- R42, R48, R66: Non-compliance consequences. Employees should be taught the effects and consequences of Non-compliance. This is included in the information security culture aspect “2. Compliance”.
- R70: Productivity impediment. Employees feel that too many security measures can impact their productivity. Employers must properly communicate the need for security to employees.
- R75: Listen to experts. This is a valid point and should be included in all information security culture aspects. Risk analysis and information monitoring and audit must be done by experts as well.
- R84: Local culture of employees should be considered. While this is a valid point, the respondent also claimed to belong to an organisation that freely shares information and made several other comments claiming that the identified aspects, delivery methods and topics do not fit an “African culture”. The literature has shown that information is a valuable resource and should be protected. Therefore these comments will be disregarded.
- R93: Expand change management. Employees should be encouraged to embrace new technology and security mechanisms, including organisational and technical change.
- R97: Employee standpoint. If the aspect pertaining to manager's perspective is not included in the information security culture (i.e. managers do not care about information security) and the employees want to improve the security, the employees are considered to be on their own. This is a very negative situation that needs to get attention.

The questionnaire aided some respondents by raising their awareness. Several others noted that their organisations have a low security culture.

The responses for the second open-ended question (included after the section regarding **awareness and training programme delivery methods**) are presented in Table 4.33. This table indicates which respondent made the comment, the exact comment, and how it was interpreted.

Respondent Number	Please give any comments or feedback that you might have regarding this aspect of your company.*	Interpretation
R10	Some of the mentioned options are ways my company could use, which it currently does not, which will improve the various security aspects.	Raised awareness
R19	N/A	
R40	My company uses formal training, informal training, mass emails and regular office meetings to communicate security related issues and risks to the organisation. Information security is taken very seriously.	Combination, Information Security important
R41	It is a concern that very little if at all training is provided to employees regarding this topic.	Raised awareness
R42	On site and External training are provided, Security awareness is effective via Poster and DMP at strategic area, accountability, policy and compliance are reminding to user on a weekly monthly basis	Has good security culture
R43	There is no single best method. A variety of methods are needed, to cater for various operational needs of the users, as well as their learning styles.	Combination
R53	N/A	
R66	As a small unit, there is a gap between the desirable training and the feasible training.	Training not always feasible (small)
R67	If I'm honest, we have only scratched the surface. These questions have prompted me to take a stronger stance on formally improving the policies in our company.	Raised awareness
R70	Various delivery methods may be advisable depending on the audience, their level of authority within the organisation and aspects of the information security there are responsible for, or engaged with. Formal training should be supported by regular short message refreshers and other forms of awareness creation, depending on the target group. One method/intervention may not be effective. Delivery will strongly correlate to the culture of the organisation, level of information security required, current legislation and other regulatory frameworks as well as the business model of the organisation (i.e. bank vs social media platform)	Combination
R75	We rarely have workshops related to security at our company. Have only the basic understanding of security (e.g. How the HTTPS protocol works, SQL Injection attacks)	Has low security culture
R81	This is more suitable to SMME	Only suitable to SMME
R84	Please read Mukuka, G. S. (2010). Reap What You Have Not Sown. Indigenous Knowledge Systems and Intellectual Property Laws in South Africa. Pretoria: Pretoria University Press. for gaining an understanding that the issues above are very different in our African setting.	Culture related
R86	mentorship and coaching form part of our everyday culture	Mentorship structure

Respondent Number	Please give any comments or feedback that you might have regarding this aspect of your company.*	Interpretation
R91	Other aspects can be done applying multiple methods starting with formal training, following up with posters just to emphasize what was learnt in the formal session, also can be added desktop messages, screen savers, daily sms's, and social media - messages on you tube from management	Combination
R93	The amount of policy is so great there getting everyone to click on it every so often could be more of a token exercise than actually getting the whole policy engrained (although the main points may stick).	Policy too big
R102	My company has been focusing on mainly on brown bag and desktop type awareness and delivery methods. I think a short training course should be compulsory for employees, especially given the security clearance of public officials. In addition, employees must be made aware of the cyber risks and organisational IT structure for ensuring compliance and understanding of roles	Raised awareness
R103	Methods must be varied - must excite and catch attention	Combination

**Table 4.33: Open-ended Question Results - Part 2**

\* Exact responses as given by questionnaire participants.

There were 18 responses to the second open-ended question. Two of these responses were "N/A" and are accordingly disregarded. The other 16 responses are discussed next:

- R10, R41, R67, R102: Raised awareness. The questionnaire raised the awareness of these respondents.
- R40, R43, R70, R91, R103: Combination. Using a combination of delivery methods each ideal to a specific topic/subject has the best chance to achieve an ideal security culture.
- R42: Strong security culture. This respondent believes that his organisation has a strong information security culture.
- R66: Training not feasible. In very small organisations, the feasibility of proper security training is sometimes low.
- R75: Weak security culture. This respondent believes that his organisation has a weak information security culture that only focuses on the basic aspects.
- R81: Training not suitable for large organisations. Training and awareness programmes should take into account the size of the organisation. This respondent feels that the identified delivery methods are not suitable for a large organisation.
- R84: Culture related. This respondent believes that security is entirely different matter in an "African Setting".
- R86: Mentorship structure. This is a good delivery method where new employees are tutored by a mentor that has experience in the work environment and know the security structure of the organisation well.

- R93: Policy too big. The policy is a long and difficult document to read, but it is pointless if employees click on it occasionally. For this reason, a training/awareness session is required to help employees read and understand the policy.

Several respondents noted that using a combination of delivery methods achieves the best results.

The responses for the third open-ended question (included after the section regarding **important topics in an awareness and training programme**) are presented in Table 4.34. This table indicates which respondent made the comment, the exact comment, and how it was interpreted.

<b>Respondent Number</b>	<b>Please give any comments or feedback that you might have regarding this aspect of your company.*</b>	<b>Interpretation</b>
R3	My earlier comments apply to this section as well	All aspects important
R8	Geen (None**)	
R24	None	
R42	Password sharing is a dismissible offense so we do check password access and transaction weekly	Password sharing and renewal
R43	In some cases requirements are controlled centrally, and the various devices are forced into updates etc, so there is no user interaction required. This reduces the need for awareness around those in the organisation. It is also important to note that awareness training can be conducted for the employees' personal environment.	Forced updates Training according to environment
R53	N/A	
R66	Awareness levels are good but not reinforced regularly.	Enforce awareness
R84	Viruses are susceptible for Windows computers mainly. Thus, these questions imply one uses Windows. There are many other Operating Systems that do not have virus issues. We try not to use Windows, because of that (and many other reasons, as Windows does not really work well in Africa). When there is no Windows, there are hardly viruses.	Operating system used
R91	Using personal firewall might not assist much because in most organisations their system is protect by the main fire wall	Organisational firewall
R93	Many of these points are not applicable to workers not supporting desktop machines. Updating antivirus is doubtless done by someone but they never need to bother me with it. A good single-sign on means you have only one password at work (different from any at home).	Wants less security/responsibility
R102	Future plans for IT infrastructure is extremely important	Planning ahead
R111	We (the majority of employees) don't really receive training on most of these topics, however, there are strong measures in place. Most of the above-mentioned topics	Strong technological security - weak



Respondent Number	Please give any comments or feedback that you might have regarding this aspect of your company.*	Interpretation
	<p>happen seamlessly in the background without most employees even being aware of it. Our Technology Infrastructure Security department are constantly busy refining policies, applying patches and so on. Our firewall block a lot, like preventing us from downloading files - need to log requests if you need something to be downloaded, then they will do on your behalf.</p> <p>When there are emails from outside the organisation are identified as being fishing emails or containing malicious attachments, emails are sent out to the whole organisation warning about the specific case. Employees are also prompted to inform our Technology Infrastructure Security department if they suspect they are affected.</p>	security culture

**Table 4.34: Open-ended Question Results - Part 3**

\* Exact responses as given by questionnaire participants.

\*\* Edited to add English translation.

Only 12 respondents answered this question. Of those respondents, three indicated that they had no feedback or comments. The remaining nine responses are discussed next:

- R3: All aspects/topics important. In the first open-ended question, R3 commented that ideally all security culture aspects should be rated as extremely important. Here he continues to say that all topics should be regarded as extremely important and none of them should be addressed partially.
- R42: Password sharing and renewal. Employees should never share their passwords with each other and should change their passwords regularly.
- R43: Forced updates. Devices should be forced to install the latest security updates before they can continue to connect on the network. A previous comment mentioned that such updates should be communicated properly to employees.
- R66: Enforce awareness. Awareness and training have to be reinforced regularly to ensure the strength of the security culture.
- R84: Operating system used. Some operating systems are more secure than others and this should be considered when setting up the organisation's information system.
- R91: Organisational firewall. The main firewall of the organisation's network is an extremely important component of protecting organisational information assets.
- R93: Less security/responsibility. This respondent feels that security is something that should be done by others and that he can function with a single password to protect his workstation.
- R102: Planning ahead. It is extremely important to plan for the future of the information system infrastructure.

- R111: Strong technological security - weak security culture .This respondent agrees with R93 that employees do not need strong training in security. He feels that their strong technical security allows for a weak security culture.

There were various responses to this question. Many respondents mentioned unique aspects of their own security culture and other important parts of information security.

The responses for the last open-ended question (included after the section regarding **the strength of the respondent's organisational security culture and their knowledge on the subject of security culture**) are presented in Table 4.35. This table indicates which respondent made the comment, the exact comment, and how it was interpreted.

Respondent Number	Please give any comments or feedback that you might have regarding this questionnaire.*	Interpretation
R24	Never realised it, but perhaps we should give more attention to some of these aspects	Raised awareness
R31	Research regarding security is important and therefore a good way to resolve issues regarding security flaws. Good technique to give one an idea regarding the knowledge of their employees.	Test employee security knowledge
R41	It could provide more information if the first set of questions on how I rate the importance of each aspect, be repeated, but that I then indicate a rating, based on my perception, of the level to which my company is implementing or performing on each aspect.	Rate respondent company
R53	Insightful and concise questions	Raised awareness
R66	None	
R70	I have a firm understanding of information security and why I deem it important. I am not aware of how my organisation information systems have been clustered and find all the various log-ins and PIN-requirements and various other restrictive measures cumbersome. One log-in with security 'in the background' would be preferable.	Claims strong security awareness Work impediment
R75	I would not think that it should be up to oneself to get on top of security threats. I think it should be the company or in-house security expert to get you up to date with threats.	Wants minimal involvement
R91	After completing this survey have noticed that I need to learn more about information security	Improved awareness
R102	I think the questionnaire could have further probed the importance of awareness and training delivery methods by looking at the regularity of such sessions	Regularity of training
R103	Important topics.	Improved awareness

Respondent Number	Please give any comments or feedback that you might have regarding this questionnaire.*	Interpretation
R107	Remember that, although the topics and aspects are very solid and relevant, it is representative of the limited perspective of one employee and the area that they are currently based in. A good addition to the questionnaire would be to ask what business unit the person answering the questionnaire is in and what overall definition their company has (i.e. a bank - finance). This is non-invasive and will give great insights into how awareness ebbs and flows from BU to BU while also helping to show that a company cannot have an uniform level of awareness across its landscape.	Business unit specific

**Table 4.35: Open-ended Question Results - Part 4**

\* Exact responses as given by questionnaire participants.

There were 11 responses to the final open-ended question. One of these responses was “None”, and is accordingly disregarded. The other responses are discussed next:

- R24, R53, R91, R103: Raised awareness. The questionnaire improved the awareness of these respondents.
- R31: Test employee security. The use of the questionnaire can help determine the security knowledge of employees.
- R41: Rate respondent company. The idea to give a rating to the perceived strength of a respondent’s organisation encouraged the app described in Chapter 5.
- R70: Claims strong security awareness, work impediment. This respondent claims to have a strong security awareness and mentions work impediment again (as in a previous question).
- R75: Minimal involvement. This respondent feels that security should be up to security experts and that other employees should have minimal involvement. R75 mentioned listening to security experts in a previous comment as well.
- R102: Frequency of training. The frequency with which a training and awareness programme is conducted is very important.
- R107: Business unit specific. Although the questionnaire did not include this field, it could provide potential future research and should also be considered when setting up a new security system.

These were all the responses to the open questions in the four sections. There are no similarities between the respondents who answered these questions.

Table 4.36 present a mapping of each respondent to the questions answered. The legend explaining each of the headings is:

- ESCA – Extra security culture aspects.
- COFS4 – Comments or feedback Section 4 (after security culture aspects).
- EDM – Extra delivery methods.
- COFS5 – Comments or feedback Section 5 (after delivery methods).
- EIT – Extra important topics.
- COFS6 – Comments or feedback Section 6 (after important topics).
- COFS7 – Comments or feedback Section 7 (at the end of the questionnaire).
- CONF1 – Confidence in own company's information security culture.
- CONF2 – Confidence in own knowledge regarding information security culture.

ESCA	COFS4	EDM	COFS5	EIT	COFS6	COFS7	CONF1	CONF2
	R3				R3		2	3
	R8	R8	R8	R8	R8	R8	3	3
	R10		R10				3	4
	R19	R19	R19	R19			2	2
R24	R24	R24		R24	R24	R24	5	4
R31						R31	5	5
				R35			3	5
R40		R40	R40	R40			4	4
	R41		R41			R41	2	4
R42	R42		R42		R42		5	5
		R43	R43	R43	R43		4	5
R48	R48						3	5
R53	R53	R53	R53	R53	R53	R53	5	5
R66	R66	R66	R66	R66	R66	R66	3	5
	R67		R67				3	4
R70	R70	R70	R70			R70	3	3
	R75		R75			R75	2	3
		R76					3	4
		R81	R81	R81			5	4
		R83					4	4
R84	R84	R84	R84	R84	R84		4	5
		R86	R86				4	4
R91	R91	R91	R91		R91	R91	2	3
	R93	R93	R93	R93	R93		5	5
R97	R97						4	5
R102			R102		R102	R102	4	4
	R103		R103	R103		R103	3	4
R107						R107	4	4
	R111				R111		5	5

**Table 4.36: Open-ended Questions - Respondent Mapping**

Conf1 and Conf2 are both the average rating out of 5 describing the respondent's confidence in his company's information security culture (Conf1) and his own knowledge regarding information security culture. As shown in Table 4.36, the respondents' confidence in their respective company's information security culture or own knowledge regarding information security culture does not affect whether they answer open-ended questions, although most respondents that answered have more confidence in their own knowledge than in the security of their organisations. As shown in Figures 4.5 and 4.6, where respondents rated their confidence, more can be done in order to raise awareness and improve knowledge.

This section described the data analysis that was done on the responses of the questionnaire. The next section discusses how the framework was created.

### **4.3 Building the Framework**

This section describes the process of building the framework to indicate different aspects of information security culture. The framework was constructed to fulfil the final aim of this study and was based on the results to the following objectives as stated in Chapter 1, Section 2:

- Investigate organisational culture and information security culture and determine important aspects of information security culture – this is done in the literature review.
- Use these aspects within different organisations to determine an acceptable baseline/standard – this is identified in the questionnaire and is found under questionnaire results.
- Identify delivery methods of training/awareness in literature and within organisations relating to information security culture – this is done in the literature review.
- Investigate which training/awareness delivery methods can be used to improve each identified information security culture factor in order to reach the identified standard/baseline – this is identified in the questionnaire and is found under questionnaire results.
- Identify important topics of an awareness and training programme in literature review and in organisations – this is found in literature and identified in the questionnaire.

In effect, the framework should present the 21 information security culture aspects, as well as the perceived importance of each aspect. The framework also needs to present the five delivery methods from the questionnaire and their respective and perceived preference rating. Lastly, the important topics that need to be included in an awareness and training programme should be presented in the framework. The comments from the questionnaire respondents are also included in the framework, showing additional aspects, delivery methods and important topics. The framework is structured according to the format as shown in Table 4.37.

Aspect	/5	Importance (%)	Delivery methods to improve the aspect		
			Method	/113	Preferred (%)
1. Policy	4.21	84.2%	1. Formal	41	36.3%
			2. Informal	29	25.7%
			3. Short	25	22.1%
			4. Computer	12	10.6%
			5. Other	6	5.3%
...	....	...	...	...	...
The same structure and design was applied to all other important information security aspects and delivery methods, as well as new aspects and delivery methods named by respondents.					
Information security important topics			Average /5		Importance (%)
Understand the risk of e-mailing passwords			4.63		92.57%
...			...		...
The same structure and design was applied to all other important information security topics, as well as new important topics named by respondents.					

**Table 4.37: Framework Design and Structure**

The complete framework can be seen in Chapter 5. The next section provides a brief summary of this chapter.

#### 4.4 Summary

The questionnaire was answered by 113 respondents. Most respondents answered the majority of the questions, with the occasional empty question. The questionnaire data was sufficient to acquire a minimum baseline for each identified security culture aspect, determine the preferred delivery methods, as well as rate the importance of the identified training and awareness delivery methods. Additional comments provided extra aspects, delivery methods and important topics that were not in the original list.

The demographical details of respondents generated statistical results that, while not vital to this study, provided interesting correlations. Open-ended questions allowed respondents to provide feedback and comments on the study, which was also analysed and interpreted. Lastly, a basic structure for the framework was designed. This chapter described the questionnaire results, data analysis, and the basic design of the framework. The next chapter presents the framework as well as a mobile application that is based on the framework and survey results.

## 5 CHAPTER 5: FRAMEWORK AND MOBILE APPLICATION

This chapter presents the full framework for information security culture, aspects, delivery methods and important topics as depicted in Figure 5.1. It further describes the process of creating the mobile application and displays snapshots of the application itself. In Chapter 4 Section 3, the layout of the framework was presented. This layout is used in this chapter to create the full framework with the results of the questionnaire.

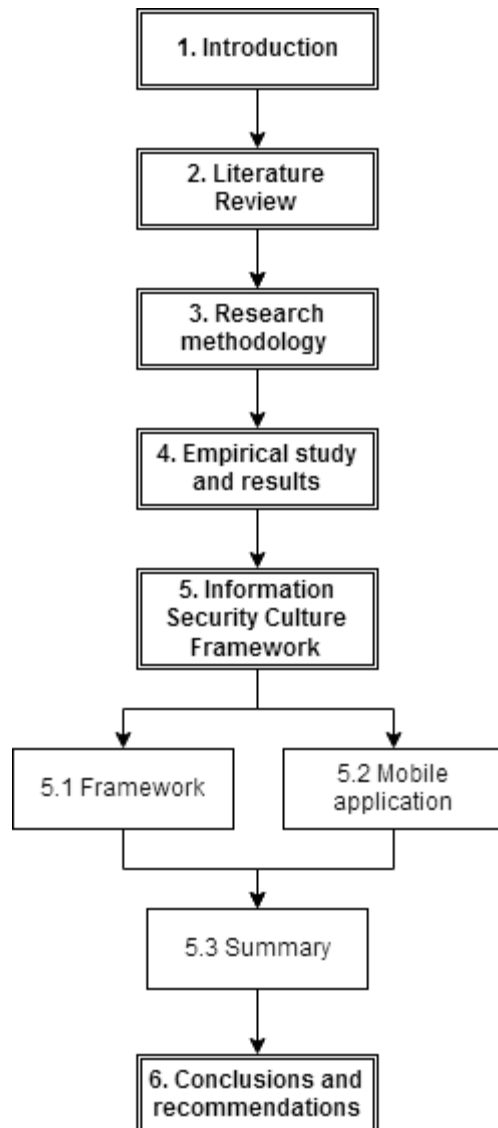


Figure 5.1: Introduction Chapter 5

### 5.1 Framework

A high level design of the framework can be seen in Chapter 4, Figure 4.37 describing the design and format of the framework.

The framework is presented as several tables that follow the layout presented in Chapter 4 Section 3. The tables can be combined to create the complete framework. The importance of

each information security culture aspect is given both as a value out of 5 and as a percentage. The same is done for each delivery method describing the preference to improve each aspect. This framework does not sort the information security culture aspects or delivery methods, but presents the aspects in the order in which they were identified in the original literature review. The delivery methods are all in the same order for every aspect.

Table 5.1 presents the first part of the framework with six information security culture aspects and the preferred delivery methods for each.

<b><u>Aspect</u></b>	<b><u>/5</u></b>	<b><u>Importance (%)</u></b>	<b><u>Delivery methods to improve the aspect</u></b>		
			<b><u>Method</u></b>	<b><u>Total</u></b>	<b><u>Preferred (%)</u></b>
1. Policy	4.21	82.4%	1. Formal	41	36.3%
			2. Informal	29	25.7%
			3. Short	25	22.1%
			4. Computer	12	10.6%
			5. Other	6	5.3%
2. Compliance	4.12	82.4%	1. Formal	33	29.2%
			2. Informal	41	36.3%
			3. Short	20	17.7%
			4. Computer	14	12.4%
			5. Other	5	4.4%
3. Managerial trust/Information security leadership	4.29	85.8%	1. Formal	32	28.3%
			2. Informal	40	35.4%
			3. Short	20	17.7%
			4. Computer	7	6.2%
			5. Other	10	8.8%
4. Education and training	3.54	70.8%	1. Formal	53	46.9%
			2. Informal	30	26.5%
			3. Short	5	4.4%
			4. Computer	18	15.9%
			5. Other	5	4.4%
5. Information security awareness	3.73	74.6%	1. Formal	22	19.5%
			2. Informal	42	37.2%
			3. Short	33	29.2%
			4. Computer	10	8.8%
			5. Other	4	3.5%
6. Information asset management	4.07	81.4%	1. Formal	26	23.0%
			2. Informal	40	35.4%
			3. Short	23	20.4%
			4. Computer	10	8.8%
			5. Other	7	6.2%

**Table 5.1: Framework - Part 1**



By looking at the framework, an organisation can easily identify which information security culture aspects they should improve on, as well as which delivery methods is preferred in order to improve the identified aspect. The framework contains 21 aspects, each with a possible five delivery methods.

Table 5.2 presents the information security culture aspects 7 to 11.

<b><u>Aspect</u></b>	<b><u>/5</u></b>	<b><u>Importance (%)</u></b>	<b><u>Delivery methods to improve the aspect</u></b>		
			<b><u>Method</u></b>	<b><u>Total</u></b>	<b><u>Preferred (%)</u></b>
7. Information monitoring and audit	3.48	69.6%	1. Formal	40	35.4%
			2. Informal	31	27.4%
			3. Short	15	13.3%
			4. Computer	13	11.5%
			5. Other	7	6.2%
8. Business continuity plan/incident management	3.70	74.0%	1. Formal	54	47.8%
			2. Informal	24	21.2%
			3. Short	15	13.3%
			4. Computer	8	7.1%
			5. Other	8	7.1%
9. Information security programme	4.05	81.0%	1. Formal	42	37.2%
			2. Informal	35	31.0%
			3. Short	12	10.6%
			4. Computer	17	15.0%
			5. Other	5	4.4%
10. Change management	3.80	76.0%	1. Formal	27	23.9%
			2. Informal	46	40.7%
			3. Short	18	15.9%
			4. Computer	10	8.8%
			5. Other	10	8.8%
11. Communication	4.15	83.0%	1. Formal	23	20.4%
			2. Informal	36	31.9%
			3. Short	30	26.5%
			4. Computer	12	10.6%
			5. Other	10	8.8%
			2. Informal	39	34.5%
			3. Short	23	20.4%
			4. Computer	9	8.0%
			5. Other	9	8.0%

**Table 5.2: Framework - Part 2**

Table 5.3 presents the information security culture aspects 12 to 17.

<b><u>Aspect</u></b>	<b><u>/5</u></b>	<b><u>Importance (%)</u></b>	<b><u>Delivery methods to improve the aspect</u></b>		
			<b><u>Method</u></b>	<b><u>/Total</u></b>	<b><u>Preferred (%)</u></b>
12. Managements' perspective	3.91	78.2%	1. Formal	28	24.8%
			2. Informal	39	34.5%
			3. Short	23	20.4%
			4. Computer	9	8.0%
			5. Other	9	8.0%
13. Strategy	3.85	77.0%	1. Formal	45	39.8%
			2. Informal	34	30.1%
			3. Short	16	14.2%
			4. Computer	7	6.2%
			5. Other	6	5.3%
14. Delegation of responsibility	4.07	81.4%	1. Formal	44	38.9%
			2. Informal	31	27.4%
			3. Short	17	15.0%
			4. Computer	6	5.3%
			5. Other	9	8.0%
15. Risk analysis	3.87	77.4%	1. Formal	49	43.4%
			2. Informal	37	32.7%
			3. Short	13	11.5%
			4. Computer	8	7.1%
			5. Other	2	1.8%
16. ROI	3.50	70.0%	1. Formal	39	34.5%
			2. Informal	35	31.0%
			3. Short	13	11.5%
			4. Computer	6	5.3%
			5. Other	17	15.0%
17. Legal and Regulatory	4.12	82.4%	1. Formal	49	43.4%
			2. Informal	30	26.5%
			3. Short	15	13.3%
			4. Computer	10	8.8%
			5. Other	6	5.3%

**Table 5.3: Framework - Part 3**

The last aspects (18 to 21) are presented in Table 5.4.

Aspect	/5	Importance (%)	Delivery methods to improve the aspect		
			Method	/Total	Preferred (%)
18. Ethical conduct	4.42	88.4%	1. Formal	38	33.6%
			2. Informal	38	33.6%
			3. Short	20	17.7%
			4. Computer	9	8.0%
			5. Other	7	6.2%
19. Accountability	4.46	89.2%	1. Formal	41	36.3%
			2. Informal	30	26.5%
			3. Short	24	21.2%
			4. Computer	7	6.2%
			5. Other	5	4.4%
20. Fairness towards employees	4.21	84.2%	1. Formal	26	23.0%
			2. Informal	40	35.4%
			3. Short	22	19.5%
			4. Computer	12	10.6%
			5. Other	11	9.7%
21. Fulfilment of personal needs of employee	3.95	79.0%	1. Formal	23	20.4%
			2. Informal	31	27.4%
			3. Short	28	24.8%
			4. Computer	11	9.7%
			5. Other	16	14.2%
Added:			Added:		
Impact of recent breaches			Face-to-face		
Productivity impediment			Mass emails		
Local culture			Email alerts		
Organisation type			Group discussion		
			Stakeholder involvement		
			Mentoring		

**Table 5.4: Framework - Part 4**

There are four additional possible information security culture aspects and six additional delivery methods at the end, as shown in Table 5.4.

The last part of the framework presents the important topics. This is presented in Table 5.5.

The framework fulfils all the aims and requirements of the study. It can be used to determine an organisation's information security culture to see whether it achieves the minimum acceptable baseline, it provides preferred delivery methods for each aspect, and it offers important topics that employees should be made aware of. Each of the 21 identified information security culture aspects is given an importance rating. In relation to each aspect, five delivery method

categories are given a rating of how much it is preferred with regard to improving the specific aspect. Lastly, the important topics are given with an importance rating for each.

This section discussed the final framework that can be used by organisations to measure their level of information security culture against a norm. The next section provides insight into the mobile application that was developed as a result of the final framework created by using the results of the questionnaire as an additional contribution.

<b><u>Information security culture important topics</u></b>	<b><u>Average /5</u></b>	<b><u>Importance (%)</u></b>
10. understand the risk of e-mailing passwords	4.63	92.6%
1. understand the need of an anti-virus program	4.52	90.4%
2. understand the need of updating virus definitions	4.52	90.4%
12. regularly backup important files	4.48	89.6%
7. understand the risk of downloading programs or files	4.48	89.5%
15. know the characteristics of a strong password	4.39	87.8%
9. understand the risk of clicking on e-mail links	4.36	87.3%
3. regularly scan a computer and storage devices	4.27	85.5%
11. understand the risk of e-mail attachments	4.27	85.5%
5. install software patches	4.19	83.7%
4. use a personal firewall	4.13	82.5%
8. understand the risks of peer-to-peer (P2P) file sharing	4.10	81.9%
18. understand legal, regulatory and ethical issues of information security	4.09	81.8%
16. use different passwords for different systems	4.07	81.4%
6. use pop-up blockers	3.95	78.9%
17. change passwords regularly	3.93	78.6%
13. understand the risk of smartphone viruses	3.78	75.5%
14. understand the need of anti-virus program for a smart phone	3.73	74.7%
Added comments:		
· Ransomware		
· Mobile devices security		
· Encryption		
· Clear desk policy		
· File storage		

**Table 5.5: Framework - Part 5**

## **5.2 Mobile Application**

This section describes the mobile application, the purpose of the application and how it was written. It presents insight into the functionality of the application and provides initial feedback regarding the application.

### **5.2.1 Aim of the Mobile Application**

The purpose of the mobile application is to apply the questionnaire data in the framework, demonstrating how it can be utilised in an organisational setting. The application should enable

users to measure the strength of their organisations' security culture and then advice users on which aspects should be improved. For each information security culture aspect, the application must describe the preferred delivery methods. It must also inform users of the important topics in the framework.

### 5.2.2 Design and Technical Aspects

The application was built using Android Studio 1.4 and consists of six layouts/screens. The first layout is the main page which introduces the application and directs the user to three buttons: Definitions, Test your organisations information security culture, and Important topics. The Definitions page provides the definitions of organisational culture and information security culture. Using the "Back" button of the mobile phone, a user can return to the main/home page of the application. The first layout is presented in Figure 5.2.

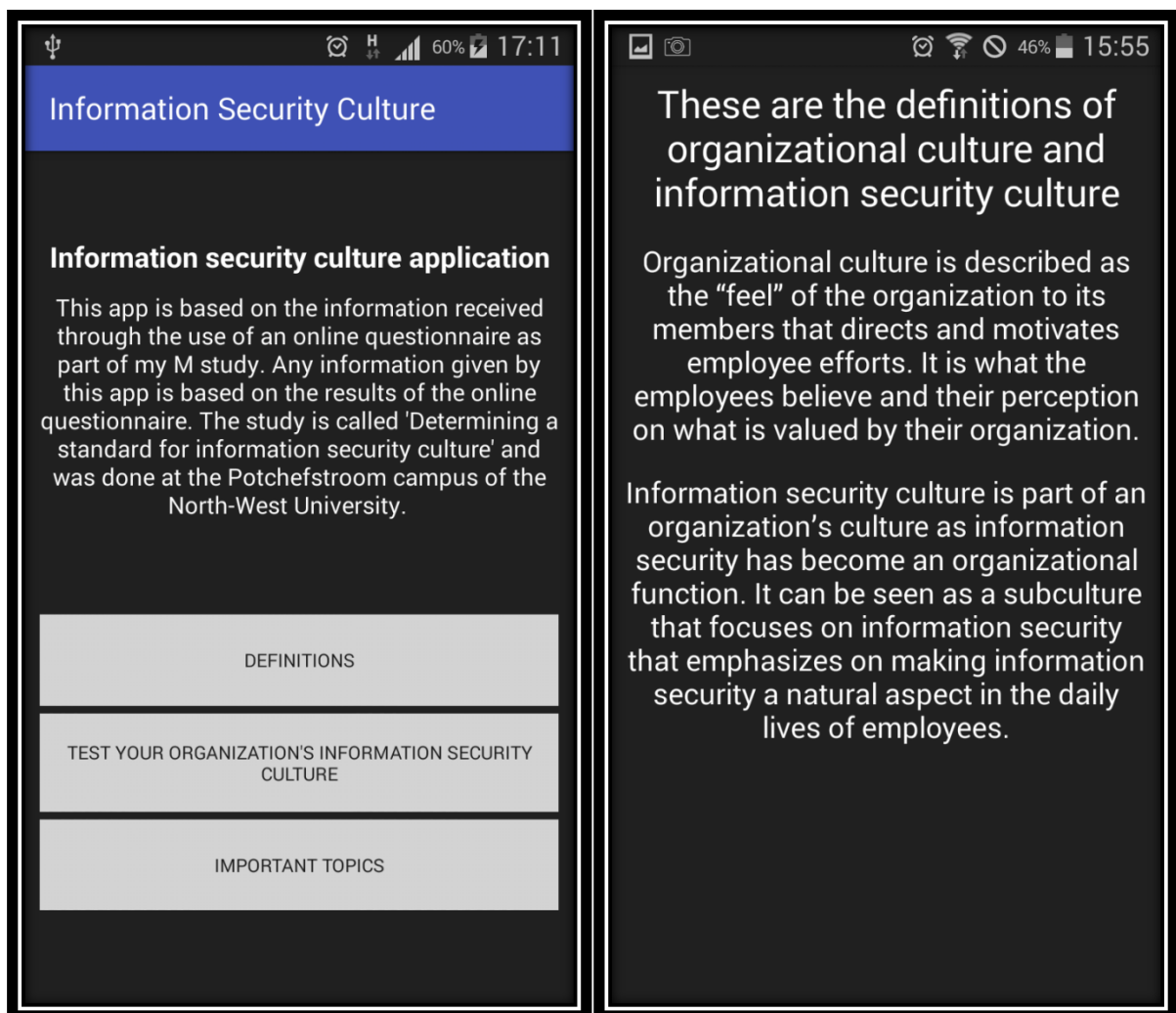
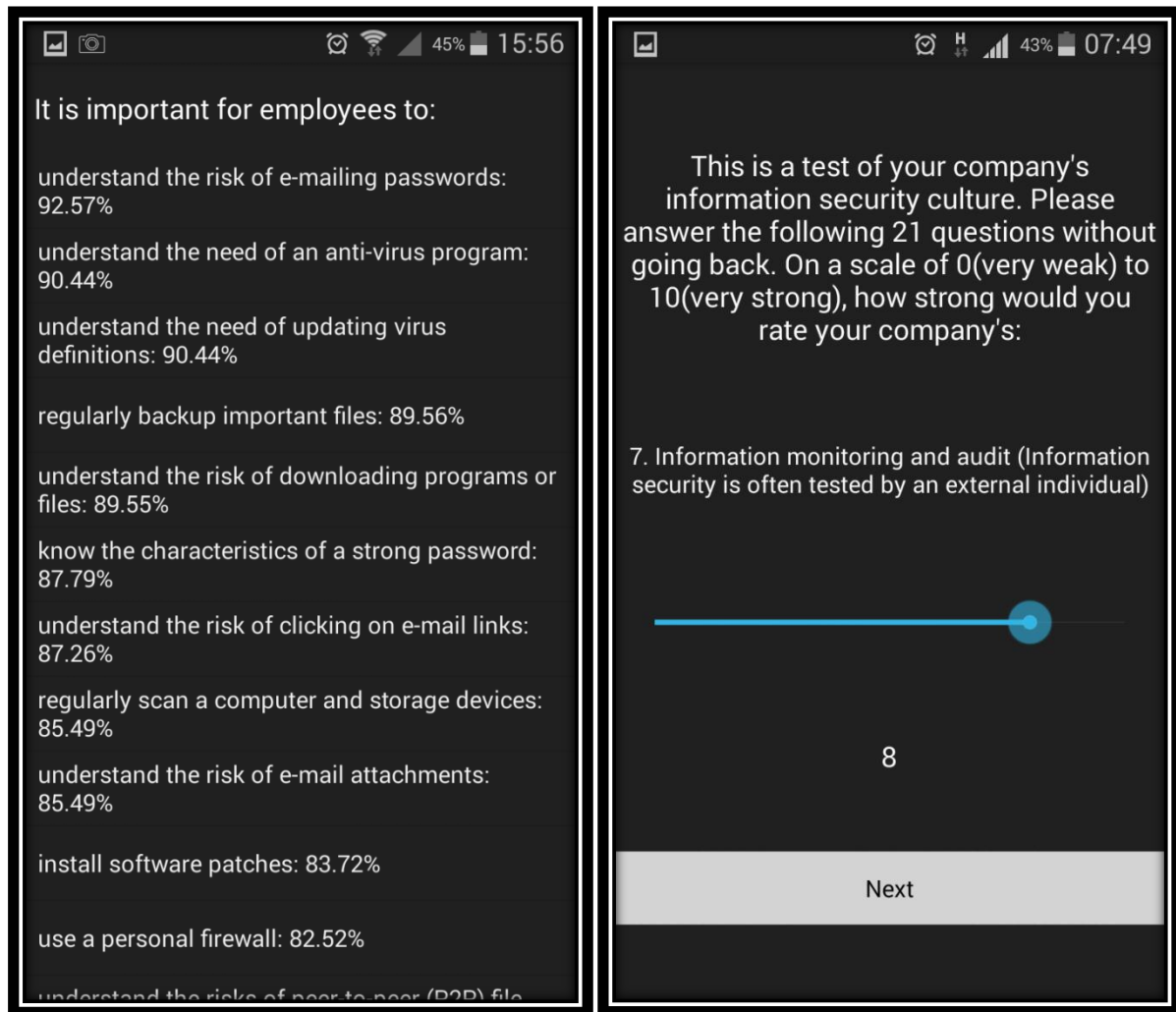


Figure 5.2: Application Home Page and Definitions Page

The Important topics page presents the data from the framework in an informative page. This is presented in Figure 5.3.

The button “Test your organisations information security culture” leads to a page where a user is asked how strongly he/she believes his/her organisation relates to a specific information security culture aspect. This is repeated with each of the 21 information security culture aspects, each aspect accompanied with an appropriate definition. This is followed by a drag-bar where the user can choose a value from 0 (very weak) to 10 (very strong). The value chosen is displayed along with a button that goes to the next aspect and definition. Once all aspects have been rated, the button transfers the user to the results page.



**Figure 5.3: Application Important Topics and Culture Aspect Testing Page**

The results page informs the user that the results are based on this study and that the percentage given can range from below 0% (-32.54%) if all the aspects have been rated 0 and up to above 100% (134.13%) if all the aspects have been rated 10. The strength is rated so that if all aspects are at their minimum baseline, the user will be at 100%. The user is presented with one of the following messages, depending on the information security culture:

- For values below 60%, the message is "Your security culture is abysmal".

- For values between 60% and 80%, the message is "You have reason to worry".
- For values between 80% and 90%, the message is "Your security culture could use some work".
- For values between 90% and 105%, the message is "Your security culture is acceptable".
- For values above 105%, the message is "Your security culture is excellent, absolutely brilliant".

The percentage is calculated as follows:

If x is the sum of the security culture baseline/standard, and y is the sum of the culture values given by the user, then the information security culture (ISC) strength is calculated as:

$$ISC\% = \frac{(y - x/21) + 6}{6}$$

Table 5.6 demonstrates the calculation of the formula.

Aspect Number:	1	2	3	4	5	6	7	8	9	10	11
Baseline (/10)	8.42	8.24	8.58	7.08	7.46	8.14	6.96	7.4	8.1	7.6	8.3
Aspect Number	12	13	14	15	16	17	18	19	20	21	
Baseline (/10)	7.82	7.7	8.14	7.74	7	8.24	8.84	8.92	8.42	7.9	
If all of the users values are =											
	0	1	2	3	4	5	6	7	8	9	10
Then y-x=	-167	-146	-125	-104	-83	-62	-41	-20	1	22	43
(y-x)/21	-7.95	-6.95	-5.95	-4.95	-3.95	-2.95	-1.95	-0.95	0.05	1.05	2.05
((y-x)/21)+6	-1.95	-0.95	0.05	1.05	2.05	3.05	4.05	5.05	6.05	7.05	8.05
ISC	-0.325	-0.159	0.008	0.175	0.341	0.508	0.675	0.841	1.008	1.175	1.341
in percentage:	-32.5%	-15.9%	0.8%	17.5%	34.1%	50.8%	67.5%	84.1%	100.8%	117.5%	134.1%

**Table 5.6: ISC Percentage Calculation**

Figure 5.4 presents the results page screen of the application. At first the results are not shown; only the text and the button are visible. When the user clicks on the button, the results are presented in a list. The results are sorted from the strongest aspect to the weakest aspect. The user can scroll up and down the list. The value presented to the user is an indication of how much the user's organisation is over/under the standard/baseline.

Once the user is on the results page, he/she can click on a specific culture aspect to view the preferred delivery methods for that aspect. The last screen (delivery methods) presents the delivery methods in simple text format. This is presented in Figure 5.5.

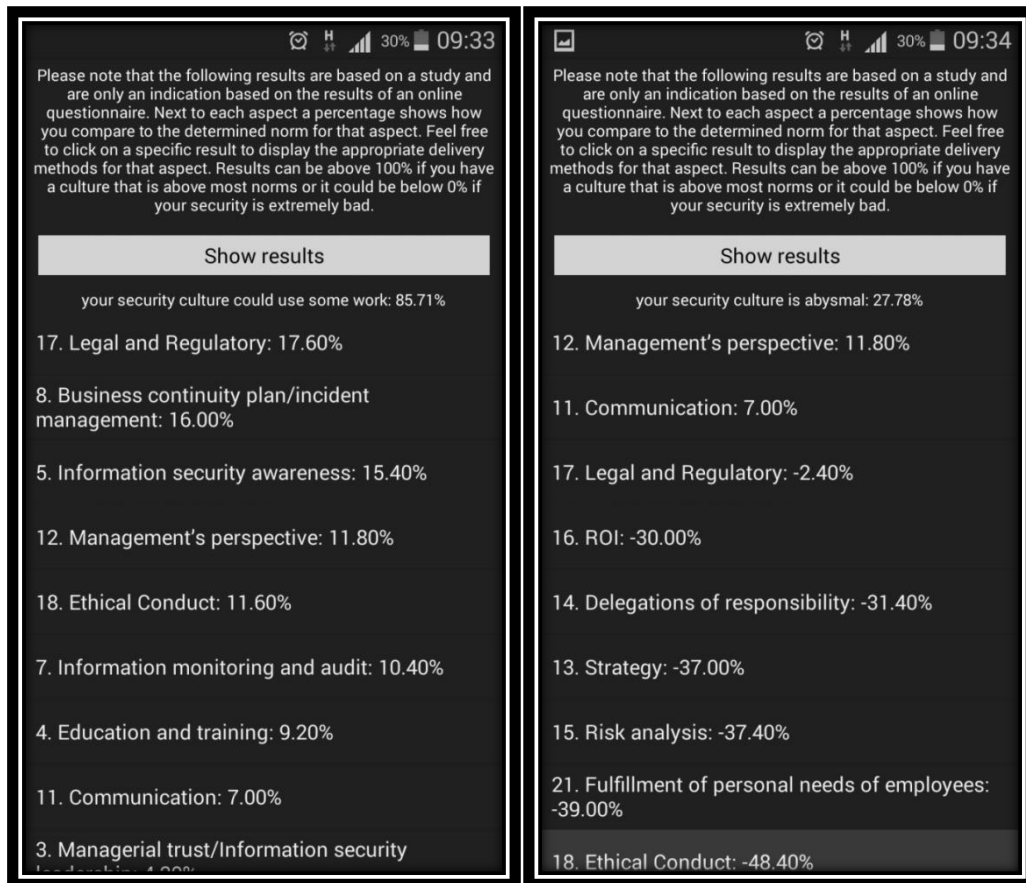


Figure 5.4: Application Results Page

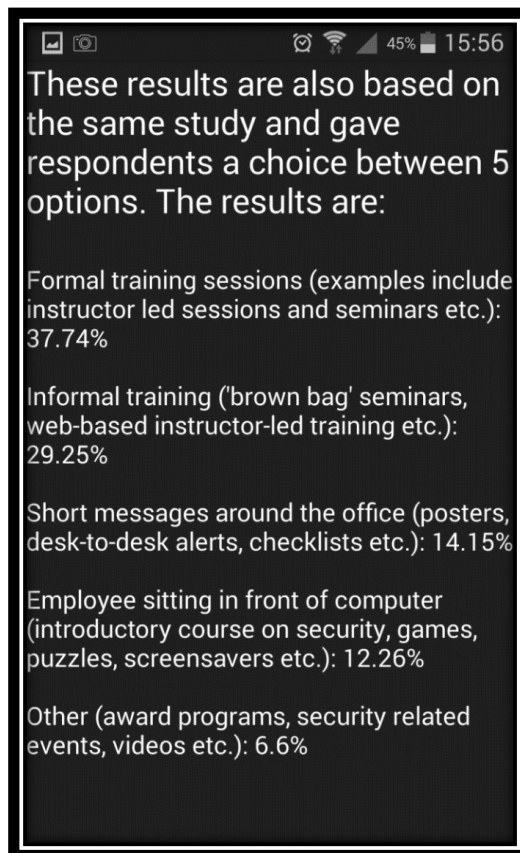


Figure 5.5: Application Delivery Methods Page



The user can use the mobile phone's "Back" button at any point to return to the home/main screen. Screen rotation is disabled for the comfort of the user. The application is available in the Google Play store under the name "Information Security Culture". It is downloadable free of charge.

This application was sent to all questionnaire respondents who indicated that they are interested in the results of the questionnaire. They were invited to leave some comments or feedback regarding the application in order to evaluate whether it achieves its aim. Although the evaluation was not done by many respondents, it is evident that the application works well and has a simple and user-friendly design. The feedback includes:

- 4 Stars – Useful app looking at research results.
- 5 Stars – **Nice app** Very insightful App. Good job, I am impressed.
- 5 Stars – **Very useful and user friendly.** I found it very easy to determine which areas of my security needed work, the app is void of useless bells and whistles, which is something I like. Definitely a must have for small business owners and medium sized companies that are looking to improve security culture without hiring expensive consultants etc.

This section described the application that was developed based on the framework. The next section is a brief summary of this chapter.

### 5.3 Summary

This chapter described the framework for organisational information security culture. The framework is divided into several tables, presenting a baseline/standard for each of the 21 security aspects that should be achieved, delivery methods to achieve the aspect, and important topics to be included in training programmes.

The framework is also used to create a mobile application that applies the framework and can be used to test the security culture strength of an organisation. The framework advises the user on how to improve his/her organisations security culture.

The next chapter is the summary and conclusion of the study. This chapter will describe how the aims of this study were reached, what the results were, what contributions were made, the limitations of this research, and possible future work that can be conducted.

## 6 CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

Figure 6.1 shows that this chapter concludes the study, stating how the aims were met, what results were found, the contributions made, the limitations on this study, and possible future research that can be grounded on this study. The first section describes the aims of this study and how they were met.

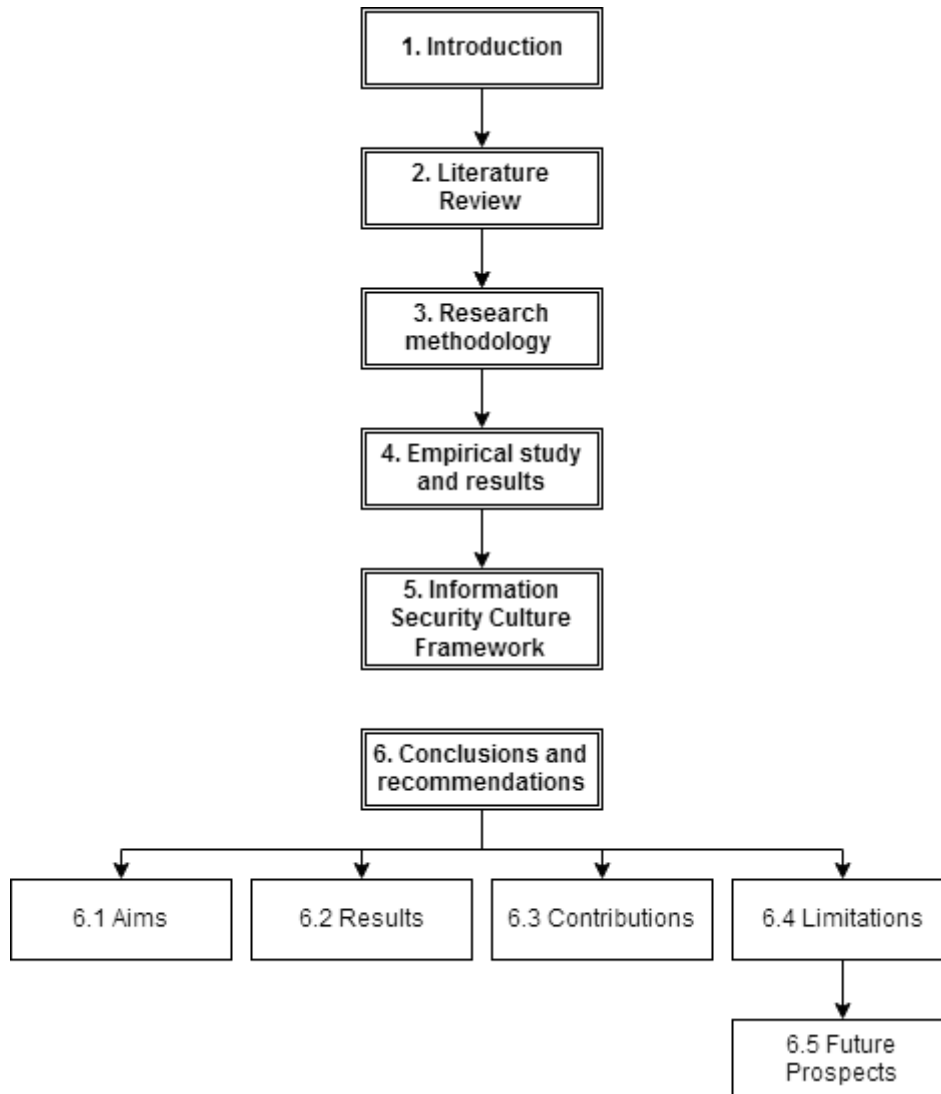


Figure 6.1: Introduction Chapter 6

### 6.1 Aims

This section describes how the aims stated in Chapter 1 have been achieved. Each aim is listed, followed by an explanation of how it was met.

- **Investigate organisational culture and information security culture as well as determining important aspects of information security culture**

In the literature review, various information security culture aspects, measuring mechanisms, and objectives were investigated. By combining these aspects, mechanisms and objectives from six studies, a list of 21 information security culture aspects was created, categorised into three groups. These groups are rated according to the number of times each aspect was found in the reviewed studies and provide an indication of how important each is. This aim is addressed in Section 2.3.

- **Use these aspects within different organisations to determine an acceptable baseline/ standard**

The online questionnaire was answered by 113 people and provided a baseline for the study. The respondents of the questionnaire were asked to rate the importance of each of the identified aspects. This provided an importance rating out of five for every aspect; this importance rating is also shown as a percentage in the framework presented. This aim is addressed in Section 4.1.2.

- **Identify delivery methods of training/awareness in literature and within organisations relating to information security culture**

The delivery methods were identified from various sources during the literature review, mainly Wilson and Hash (2003). Most of these sources provide guidance in the creation of an awareness and training programme. Various delivery methods were investigated, both for a short term awareness course and for a more permanent training event. The possibility of buying a pre-packaged awareness and training programme was also mentioned. This aim is addressed in Section 2.4.2.

- **Investigate which training/awareness delivery methods can be used to improve each identified information security culture factor in order to reach the identified standard/baseline**

To avoid confusion in the questionnaire, the long list of delivery methods identified in the literature review were summarised into five options. Respondents were asked to indicate the preferred delivery method from the list of five for each information security culture aspect. Respondents were also asked whether there are any other delivery methods not identified by the study; these responses are included in the framework. This aim is addressed in Section 4.1.3.

- **Identify important topics of an awareness and training programme in literature and in organisations**

The work of Wilson and Hash (2003) was the main source used in the study as it provides a long list of topics that can be discussed in an awareness and training programme. Kim (2014) shortened this list to the most important topics. This list was used in the questionnaire. Respondents were asked to rate the importance of each identified important topic, as well as naming other topics they believe are important that were not included in the list. This aim is addressed in Section 2.4.1.

- **Use the results of the security culture aspects, delivery methods, and important topics to create a framework for security culture in organisations**

The final framework combines the security culture aspects, delivery methods and important topics into a single framework. The framework is presented in the form of several tables in Chapter 5 and is used as the foundation for the creation of a mobile application for this study. The framework indicates the importance of each of the 21 identified information security culture aspects and identifies which delivery methods are preferred to improve each aspect. The framework further provides the perceived importance ratings of the identified important topics. This aim is addressed in Sections 4.3 and 5.1.

This section described how the aims of this study were achieved. The next section describes the results of this study.

## 6.2 Results

This section summarises the results of this study. From the literature reviewed, 21 information security culture aspects were identified (policy, compliance, managerial trust/information security leadership, education and training, information security awareness, information asset management, information monitoring and audit, business continuity plan/incident management, information security programme, change management, communication, managements' perspective, strategy, delegation of responsibility, risk analysis, ROI, legal and regulatory, ethical conduct, accountability, fairness towards employees, and fulfilment of personal needs of employee). Of these aspects, *accountability* was rated by the respondents as the most important, closely followed by *ethical conduct*. *Information monitoring and audit* is considered the least important aspect. Several other information security culture aspects were added by respondents.

For each aspect, the preferred delivery method was identified. Most aspects have *formal training* (instructor led sessions, seminars etc.) as the ideal delivery method, followed by

*informal training* ("Brown bag" seminars, web-based instructor-led training etc.). This is followed by *short messages around the office* (posters, desk-to-desk alerts, checklists etc.) and *employee sitting in front of computer* (introductory course on security, games, puzzles, screensavers etc.). The least preferred delivery method is *other* (award programmes, security related events, videos etc.). Respondents named additional delivery methods that can be considered, including face-to-face, using a combination of delivery methods, and a mentoring system.

A long list of important topics in an awareness and training programme was compiled. This list was subsequently shortened to 18 items that is important for employees to do/understand (to understand the need of an anti-virus program; to understand the need of updating virus definitions; to regularly scan a computer and storage devices; to use a personal firewall; to install software patches; to use pop-up blockers; to understand the risk of downloading programs or files; to understand the risks of P2P file sharing; to understand the risk of clicking on e-mail links; to understand the risk of e-mailing passwords; to understand the risk of e-mail attachments; to regularly backup important files; to understand the risk of smartphone viruses; to understand the need of anti-virus program for a smart phone; to know the characteristics of a strong password; to use different passwords for different systems; and to change passwords regularly). All these topics were rated by the respondents and *understanding the risk of emailing passwords* was regarded as the most important topic. The least important topic is *understanding the need of anti-virus program for a smart phone*. Other topics were added in the course of the study as stated by respondents, including ransomware and clean desk policy.

This section summarised the results of this study, although specific statistical interpretations are presented in Chapter 4. The next section presents the contribution made by the study.

### **6.3 Contributions**

This section describes the contribution/original value of this study.

The first contribution is conceptual model found in Section 2.3.3. This framework is compiled by comparing different literature studies and contains 21 identified information security culture aspects. Each aspect is accompanied by a clear definition, as well as a basic idea of how important it is based on the number of times it was found in previous studies.

The final framework is the second contribution of this study. The framework allows an organisation to compare its own information security culture to a set of baseline values for 21 different information security culture aspects. Both the list of aspects and the minimum

baseline/importance rating for each of these aspects are results from this study. The framework is seen in Tables 5.1 to 5.5.

For each information security culture aspect included in the initial framework, there is a list of five possible delivery methods and a percentage indicating the preference for each. Additional delivery methods and aspects that should be considered are also mentioned. Important information security topics that should be considered when building an information security awareness and training programme is included in the framework, each accompanied by an importance rating. This framework can be used to increase the security culture of an organisation and can also be used further in future research.

The third contribution is the mobile application. Based on the framework, it provides an interactive method to measure an organisation's security culture as well as offering guidelines to choose delivery methods for each aspect. The application is available on the Google Play store under the name "Information Security Culture" and is available for download at no cost (refer to Section 5.2).

The outputs that resulted from this study are the dissertation, a presentation as part of an MSc workshop, as well as an article that will be submitted to the 'Information and Computer Security' Journal.

This section described the contributions of this study. The next section presents the limitations of this research.

## **6.4 Limitations**

This section describes the limitations of this research and how it might have affected the results.

There were many limitations to this study. These limitations are:

- There were only 113 respondents. Ideally the questionnaire should have been completed by at least 200 respondents, making it possible to apply better statistical analyses regarding organisation type, organisation size, employment level etc.
- With a single exception, all respondents are South African. The responses might have resulted in a different framework if respondents were found on a global scale.
- The additional security culture aspects, delivery methods, and important topics cannot be rated because they were added to the study at the end of the questionnaire.

This section described the limitations on this study. The next section presents possible future aspects that can be researched based on this study.

## **6.5 Future Work**

This section presents possible future prospects that can be endeavoured. Each of the limitations can be investigated in order to improve this study or conduct a new study. A similar framework can be created with sections for organisation type, organisation size, employment level and geographical location. The additional information security culture aspects, delivery methods and important topics found in this study can be included in a new survey in order to be considered for rating and evaluation by respondents.

## BIBLIOGRAPHY

- AlHogail, A. 2015. Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575.
- AlHogail, A., & Mirza, A. 2014. Information security culture: A definition and a literature review. *Computer Applications and Information Systems (World Congress on Computer Applications and Information Security)*.
- Banerjee, C. & Pandey, S. K. 2010. Research on software security awareness: Problems and prospects. *Special Interest Group on Software Engineering (ACM) Software Engineering Notes*, 35(5), 1-5.
- Beck, K. 1999. Embracing Change with Extreme Programming. *Computer (IEEE)*, 32(10) 70-77
- Bryman, A. 2006. Integrating quantitative and qualitative research: How is it done? *Qualitative research*, 6(1), 97-113.
- Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly*, 34(3), 523-548.
- Cooper, D. & Schindler, P. 2014. Business research methods. 12th ed. United States of America: McGraw-Hill Irwin. 679p.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. 2013. Future directions for behavioural information security research. *Computers & Security*, 32, 90-101.
- Da Veiga, A. & Eloff, J. 2010. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.
- Da Veiga, A. & Martins, N. 2015. Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, 31(2), 243-256.
- Da Veiga, A., Martins, N. & Eloff, J. H. 2007. Information security culture – Validation of an assessment instrument. *Southern African Business Review*, 11(1), 147-166.
- Dhillon, G. & Torkzadeh, G. 2006. Value-focused assessment of information system security in organisations. *Information Systems* 16(3), 293-314.



Field, A. 2013. Discovering statistics using IBM SPSS statistics. 4<sup>th</sup> ed. London: Sage Publications. 916p.

Guba, E. G., ed. 1990. The paradigm dialog. Newbury Park California: Sage Publications. 427p.

Henning, V. R. 2004. Research methodology and design, 1. [http://uir.unisa.ac.za/bitstream/handle/10500/4245/05Chap%204\\_Research%20methodology%20and%20design.pdf](http://uir.unisa.ac.za/bitstream/handle/10500/4245/05Chap%204_Research%20methodology%20and%20design.pdf). Date of access: 16 October 2016.

Herath, T. & Rao, H. R. 2009. Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 42(2), 154-165.

Katsikas, S. K. 2000. Health care management and information systems security: awareness, training or education? *International Journal of Medical Informatics*, 129-135.

Kim, E.B. 2014. Recommendations for information security awareness training for college students. *Information Management & Computer Security*, 22(1), 115-126. Klein, H. & Myers, M.

2001. A classification scheme for interpretive research in information systems. *Qualitative Research in Information Security: Issues and Trends*, 218-239.

Krauss, S. E. 2005. Research paradigms and meaning making: A primer. *The Qualitative Report*, 10(4), 758-770.

Mackenzie, N. & Knipe, S. 2006. Research dilemmas: Paradigms, methods and methodology. <http://www.iier.org.au/iier16/mackenzie.html>. Date of access: 03 June 2016.

McCoy, C. & Fowler, R. T. 2004. You are the key to security: Establishing a successful security awareness program. *Proceedings of the 32<sup>nd</sup> Annual ACM Special Interest Group on University & College Computing Services conference on user services*.

Mertens, D. M. 2014. Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods. 4th ed. Thousand Oaks California: Sage Publications. 511p.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N. & Skourlas, C. 2014. The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, 147, 424-428.

- Munteanu, A.B. & Fotache, D. 2015. Enablers of information security culture. *Procedia Economics and Finance*, 20, 414-422.
- O'Brien, J., Islam, S., Bao, S., Weng, F., Xiong, W. & Ma, A. 2013. Information security culture: literature review. The University of Melbourne.
- Oates, B. J. 2006. Researching information systems and computing. 1<sup>st</sup> ed. Thousand Oaks California: Sage Publications. 326p.
- Orlikowski, W. J. & Baroudi, J. J. 1991. Studying information technology in organisations: Research approaches and assumptions. *Information systems research*, 2(1), 1-28.
- Peltier, T. R. 2005. Implementing an information security awareness program. *Information Systems Security*, 14(2), 37-49.
- Pfleeger, C. P., Pfleeger, S. L.N. & Margulies, J. 2015. Security in computing. 5th ed. Upper Saddle River, New Jersey: Prentice Hall. 877p.
- PricewaterhouseCoopers. 2015. Information security breaches survey. Executive summary. <http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html>. Date of access: 10 June 2016.
- Puhakainen, P. & Siponen, M. 2010. Improving employees' compliance through information systems security training: an action research study. *Management Information Systems Quarterly*, 757-778.
- Saint-Germain, R. 2005. Information security management best practice based on International Organisation for Standardization/International Electrotechnical Commission 17799. *Information Management Journal*, 39(4), 60-66.
- Schein, E. H. 1999. The corporate culture survival guide. San Francisco: John Wiley & Sons-Jossey-Bass. 223p.
- Schneider, B., Brief, A. P. & Guzzo, R. A. 1996. Creating climate and culture for sustainable organisational change. *Organisational Dynamics*, 24 (4):7-19.
- Shaw, R. S., Chen, C. C., Harris, A. L. & Hui-Jou, H. 2009. The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52(1), 92-100.

- Singh, N., Gupta, A. M. & Ojha, A. 2014. Identifying factors of “organisational information security management”. *Journal of Enterprise Information Management*, 27(5), 644-667.
- Thomson, K.-L., von Solms, R. & Louw, L. 2006. Cultivating an organisational information security culture. *Computer Fraud & Security*, 10, 7-11.
- Tribe, J. 2001. Research paradigms and the tourism curriculum. *Journal of Travel Research*, 39(4), 442-448.
- Valentine, J. A. 2006. Enhancing the employee security awareness model. *Computer Fraud & Security*, 6, 17-19.
- Van Den Steen, E. 2003. On the origin and evolution of corporate culture. *Research and Development Journal of Economics*, 41(4):617-648.
- Van Niekerk, J. & Von Solms, R. 2010. Information security culture: A management perspective. *Computers & Security*, 29(4), 476-486.
- Whitman, M. E. & Mattord, H. J. 2016. Principles of information security. 5 ed. Boston: Cengage Learning. 656p.
- Williams, C. 2007. Research methods. *Journal of Business & Economic Research*, 5(3), 65-72.
- Wilson, M. & Hash, J. 2003. Building an information technology security awareness and training program. Gaithersburg: National Institute of Standards and Technology (NIST). 70p.

## 7 APPENDIX A: Certificate of language editing

### CERTIFICATE OF EDITING

This certifies that the manuscript

Determining a standard for information security culture

by the author

Frans Nel

has been edited for English language usage.

I have read through his manuscript and indicated all deviations from customary academic English. I also checked punctuation and improved where required. It remains the responsibility of the author to accept all recommended changes to the manuscript.

Prof Marthie Grobler (Mrs), PhD, CISM

[grobler.postgraduate@gmail.com](mailto:grobler.postgraduate@gmail.com)

9 November 2016

Pretoria, South Africa

---

Date

---

Place

## 8 APPENDIX B: QUESTIONNAIRE

### Determining a standard for information security culture

To whom it may concern

Research project on: Determining a standard for information security culture

I am currently enrolled for my Master's degree in Computer Science at the Potchefstroom campus of the North-West University. I am conducting a study about information security culture in organizations. You are invited to take part in this research project by completing the accompanying questionnaire.

This should only take 10 to 15 minutes to complete.

Contact Details:

Frans Nel (MSc Student)

Email: [snarfnel@gmail.com](mailto:snarfnel@gmail.com)

Supervisor: Dr L Drevin

Email: [lynette.drevin@nwu.ac.za](mailto:lynette.drevin@nwu.ac.za)

**\*Required**

### Key terms and aims of this study

Key terms:

Organizational culture is described as the “feel” of the organization to its members that directs and motivates employee efforts. It is what the employees believe and their perception on what is valued by their organization.

Information security culture is part of an organization's culture as information security has become an organizational function. It can be seen as a subculture that focuses on information security that emphasizes on making information security a natural aspect in the daily lives of employees.

Aims of this study:

To learn what organizations see as the minimum acceptable baseline of each information security culture aspect.

Learn which training and awareness delivery methods are preferred to improve each information security culture aspect.

And rate the importance of awareness and training topics as seen by modern organizations.

Please read the following general principles as it is important that you understand what you are agreeing to:

1. Your participation in this research project is completely voluntary, and no pressure, however subtle, may be placed on you to take part.
2. It is possible that you may not gain any benefit personally from your participation in the research project, although the knowledge that you provide may benefit other persons or communities.
3. You are free to withdraw from the research project at any time, without giving reasons for your decision. You will in no way be harmed in doing so. You may also request that your information provided, no longer be used in the research project. However, you are kindly requested not to withdraw from the project without careful consideration, since it may have a negative effect on the reliability of the project.
4. By agreeing to take part in the research project, you are also giving consent for the data that will be generated to be used by the researchers for scientific purposes as they see fit, with the agreement that it will be confidential and that your name will not be linked to any of the data without your consent.

By completing the accompanying questionnaire, you agree that you have read the previous information in connection with the research project and that you understand it. You also declare that you are taking part in the project voluntarily.

#### 1. Untitled Question \*

*Tick all that apply.*

☐ I have read and understand the general principles

## Part 1: Biographical Details

Please fill in all the fields.

### 2. Age (in years)

\_\_\_\_\_

### 3. Gender

*Mark only one oval.*

- ☐ Male
- ☐ Female
- ☐ Other: \_\_\_\_\_

### 4. Level of education

*Mark only one oval.*

- ☐ High School Diploma (Upper secondary education)
- ☐ Post-secondary non-tertiary education
- ☐ Bachelor or equivalent
- ☐ Master or equivalent
- ☐ Doctoral or equivalent
- ☐ Other: \_\_\_\_\_

### 5. Level of employment

*Mark only one oval.*

- ☐ Top Level Management
- ☐ Middle Management
- ☐ Admin
- ☐ Technical
- ☐ Other: \_\_\_\_\_

### 6. Years of computer experience

*Mark only one oval.*

- ☐ 0 - 2 years
- ☐ 3 -5 years
- ☐ 6 - 8 years
- ☐ >8 years

### 7. Do you live in a urban(city) or rural(town) area

*Mark only one oval.*

- ☐ Urban (Major cities like Cape town or Johannesburg)
- ☐ Rural(Smaller towns like Potchefstroom or Bethlehem)
- ☐ Other: \_\_\_\_\_

## 8. Type of organization (core business)

Mark only one oval.

- ☐ Civil
- ☐ Finance
- ☐ I.T.
- ☐ Sales
- ☐ Admin
- ☐ Academic/Education
- ☐ Other: \_\_\_\_\_

## 9. Number of Employees in organization

Mark only one oval.

- ☐ 1 - 10
- ☐ 11 - 50
- ☐ 51 - 200
- ☐ 201 - 500
- ☐ 501 - 1000
- ☐ >1000

## Information security culture aspects

The aim of this section is to learn what organizations see as the minimum acceptable baseline of each information security culture aspect. Please rate how important the following aspects of information security culture is for employees in your organization. In all the following questions, the scale is 1 (not important), 2 (somewhat important), 3 (important), 4 (very important), 5 (extremely important).

### 10. 1. Policy (The data policy describes all procedures, standards, guidelines, and best practices)

Mark only one oval.

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

### 11. 2. Compliance (Employees comply to security protocols and know that there are clear reprisals to noncompliance)

Mark only one oval.

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

### 12. 3. Managerial trust/Information security leadership (Employees know that managers also adhere to security protocols)

Mark only one oval.

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

13. **4. Education and training (Regular training and awareness programs are run to ensure all employees know how to respond to security threats)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

14. **5. Information security awareness (Continuous awareness programs to keep employees up to date on security threats)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

15. **6. Information asset management (Employees understand the value of information in the organization and how vulnerable a resource it can be)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

16. **7. Information monitoring and audit (Information security is often tested by an external individual)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

17. **8. Business continuity plan/incident management (Procedures describing actions to be taken in the event of an information security incident)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

18. **9. Information security program (Technical and physical elements used to protect assets)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important



19. **10. Change management (Employees should be encouraged to be open to change in the organization)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

20. **11. Communication (Clear lines of communication between employees, management, and security officers).**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

21. **12. Management's perspective (Those in managerial positions are willing to contribute time, effort and money into the program.)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

22. **13. Strategy (Leaders should have a clear strategy on implementing a awareness and training program.)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

23. **14. Delegations of responsibility (Specific tasks are delegated to employees in such a way that all employees are sure of their roles)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

24. **15. Risk analysis (All potential risks to information assets are analyzed and managed in such a way that security protocols are set according to the value of assets and the potential security threat s to each of them)**

*Mark only one oval.*

	1	2	3	4	5	
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	extremely important

25. **16. ROI - return on investment (Leaders in the organization should see how investing in information security training returns a financial gain to the organization)**

*Mark only one oval.*

1	2	3	4	5
---	---	---	---	---

not important ☐ ☐ ☐ ☐ ☐ extremely important

26. **17. Legal and Regulatory (Employees should be aware of the legal consequences of security breaches and how it can affect them)**

*Mark only one oval.*

1 2 3 4 5

not important ☐ ☐ ☐ ☐ ☐ extremely important

27. **18. Ethical Conduct (Employees should be encouraged to behave in an ethical manner towards each other and all organizational assets)**

*Mark only one oval.*

1 2 3 4 5

not important ☐ ☐ ☐ ☐ ☐ extremely important

28. **19. Accountability (Employees should be encouraged to take accountability for their own actions without constant managerial supervision)**

*Mark only one oval.*

1 2 3 4 5

not important ☐ ☐ ☐ ☐ ☐ extremely important

29. **20. Fairness towards employees (Managers and employees in leadership positions should focus on being fair to lower level employees in terms of work allocation and rewards for good services)**

*Mark only one oval.*

1 2 3 4 5

not important ☐ ☐ ☐ ☐ ☐ extremely important

30. **21. Fulfillment of personal needs of employees (By spending some resources into the personal needs of employees, an organization can once again improve their loyalty and reduce the risk of intentional harm from employees)**

*Mark only one oval.*

1 2 3 4 5

not important ☐ ☐ ☐ ☐ ☐ extremely important

31. **Are there any aspects not mentioned here that you believe is important? If yes, please name these aspects and give a rating to each of 1 (not important) to 5 (extremely important).**

---

---

---

---

32. Please give any comments or feedback that you might have regarding this aspect of your company.

---

---

---

---

---

## Awareness and Training delivery methods

This section is to learn which training and awareness delivery methods are preferred to improve each information security culture aspect. Please mark your preferred delivery method that you would choose to use to improve each information security aspect. The definitions of each security aspect term are the same as in part 2.

33. **1. Policy**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

34. **2. Compliance**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

35. **3. Managerial trust/Information security leadership**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**36. 4. Education and training**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**37. 5. Information security awareness**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**38. 6. Information asset management**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**39. 7. Information monitoring and audit**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**40. 8. Business continuity plan/incident management**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**41. 9. Information security program**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**42. 10. Change management**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**43. 11. Communication**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**44. 12. Management's perspective**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**45. 13. Strategy**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**46. 14. Delegations of responsibility**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**47. 15. Risk analysis**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**48. 16. ROI (return on investment)**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**49. 17. Legal and Regulatory**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**50. 18. Ethical Conduct**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.)
- ☐ Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**51. 19. Accountability**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.) Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**52. 20. Fairness towards employees**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.) Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**53. 21. Fulfillment of personal needs of employee**

*Mark only one oval.*

- ☐ Formal training sessions (examples include instructor led sessions and seminars etc.) Informal training ("brown bag" seminars, web-based instructor-led training etc.)
- ☐ Short messages around the office (posters, desk-to-desk alerts, checklists etc.)
- ☐ Employee sitting in front of computer (introductory course on security, games, puzzles, screensavers etc.)
- ☐ Other (award programs, security related events, videos etc.)

**54. Are there any delivery methods not mentioned here that you believe is important? If yes, please name them and supply the number of the aspects (1-21) you would improve using them.**

---

---

---

---

---

**55. Please give any comments or feedback that you might have regarding this aspect of your company.**

---

---

---

---

---

## Important topics of Awareness and Training programs

This section aims to rate the importance of awareness and training topics as seen by modern organizations. In all the following questions, the scale is 1 (not important), 2 (somewhat important), 3 (important), 4 (very important), 5 (extremely important). Please rate how important it is for employees to:

### 56. understand the need of an anti-virus program

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

### 57. understand the need of updating virus definitions

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

### 58. regularly scan a computer and storage devices

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

### 59. use a personal firewall

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

### 60. install software patches

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

### 61. use pop-up blockers

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important



**62. understand the risk of downloading programs or files**

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**63. understand the risks of peer-to-peer (P2P) file sharing**

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**64. understand the risk of clicking on e-mail links**

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**65. understand the risk of e-mailing passwords**

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**66. understand the risk of e-mail attachments**

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**67. regularly backup important files**

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**68. understand the risk of smartphone viruses**

*Mark only one oval.*

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**69. understand the need of anti-virus program for a smart phone**

Mark only one oval.

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**70. know the characteristics of a strong password**

Mark only one oval.

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**71. use different passwords for different systems**

Mark only one oval.

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**72. change passwords regularly**

Mark only one oval.

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**73. understand legal, regulatory and ethical issues of information security**

Mark only one oval.

	1	2	3	4	5
not important	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> extremely important

**74. Are there any topics not mentioned here that you believe is important? If yes, please name these topics and give a rating to each of 1 (not important) to 5 (extremely important).**

---

---

---

---

---

**75. Please give any comments or feedback that you might have regarding this aspect of your company.**

---

---

---

---

---

## Thank you

I thank you for your participation, time, and valuable contribution to this project. Your participation is greatly appreciated.

Frans Nel (MSc Student) Email:

[snarfnel@gmail.com](mailto:snarfnel@gmail.com) Supervisor: Dr L Drevin

Email: [lynette.drevin@nwu.ac.za](mailto:lynette.drevin@nwu.ac.za)

Please fill in the last 2 questions

**76. I am confident that my company has a strong information security culture. \***

*Mark only one oval.*

	1	2	3	4	5	
severely pessimistic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	very confident

**77. I am confident that I have a strong knowledge/insight on these topics. \***

*Mark only one oval.*

	1	2	3	4	5	
severely pessimistic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	very confident

**78. Please give any comments or feedback that you might have regarding this questionnaire.**

---

---

---

---

---

---

Powered by

