

bradscholars

Organisational information security management: The impact of training and awareness. Evaluating the socio-technical impact on organisational information security policy management.

Item Type	Thesis
Authors	Waly, Nesren Saleh
Rights	<p>
The University of Bradford theses are licenced under a Creative Commons Licence.</p>
Download date	2026-03-05 23:26:07
Link to Item	http://hdl.handle.net/10454/5666



University of Bradford eThesis

This thesis is hosted in [Bradford Scholars](#) – The University of Bradford Open Access repository. Visit the repository for full metadata or to contact the repository team



© University of Bradford. This work is licenced for reuse under a [Creative Commons Licence](#).

**Organisational information security
management: The impact of training and
awareness**

Evaluating the socio-technical impact on organisational
information security policy management

NESREN SALEH WALY

Submitted for the degree of
Doctor of Philosophy

Department of Computing
School of Computing, Informatics and Media
University of Bradford

2013

Abstract

Security breaches have attracted attention from corporations and scholars alike. The major organisations are determined to stop security breaches as they are detrimental to their success. Arguably the most common factor contributing to these breaches is employee behaviour, which suggests that changes in employee behaviour can have an impact on improving security.

This research aims to study the critical factors (CFs) that impact on employee behaviours toward compliance with their organisation's information security policy. This investigation will focus on the various critical success factors based on their grouping into one of the following three major categories, namely: organisational factors, behavioural factors and training factors. Each of these categories affects a different aspect of information security and the objective is to not only understand the interaction of different factors but also to study further the aims in order to provide practical recommendations for improving organisational information security management.

This study has utilised empirical research through the use of both qualitative and quantitative methodologies to inform each stage of the research. This study focused on the health, business and education sectors by empirically evaluating the obstacles and success factors that affect employee compliance to organisational security policies. In addition, this study also evaluated the affect of the socio-technical impact on organisational information security management. The final stage of the research focused on developing an effective training and awareness programme. This training programme was constructed by incorporating the techniques that were identified as enhancing employee perceptions, attitudes and motivations, in order to facilitate a better transference of skills and more sustainable and appropriate behaviours to improve organisational information security management in the workplace. The techniques utilised included: effective communication, knowledge reinforcement, pre- and post-assessment and motivational techniques.

Keywords

Information security (info-sec), human factors, organisational factors, training, employee behaviour, policy compliance.

Declaration

I hereby declare that this thesis has been genuinely carried out by myself and has not been used in any previous application for a degree. The invaluable participation of others in this thesis has been acknowledged where appropriate.

Nesren Waly

Acknowledgments

**In the name of Allah, the most gracious, the most merciful.
All praise is due to Allah, the Lord of the worlds, and blessings and
peace be upon our prophet Muhammad.**

First, I must express my sincerest gratitude to Allah, I would like to give praise and thanks for making my dreams come true and for providing help in times of difficulty, from sources of which I had never dreamed.

My deepest, overriding and most heartfelt gratitude goes to my loving husband Marwan Gammash, and to my sons for their sacrifices, encouragement and their unbounded and invaluable support throughout my life.

I would like to also express my deepest gratitude to my parents, Saleh Waly and Huda Nooh, for their Duaa and support – their kindness could never be truly rewarded.

My deepest appreciation and thanks go to my research advisers, Dr. Rana Tassabehji and Dr. Mumtaz Kamala, for all of their guidance, comments, encouragement, enthusiasm and support during this period of study. They have been a source of continual inspiration throughout my research and without their guidance, comments and encouragement, much of this work would not have been possible.

My deep and abiding respect and appreciation goes out to all of those who helped to provide all of the necessary support, guidance and materials that have helped me stay focused throughout this project.

Finally, I would like to send my appreciation and thanks to all of the organisations which participated in this research – I thank you all for your comments, support and participation, all of which has led to the successful accomplishment of this study.

Publications

1. N. Waly, R. Tassabehji and M. Kamala, "Information Security: Critical Training Factors", *The 5th Saudi International Conference*, Coventry, UK. 20th-24th June 2011.
2. N. Waly, R. Tassabehji and M. Kamala, "Measures for Improving Information Security Management in Organisations: The Impact of Training and Awareness", *The 17th UKAIS International Conference on Information Systems (UKAIS)*, Oxford University, Oxford, UK, 26-28th March 2012.
3. N. Waly, R. Tassabehji and M. Kamala, "Improving Organisational Information Security Management: The Impact of Training and Awareness", *14th IEEE International conference on High Performance Computing and Communication*, published by IEEE, Liverpool, UK. 25th-27th June 2012, ISBN: 978-0-7695-4749-7/12.

Contents

Abstract.....	i
Keywords	i
Declaration.....	ii
Acknowledgments.....	iii
Publications.....	iv
Contents	v
Table of Figures	xv
List of Tables.....	xvi
Chapter 1: Introduction	1
1.1 Background.....	1
1.2 Problem Statement.....	3
1.3 Research Questions	6
1.4 Research Aims	6
1.5 Research Objectives.....	7
1.6 Research Structure.....	8
1.6.1 Thesis Outline	9
1.7 Research Approach	11
Chapter 2: Literature Review	12
2.1 Introduction	12

2.2	Information Security Management	12
2.3	Organisational Factors	14
2.4	Information Security Policy	16
2.4.1	Policy Procedure	18
2.4.2	Role and Responsibility	20
2.4.3	Communication and Documentation	21
2.4.4	Employee Involvement	23
2.4.5	Risk Management	24
2.4.6	Employee Awareness.....	26
2.4.7	Reward and Sanction	27
2.4.8	Regular Training.....	28
2.5	Human Factors	29
2.5.1	Behavioural Factors	32
2.5.2	Belief Factor	33
2.5.3	Attitude Factor	34
2.5.4	Intention Factor	37
2.6	Training Factors	38
2.6.1	Communication	39
2.6.2	Learning Motivation	41
2.6.3	Self-efficacy.....	42
2.6.4	Satisfaction.....	43

2.6.5	Reinforcement	43
2.7	Summary	44
Chapter 3: Research Design and Methodology		46
3.1	Research Methodology	46
3.1.1	Qualitative Research Methods	46
3.1.2	Quantitative Research Methods	47
3.1.3	Triangulation Method.....	49
3.2	Research Design	51
3.2.1	Interview	52
3.2.2	Questionnaire.....	54
3.3	Reliability and Validity	55
3.4	Summary	57
Chapter 4: Qualitative Data Analysis		58
4.1	Introduction	58
4.2	Selecting Participants	59
4.3	Interview Structure and Format.....	59
4.4	Employee Views on Organisational Information Security Management	62
4.4.1	Information Security Policy	63
4.4.2	Awareness	64
4.4.3	Role and Responsibility	67

4.4.4	Communication and Dissemination	71
4.4.5	Rewards and Sanctions	74
4.4.6	Risk Management	76
4.4.7	Summary of Employee Views on Organisational Factors Affecting Security.....	79
4.5	Employee Views on Behavioural Factors Affecting Information Security	80
4.5.1	Beliefs:	81
4.5.2	Influence of Others:.....	85
4.5.3	Behavioural Intention:.....	87
4.5.4	Changing Behaviours:.....	91
4.5.4	Summary of Employee Views on Behavioural Factors.....	93
4.6	Training and Awareness Programmes to Impact on Information Security Management Behaviours.....	95
4.6.1	How effective do the employees think the current information security training is?	96
4.6.2	Have those that received training changed their attitudes and behaviours after receiving the training?	99
4.6.3	If you help to devise or deliver training, how successful do you think it has been, and how do you think it can be improved?.....	102
4.7	Summary of the Criteria to Address When Devising Training	105
4.7.1	Motivation.....	106

4.7.2	Awareness	107
4.7.3	Communication	107
4.7.4	Reinforcement.....	108
4.7.5	Training Methods.....	109
4.8	Conclusion	111
Chapter 5: Quantitative Data Analysis		112
5.1	Introduction	112
5.2	Quantitative Research Methods.....	113
5.2.1	Questionnaire Design.....	113
5.2.2	Pilot Test	114
5.3	Participating Organisations	115
5.3.1	Organisation (A)	115
5.3.2	Organisation (B)	116
5.3.3	Organisation (C).....	117
5.4	Questionnaire Analysis	118
5.4.1	Statistical Techniques	118
5.4.2	Data Analysis	119
5.4.3	Habits of Employees	122
5.5	Barrier and Effective Factors	126
5.5.1	The Health Sector	126
5.5.2	Business and Education Sector.....	128

5.5.3	Statistical Analysis.....	130
5.5.4	Training and Awareness Programme Factors	132
5.5.5	Correlation Analysis	133
5.6	Conclusion	135
Chapter 6: Information Security Awareness – The Training Programme ...		137
6.1	Introduction	137
6.2	Training Effectiveness.....	138
6.3	Training Objective	139
6.4	Training Strategy and Plan	140
6.5	Implementation of Effective Training Factors.....	141
6.5.1	Communication Mechanism	141
6.5.2	Motivation Mechanism.....	142
6.5.3	Feedback Mechanism	143
6.5.4	Reinforcement Mechanism.....	144
6.5.5	Awareness Mechanism	145
6.6	Designing an Awareness and Training Programme.....	146
6.6.1	Contents of the Security Policy	147
6.6.2	Physical Security	147
6.6.3	Desktop Security	148
6.6.4	Password Security.....	148
6.6.5	Phishing	149

6.6.6	Hoaxes	150
6.6.7	Malware.....	150
6.6.8	Viruses	151
6.6.9	Spyware and Adware	151
6.6.10	Firewall.....	152
6.6.11	Backup and Restore Data	152
6.6.12	Encryption	153
6.6.13	Software Copyright.....	153
6.6.14	Risk Assessments	154
6.6.15	Disciplinary Procedures.....	154
6.7	Observation	154
6.8	Assessment	155
6.8.1	Pre-Assessment.....	159
6.8.2	Knowledge Reinforcement	160
6.8.3	Post-Assessment: Knowledge.....	162
6.8.4	Post-Assessment: Attitude	163
6.8.5	Evaluation Assessment	164
6.9	Conclusion	164
Chapter 7: Discussion of Key Findings		166
7.1	Introduction	166

7.2	The Main Obstacles of Complying with the Information Security Policy.....	168
7.2.1	Security Policy.....	169
7.2.2	Work Pressure.....	169
7.2.3	Someone Else’s Problem.....	170
7.2.4	Lack of Communication.....	170
7.2.5	Lack of Disciplinary Procedure.....	171
7.2.6	Lack of Awareness.....	171
7.2.7	Lack of Effective Training.....	172
7.2.8	Lack of Roles and Responsibilities.....	172
7.2.9	Individual Beliefs and Attitudes.....	172
7.2.10	Employee Habits.....	173
7.2.11	Trust.....	173
7.2.12	Lack of Top Management Support.....	173
7.2.13	The Main Problems Summarised.....	174
7.3	Critical Factors in Complying with the Organisation’s Information Security Policy and Improvement of Information Security Management	176
7.3.1	Awareness.....	177
7.3.2	Communication.....	178
7.3.3	Employee Involvement.....	179
7.3.4	Reward.....	179

7.3.5	Beliefs and Attitudes.....	180
7.3.6	Habits.....	181
7.3.7	Intention	181
7.3.8	Motivation.....	182
7.3.9	Reinforcement.....	183
7.3.10	Satisfaction.....	183
7.3.11	Assessment.....	184
7.3.12	Training	184
7.4	Summary	186
Chapter 8: Conclusions and Future Research		189
8.1	Introduction	189
8.2	Theoretical Contributions	189
8.3	Practical Contributions.....	191
8.4	Limitations of the Study.....	193
8.5	Future Research	194
8.6	Conclusions	195
References.....		1
Appendix A: Interview Information		1
A-A1:	Letter	1
A-A2:	Interview Questions.....	2
Appendix B: Questionnaire		1

Appendix C: Training Information.....	1
A-C1: Letter for the Company for Training	1
A-C2: Training Programme.....	1
A-C3: Final Assessment.....	0

Table of Figures

Figure 1-1: Research Approach	11
Figure 2-1: Information Security Elements	18
Figure 2-2: The Various Factors Affecting InfoSec	45
Figure 4-1: Organisational Obstacles Affecting InfoSec.....	80
Figure 4-2: Behavioural Obstacles Affecting InfoSec.....	95
Figure 4-3: Training Obstacles Affecting InfoSec.....	110
Figure 5-1: Response by Industry	120
Figure 5-2: Response by Gender.....	120
Figure 5-3: Response by Level of Education	121
Figure 5-4: Response by Age	122
Figure 5-5: Receiving Training.....	122
Figure 5-6: Sharing My Password at Work	124
Figure 5-7: Routinely Follow ISP at Work	125
Figure 5-8: Routinely Follow Risk Management.....	126
Figure 6-1: The Security Awareness and Training Programme	146
Figure 6-2: Pre-Assessment: Knowledge.....	159
Figure 6-3: Pre-Assessment: Attitude	160
Figure 6-4: Post-Assessment: Knowledge	162
Figure 6-5: Post-Assessment: Attitude.....	163
Figure 7-1: Critical Factors of Compliance to InfoSec Policy	187

List of Tables

Table 3-1: The Strengths and Weaknesses of the Quantitative and Qualitative Methods	49
Table 5-1: Organisational Factors on the Health Sector	127
Table 5-2: Organisational Factors on the Business and Education Sectors	128
Table 5-3: Organisational Factors for Encouraging Employees to Comply with Information Security.....	131
Table 5-4: Training and Awareness Programme Factors.....	133
Table 5-5: Correlation Analysis	134
Table 6-1: Observation Scenario	155
Table 6-2: Knowledge, Attitude and Training Evaluation	157

Chapter 1: Introduction

This chapter will provide an introduction to the research scope of this thesis, in doing so it will provide a clear outline of the content of each chapter. The first section will outline how information security has emerged and how it is continually developing. Secondly, a problem statement will be presented which will then lead into a presentation of the research questions, in the third section. Finally, in three further sections, the research aims, objectives and an outline of this thesis project will be presented.

1.1 Background

The world of information technology is constantly developing; to illustrate, the Department for Business Innovation and Skills (BIS, 2012) produced results from a survey to show that security breaches cost, in the UK alone, billions of pounds every single year. Lawrence and Richardson (2004) argue that the problem of security breaches is overwhelming because they have now reached critical levels. Furthermore, the research indicates that security needs to be tightened in order to counteract the increasing number of security breaches affecting organisations (Workman et al., 2008). Consequently a lot of problems and difficulties are facing the organisations that are failing to adequately manage their information security breaches. As a result, an organisation's integrity could be compromised as they may lose money and trust which could affect their competitive position as consumers will lose confidence and trust in the organisation (Blakley et al., 2002). Information security has therefore become one of the most important issues

within all successful organisations; thus, the organisation needs to ensure that their information is properly protected in order to maintain the highest level of information security.

According to Herath and Rao (2009a), Kankanhalli and Xu (2009) and Kim and Ryu (2009), the most obvious response of an organisation, to the increasing security breaches, is to utilise effectively their own corporate IT in order to implement many technological fixes and defences, such as: firewall, antivirus and filtering software. Although such technical tools may play an essential role in improving information security, particularly with respect to protecting an organisation from external risk, they are less well suited to detecting naïve negligent or destructive employee behaviour (Ng et al., 2009). It is important to understand that technology is a tool that can be used or misused by people and no matter how strong the security system is, or how powerful the policy is, there will always be a potential threat to information security as a result of user or employee misbehaviours.

In recent years, various efforts have been made to examine security problems, and numerous security issues have been addressed by existing studies which have aimed to identify the main reasons behind the different security breaches. Most of these studies focus on technical perspectives rather than on the actual process of security management. Indeed, Mader et al. (2005) state that security is, in the most general sense, more of a management issue than a technical one. Research confirms that information security has been regularly measured as a technological problem with a technological solution (Ruighaver et al., 2007). It should be noted that this

approach is possible if the environment is static, but this is rarely the case in real-life environments.

As Lampson (2002) and Sasse and Flechais (2005) highlight, security is not just a technological problem it is a people problem because the people are the ones implementing and managing information security. Therefore, the employees' behaviours and attitudes toward the organisation's assets can potentially harm the organisation's success as they can directly influence information security failures.

Finally, the literature indicates that the information security issues identified need to be resolved from a different perspective. It is therefore essential that this problem is improved through the implementation of other approaches, such as the socio-technical approach. Interestingly, this approach focuses on the involvement of both human and organisational management aspects in order to achieve improvements within information security management.

1.2 Problem Statement

Security breaches have attracted considerable corporate attention and organisations are increasingly determined to stop these security breaches. Information security concerns people and is actually more of a managerial problem than a technical issue; therefore, it cannot be dealt with in a purely technical way. The literature investigation highlights the importance of information security that has been implemented since the 1990s; however, organisations are still facing problems with the implementation and

compliance of information security. The literature review shows that policies are often in place, but employees are not complying with these policies; this raises the important question of why this is so.

In addition, it can be argued that the reason for security breaches is that most organisational information security is far too techno-centric (Dhillon and Torkzadeh, 2006), and the policies employed often ignore socio-organisational issues (Dhillon and Backhouse, 2000). No matter how strong an organisation's technical defences are, its information security eventually depends on user behaviours (Rhee et al., 2009: p. 2). As shown in the literature review, there is growing evidence that security problems occur as a result of errors, mistakes or simply by misuse by the organisation's own employees (Stanton and Jolton, 2005).

The literature also suggests that there is little proof that awareness programmes reduce employee breaches; furthermore they do not appear to influence compliance to organisational information security policy. It is important to understand that what makes training effective is not only the way that the participant feels after the training and, nor should it be simply based on how a training programme is evaluated. It should therefore be based on how sustainable the appropriate behaviour is after the training has occurred and how the new knowledge is actually transferred into the work environment. As Laoledchai (2008) states, if a user fails to transfer the skills and knowledge gained from the training programme into actual practice, then the training has failed as it has added no value to the organisation.

Therefore, this research aims to study the critical factors (CFs) of information security management, in order to overcome some of the gaps in the literature with regards to socio-organisational issues that provide guidelines to help organisations to formulate effective information security management policies. Information security should aim to ensure the continuity of employee compliance, in order to reduce security breaches, which will ultimately improve information security management within the designated organisation.

The study will focus on exploring the obstacles and the success factors influencing information security policy. Throughout the research, the employee attitudes to compliance with the organisational policies will be considered by reviewing the aspects which caused concern to employees about information security. In addition, in order to fulfil the gaps in the existing literature regarding the importance of the success factors and the implementation of it, various techniques and factors will be identified which could potentially be incorporated into new awareness programmes which could help to establish a successful link between training, learning and behaviour.

1.3 Research Questions

What are the external and internal factors impacting employee compliance with organisational information security policies?

To address this research question, three further areas need to be addressed, as follows:

1. What organisational factors impact employee compliance with organisational information security policies?
2. What human behavioural factors impact employee compliance with organisational information security policies?
3. Can training alter employee attitudes toward organisational information security policies?

This study will focus on these three stages, each additional stage will be developed in light of the results from the previous stage.

1.4 Research Aims

This research aims to study the critical factors (CFs) that impact on an employees' behaviour towards complying with organisational information security policies. The study aims to explore the reasons behind employee non-compliance with organisational security policies in order to identify the factors affecting the successful implementation of information security policies.

The investigation of these critical success factors will be grouped into three major categories, namely: organisational factors, behavioural factors and training factors; each of these categories affect a different aspect of information security. The objective of this research is to not only understand the interaction of different factors, but to further study the aims which provide practical recommendations for improving information security management for organisations.

The study will also evaluate the impact of socio-technical factors on organisational information security management. The final stage will focus on developing an effective training and awareness programme. The training programme will be constructed by incorporating various techniques that enhance employee perception, attitudes and motivations as well as the transfer of skills and appropriate sustainable behaviours in order to improve organisational information security management.

1.5 Research Objectives

This research thesis aims to fulfil the following objectives:

- To conduct an in-depth study to investigate organisational factors that impact employee compliance with organisational information security policies.
- To conduct an in-depth study to investigate human behavioural factors that impact employee compliance with organisational information security policies.

- To identify effective training techniques that will improve employee awareness by changing their attitudes and habits in order to enhance their motivation to transfer knowledge and sustain information security management practices in their work environments.
- To investigate the impact of implementing effective training and awareness programmes for information security management.

1.6 Research Structure

Mixed methodologies of qualitative and quantitative approaches are used in this study. Semi-structured interview will be conducted and analysed, to explore the factors and the elements that improve the implementation of the organisational information security policies.

A further investigation will be needed to confirm the identification of critically effective factors which could help employees to maintain the implementation of organisational information security policies. Quantitative technique will therefore be applied to analyse the results further.

Because the aim of the study is to improve the compliance of the organisational information security policy and evaluate the impact of the effective factors, a further experiment will be needed. Therefore, the findings from the literature review will be combined with the qualitative and quantitative data in order to reach the aim of the study. An experiment that will identify the most effective training and awareness programme in order to improve employee awareness of information security management, change

employee attitudes, habits and motivations through knowledge of information security management, ultimately leading to sustained change in behaviour where organisational information security policies by employees are implemented in the short and longer term.

1.6.1 Thesis Outline

The remaining chapters of this thesis will be organised as follows:

Chapter 2: Literature Review

This chapter will review and explore issues related to information security, management from the perspective of (i) the organisational information security policies, (ii) factors that impact employee behaviour related to information security policy compliance and, (iii) effective training that impact employee behaviour regarding information security management and compliance with information security policies.

Chapter 3: Research Design and Methodology

The third chapter will present and discuss the research methodologies used for this thesis.

Chapter 4: Qualitative Data Analysis

This chapter will analyse and discuss the results from the qualitative investigation into the critical factors that impact on employee compliance with organisational information security policies.

Chapter 5: Quantitative Data Analysis

The fifth chapter will present the findings from the quantitative stage of the research project and discuss the findings and also links with the qualitative stage of the project.

Chapter 6: Developing an Effective Information Security Awareness and Training Programme

This chapter will explore and identify effective training techniques in the context of information security management and policy compliance. This chapter will also present suggested criteria and techniques that should be used to develop an effective information security awareness and training programme to improve employee awareness, change employee attitudes and habits enhance their motivation and influence their behaviour for information security management. .

Chapter 7: Discussion of the Key Findings

The seventh chapter will consolidate and summarise the findings from the three stages of the research study and will critically review these findings, discussing the implications and the contributions this study makes to the field of information security management.

Chapter 8: Conclusions and Future Work

The final chapter will present the theoretical and the practical contributions identified as a result of the study. It will also discuss any limitations identified

in the project, as well as presenting the final research conclusions and suggestions for future work.

1.7 Research Approach

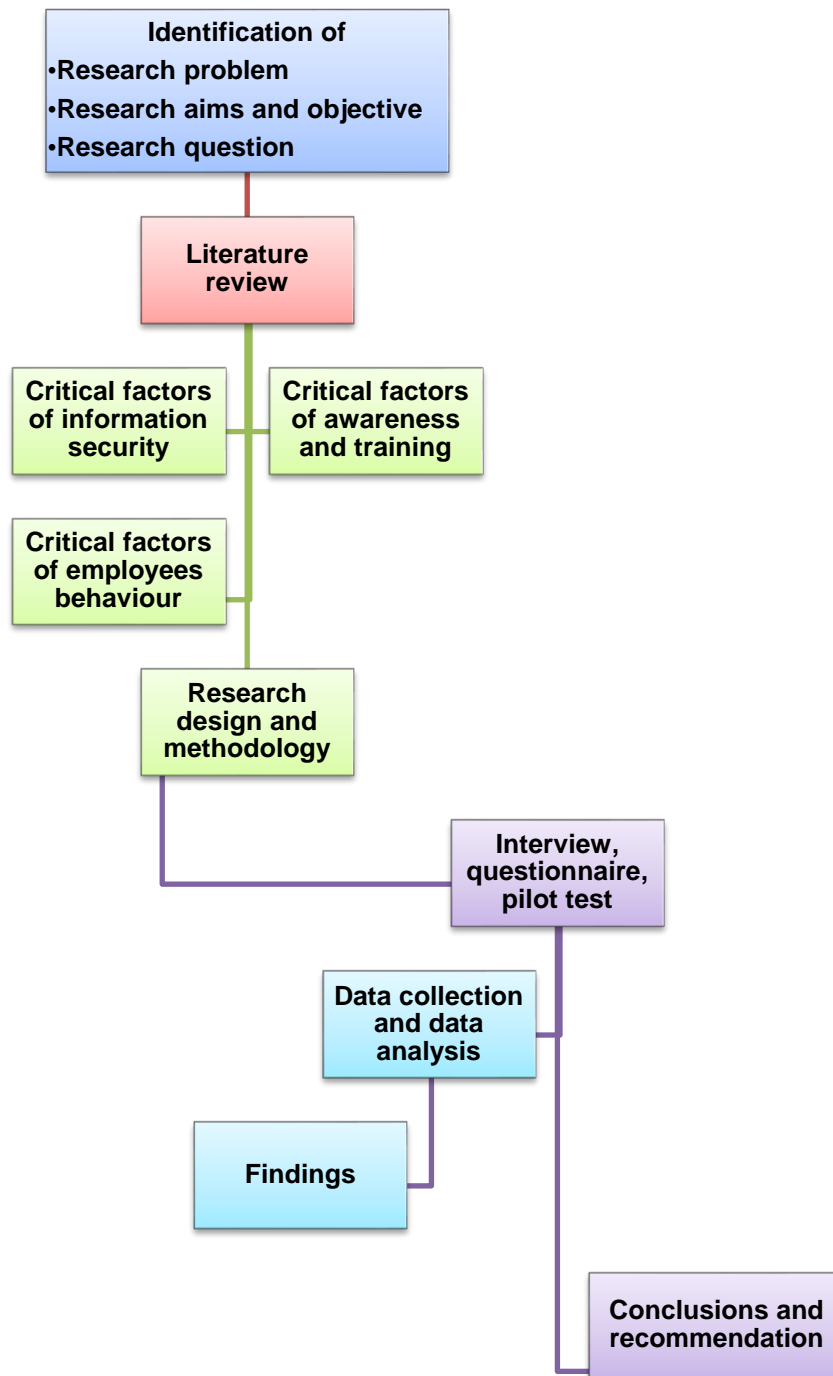


Figure 1-1: Research Approach

Chapter 2: Literature Review

2.1 Introduction

This chapter will present a review of the literature of security management which identifies critical factors affecting information security policies in organisations, in particular three separated mechanisms: organisational policy factors, behavioural factors and training factors. The remainder of this chapter will discuss information security management; describe the lack of organisational factors in terms of the implementation of organisational information security policies. Integrate the theory of reasoned action in order to identify the human factors that impact employee behaviours which will help to determine how to accommodate these factors when implementing organisational information security policies. Explore the most effective techniques that should be employed within a training and awareness programme in order to improve the sustainability of information security management practices. Finally, the eighth section will provide a summary of this second chapter.

2.2 Information Security Management

The concept of information security management refers to the activities which control the security of the information assets of an organisation. Many researchers agree and recognise the importance of considering and involving the socio-organisational perspective (Hitchings, 1996; Dhillon, 2001; Karyad et al., 2003). It is critical that all organisations take active steps to maintain the security and integrity of their information resources.

Therefore, it is important to understand the individual values and beliefs in order to integrate the socio-organisational aspect which will increase the success of information security management. According to Dhillon and Backhouse (2001), there has been little investigation into the factors that affect employee behaviours and attitudes toward the implementation of organisational information security. Thus, there are no studies or models that test whether the beliefs of an individual influence their behaviours towards information security in an organisation (Hinson, 2003). Despite the fact that issue of employees' failure to comply with information security policy is remaining a key concern for organisations today. Recent study by Vance et al., (2012), prior studies have not examined the influence of behaviour on employee decisions to comply with the organisational information security policy.

As previously mentioned security is a people problem because it is the people who implement and manage the information security policies (Lampson, 2002; Sasse and Flechais, 2005). The technology within a company can be used or misused, irrespective of how strong the security systems and policies are, as a result of the behaviour of the employees. Consequently, a significant improvement in the management of information security requires investigation in terms of the organisational and behavioural factors affecting it (Bruque and Moyano, 2007).

2.3 Organisational Factors

The research suggests that organisational factors can lead to improvements in security management (Swanson and Wang, 2005; Traafdar and Vaidya, 2006). The literature review shows that there are numerous studies which discuss the implementation of different factors; furthermore, various factors have been explored as possibly influencing the level of success of information security management. To illustrate, AbuZineh (2006) explored various information security management factors by conducting a comparative analysis between companies to evaluate the factors that are deemed as influencing success (to the competitors), they included: top management support, commitment to job responsibilities, motivation of employees and awareness. Their study identified the above factors as being the most relevant to the improvement of security management.

Furthermore, Fulford and Doherty (2003), in their research, summarised a number of key factors that led to effective information security management, including: the commitment and support from information security management; conducting assessment of potential security risks and threats; the communication of security issues as well as the transfer of awareness and knowledge. Their study concluded that the above factors need to be improved and implemented in order to allow for better security management. Similarly, Mak (2001) proposed a model of information management that identified six critical success factors that are needed for successful implementation of information security, including: planning, involvement, leadership, awareness, risk assessment and teamwork.

Moreover, Tucker and Mohamed (1996) proposed a four factors approach which affects the success of information security implementation. Firstly, the purpose needs to be defined in advance by the senior management to the employee. Secondly, the people need to be considered as their lack of enthusiasm and unwillingness to change could affect their existing work responsibilities; therefore, successful implementation needs support and involvement from the people. Thirdly, a strategic plan should be in place as this allows for involvement from both the employees and the developers responsible for it. Finally, progress needs to be measured throughout the implementation and at regular reviews in order to identify and resolve any problems.

A recent study, conducted by Ebrahimi and Naini (2012), indicates the complexity of the organisational factors further. They analysed the results from a survey conducted by CSO Magazine, this survey investigated 7,596 information security senior managers from 54 different countries. These managers claimed that security breaches were not related to technology, they noted that the events were few, but when they did occur the main problems were usually non-technical in nature.

It should be noted that despite significant advancements and developments in the implementation of technical solutions, organisations are still facing security breaches. The literature proves that the problem has not been resolved over the years, In addition, the majority of researchers indicate that humans are the main reason for security breaches across organisations. As Liisa et al. (2009) and Herath and Rao (2009) note, the majority of security

problems are indirectly caused by employees who violate or neglect the information security policies within their organisations. Therefore, the exploration and investigation of information security policy is essential to the improvement of information security management.

2.4 Information Security Policy

Information security policy, according to Rossouw et al. (2004) is defined as a plan or a set of guidelines that are intended to influence and determine decisions, actions and other matters which may follow. It is therefore a plan which identifies the organisation's policy by explaining what acceptable and reasonable behaviours are expected from the employee in order to effectively ensure information security (Hone and Eloff, 2002). The development of an information security policy is the first step toward preparing an organisation for attacks from internal and external sources. If employees are unwilling or indifferent in following the security policies, then the efforts will most likely be ineffective.

As such, Kenneth et al. (2009) suggest that there are a number of very important policy management decisions to consider when creating policies and procedures, such as: developing the policies and procedures, reviewing them, developing risk assessments, gaining approval for them and then communicating them effectively to the employees. Failure to establish, disseminate or educate the members of an organisation could devalue the importance of the policies and the procedures which could expose security vulnerabilities (Mader and Srinivasan, 2005). It should be noted that people

with higher levels of responsibility and accountability generally help to develop the policies, whereas it is usually people with limited responsibility that actually help to enforce the policies.

Mader and Srinivasan (2005) therefore declare that the policies and procedure are the backbone of what is and what is not acceptable; furthermore, penalties should be associated with misuse in order for the policies to be more effective. Security policies should protect people, their information and the system; by identifying the rules for expected behaviour and the consequences of breaking the rules, these policies are more enforceable as risk can be monitored and minimised and a framework for best practice can be developed and followed. Moreover, these policies and procedures actually define the organisation's attitude towards information, based on their approach to protecting it from unauthorised access, modification, disclosure and destruction.

Finally, these systems act to preserve an appropriate level of confidentiality, integrity and availability (see Figure 2-1). Confidentiality focuses on the processes of preventing the unauthorised disclosure of information, integrity focuses on the processes of preventing the unauthorised amendment or deletion of information, and availability focuses on the processes of preventing the unauthorised withholding of information or resources (Gollmann, 1999; Pfleeger and Pfleeger, 2003). In addition, Hare (2007) acknowledges that organisations need a security policy based on their need to set standards and controls.

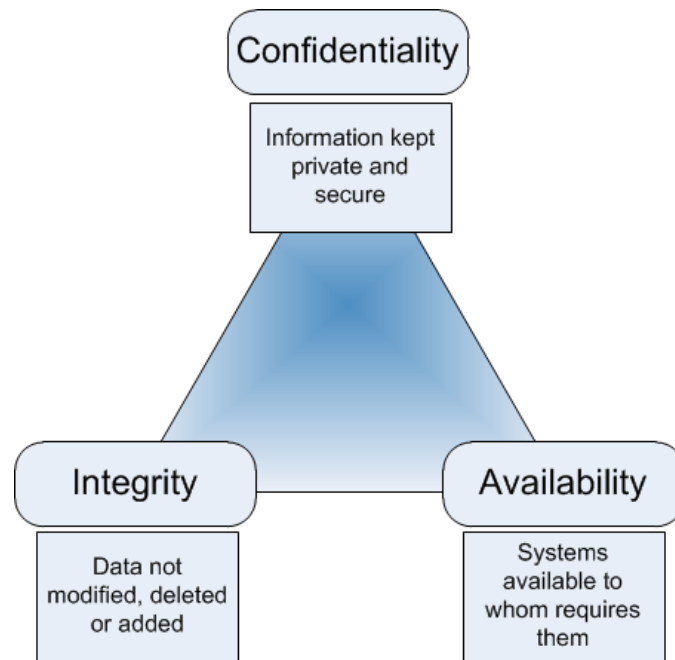


Figure 2-1: Information Security Elements

(Source: Lachapelle and St-Germain, 2005)

2.4.1 Policy Procedure

Mader and Srinivasan (2005) state the difference between security policy and procedure, security policy is the rule that identifies what must be done in order to maintain security in the system, and the procedure is the process that is to be followed in order to enforce the identified rule. The policies and procedures should contain as much detail as possible, to avoid any misinterpretation by the user. According to Wheelen and Hunger (2000), procedure involves the transforming of strategies and policies into actions; thus, the implementation can be defined as putting the plans into action.

Many researchers indicate that there is a lack of implementing the policy's procedure across an organisation (Known and Zmud, 1987; Lederer and Sethi, 1988; Lederer and Mendelow, 1993; Gottchalk, 1999). The research

shows that the majority of security problems are caused by the employees who neglect the information security policies within their organisation (Liisa et al., 2009; Herath and Rao, 2009). Furthermore, one investigation into the causes of recent security incidents shows that employee negligence has led to security breaches that have cost organisations millions of dollars in losses.

The following points identify the various issues that impact on the compliance of organisational policy's procedure. The feedback of policies and procedures from users is essential in order to improve the effectiveness of it. Scott et al. (2009) state that when individuals are not motivated to follow the procedures and protect the information, then security fails. Conversely, others believe that policies must be enforced to make them effective as without enforcement a policy might as well not exist (Kenneth et al., 2009).

It is also vitally important that all employees be provided with the proper education and training to ensure that they can follow the policies and the procedures that a given company provides. Mader et al. (2005) notes that many studies have shown that understanding the policy and the procedure will allow all members of staff to be informed of what is expected of them as well as the penalties that they will face if they do not comply.

Furthermore, Russell et al. (2002) states that the most basic security tool an organisation has, is the implementation of a successful security policy. Research by Doherty and Fulford (2005) suggests that there are sometimes reasons for people failing to follow security policies, such as: a lack of awareness; a lack of documentation; difficulties of enforcement; the policy

being too complex; a lack of skills; as well as, a lack of proper resources for monitoring the policy. In contrast, Taylor (1997) suggests that many strategies are not implemented because much, if not all, of the documentation is so large that it is simply locked away in cabinets.

2.4.2 Role and Responsibility

An understanding of roles and responsibilities is important and needs to be one of the main priorities for all employees, from the senior manager to each employee and information system user within the organisation. All members need to know how to perform their tasks successfully in order to understand what is required of them, individually. Employees are expected to develop their own work practices on the basis of a clear understanding of their own responsibilities. Gurpreet and James (2000) mention that responsibilities, integrity, trust and ethics are considered to be the major issues within an organisation that form the first steps in securing information.

The literature shows that the lack of understanding and applying the role and responsibilities from within an organisation's policy is an old issue, but this problem has not been resolved over the decades. In addition, organisations cannot protect the three aspects of integrity, confidentiality and availability of information without ensuring that each employee is truly involved in clearly understanding their roles and responsibility, as such they need to be adequately trained to perform them (Wilson et al., 1998). It is essential to understand that security should be the responsibility of all employees,

irrespective of the policies or technological instruments that are in place as security cannot be successful without the full cooperation of all employees.

According to Gurpreet and James (2000) some organisations have not developed separate functions or roles with responsibilities. Many organisations lack specific roles and there is no utilitarian system of reporting in existence; as such, there is often a lack of integration of the role and responsibilities with the policies and procedures. Many researchers have concluded that compliance with organisational policy can be a difficult and complex task for employees (Earl, 1993; Lucas et al., 1990; Barne, 1997).

The main reason that the employees are failing to fully implement their roles and responsibilities is because the employees are not always aware when a security issue or incident has occurred, at this time they look to the proposed administrator to source solutions. Similarly, Soliman's (2009) research proves that the main constraint regarding information security is in the employees' lack of motivation and knowledge of information security.

2.4.3 Communication and Documentation

One of the major barriers affecting an employee's ability to comply with the organisational policy is as a result of too little communication (Lederer and Mendelow, 1989; Frederick, 1996; Smith, 1999). Communication is such a vitally important element as it ensures that all employees are aware of all the issues affecting an organisation. In addition, it is important that there is documentation of the policy as this should explain the processes and the

attributes, as well as the actual policies, procedures and processes. Neil and Heather (2006) state that in order for policy documentation to be effective, it must indicate the steps that need to be taken to recover from breaches while also adequately recording the security incidents to ensure that steps are taken to prevent them from occurring again.

Sumner (1999) states that all employees must know, in advance, the organisation's goals, objectives and the tasks that need to be completed from a good communication strategy. Farahmand et al. (2003) argue that the organisations that fail to adequately document security incidents generally struggle to make decisions about security which often result in financial losses. Moreover, when support, feedback and assistance is provided to employees for the resolution of security problems, performance is increased and these employees are more likely to be prepared to make decision and engage to change activities and procedures in the future. In addition, many researchers identify the significance of communication, between management and the employee, to the successful implementation of the policy (Lederer and Sethi, 1992; Earl, 1993; Premkumar and King, 1994; Gottchalk, 1999). Furthermore, in order to ensure successful, long-term, change, Kritsonis (2005) states that the provision of advice and feedback from management is essential.

Clearly, documentation and communication are very important information security management methods that allow for the review and exploration of what has occurred previously as they help to provide a clear idea of what needs to be done in the future as well as how results might be achieved.

Sumner (1999) considers the lack of communication to be one of the major barriers affecting organisations. Based on the above literature, the implementation of a comprehensive communication and documentation process within an organisation is an essential factor that can lead to the improvement of information security management.

2.4.4 Employee Involvement

Various researchers identify a lack of employee involvement, when reviewing the organisational security policy, as being one of the main reasons that employees fail to comply with it (Robey et al., 1990; Mak, 2001). In addition, if employees agree with the information and deployment of a security policy, they are more likely to implement it. Kim and Lee's (2007) research takes this notion a step further by indicating that employee involvement actually enhances their satisfaction and the employee will either follow the policy or reject it based on how much input and involvement they had during the planning stages of the policy. To further support this notion, Lucas (1975) concluded that the main reason that many organisations have fail to deliver the expected benefits from their policies is because more concentration was placed on the technology rather than on the employee's involvement. Kim and Lee (2007) took this further by proposing that when employee involvement is not viewed as part of the overall transformation, the result is unlikely to accomplish the expected level of security. Herath and Rao (2009) argue that the main problem regarding employee roles in information security is in their lack of motivation and involvement in the information security policy.

The literature therefore indicates that employee involvement should be utilised as a powerful means of self-realisation which, if used positively, could significantly influence performance to achieve better information security management.

2.4.5 Risk Management

Another important organisational factor affecting the improvement of information security management is risk management. By applying risk management it is possible to reduce the organisational risk. Reducing risk can be achieved via the following means: avoiding risk, transferring risk, decreasing the possibility of threats/risk and by discovering and identifying unwanted events early (Van Wyk et al., 2008). The main objectives of risk management focus on the provision of the understanding of the likelihood of different vulnerabilities, threats, losses or impact and the theoretical effectiveness of security measures.

Ge et al. (2006) and Straub and Welke (1998) argue that risk assessment provides a report that describes the threats and vulnerabilities by measuring the risks and by providing recommendations for the control of implemented changes. Robert and Rolf (2003) argue that the reasons sometimes given for failing to undertake a risk assessment is as a result of the cost, time, energy or money involved.

It should be noted that risk management allows employees to respond quickly and effectively to threats, as they arise. Incident response is likely to

be quicker as these employees/organisations have the ability to take action appropriately and completely as quickly as possible to resolve any incidents, situational compromises or threats from any source, at any time, in order to recover from an incident.

Incident response is a practical way to resolving the accrument of risk. The incident response plan should identify who is responsible for conducting the duty to end the risk and to bring back order to the system. Hawkey et al. (2008) suggest that the organisation should determine the security incident response by identifying which tasks, strategies, skills and tools should be used during a response. Neil and Heather (2006) take this notion further by stating that it is essential that organisations have a contingency plan in place, which specifies how to bridge the gaps and how to cope with and recover from a significant security breach, such as a natural disaster or a serious virus.

The literature clearly shows that risk management is one of the most important factors to improve information security management. Therefore, the organisation must carry out a comprehensive risk analysis, this should include an incident response methodology of who will tackle the problem, how it will be tackled and the recovery of it. It is very important to understand that the concept of information security is not only about the creation of the total protection of information, but, that information security is also about risk management.

2.4.6 Employee Awareness

Kenneth et al. (2009) states that knowledge and employee awareness are key to enabling the employee to make decisions that are consistent with the organisation's objectives. A lack of information security awareness can make an organisation vulnerable to internal and external threats. To illustrate, Glisson et al. (2006) conducted empirical research that was based on an in-depth security survey that was conducted within the financial service sector of Fortune 500 organisations. The survey indicated that threats are becoming more sophisticated, but the main reason for the threat is as a result of a severe lack of employee awareness.

Recent research by David et al., (2011) agreed that poor computing security practices in organisations can have significant direct and indirect consequences. Many organisations conduct and provide training and awareness programmes to their employees, however, Jaspersen et al., (2005) identified that most of these training programmes are wasted as the employees do not transfer the learned skills into sustainable and appropriate behaviours in the work environment.

Furthermore, Knapp et al. (2009) argue that one of the basic steps to cope with information security risks is to establish a training awareness programme that is clear and specific. The ultimate goal should be to raise employee capabilities, so that the employee can realise their own capacity to improve performances. The security training should not only include raising awareness of the different types of technical attacks, but it should also

include information about current environmental and everyday life experiences.

In addition, during the last decade, awareness has become recognised as one of the most important organisational factors to improving information security management. However, as the above literature suggests, the lack of employee awareness is still a critical issue facing the majority of organisations today.

2.4.7 Reward and Sanction

According to Solms (2004) there is no point in an organisation having information security policies unless they plan to implement some enforcement techniques. Rewards can be utilised to increase employee interest, performance and motivation to comply with organisational security. As Cameron and Pierce (2002) and Stanton et al. (2005) note, reward and motivation can improve organisational management. A study by Gonzales et al. (2002) found that employees consider reward to be the best motivator for compliance with organisational policies; however, if/when the reward is removed the employees may stop complying with the policy. An example of reward could be in the form of bonuses, salary increases, praise and recognition in the form of titles, certificates, new responsibilities, extended breaks, more flexible working hours or simply a show of appreciation. Others believe that the reinforcement of sanctions will decrease the probability of organisational risk occurring (Puhakainen, 2006). There are numerous

examples of possible sanctions, which include: a reduced salary, criticism, increased monitoring, stricter control or a reduction to flexible working hours.

Ultimately, the literature confirms that a reward and sanction procedure can be used as an organisational factor to improve information security management and to help employees to comply with organisational information security policies.

2.4.8 Regular Training

Inadequate training is considered a major barrier facing an employee's ability to implement organisational security policies (Tucker and Mohamed, 1996; Lederer and Singh, 1997; Mak, 2001). Islam and Dong (2008) argue that one of the major reasons that people who are involved in developing, managing and using the software make mistakes is due to a lack of an organisational security policy and knowledge that these mistakes will have a significant effect if they are not handled appropriately. According to Dourish and Bellotti (1992) and Gon and Sangjae (2007), training should be considered an important factor that can improve information security management within an organisation. Furthermore, the introduction of an organisational awareness programme is often the initial phase of teaching and educating about the various organisational factors (Gon and Sangjae, 2007).

Knapp et al., (2009) argue that one of the basic steps to coping with information security risks is in the establishment of a training awareness programme. Security training should not only include raising awareness of

the different types of technical attacks, but it should also include information about current environmental and everyday life experiences. Every employee needs to be aware of and trained in how to deal with all security subjects, including guidance on how to identify and resolve security incidents quickly and in an appropriate way. Interestingly, Norris (1999) stated that public organisations reported that their employees were not trained regularly and that this lack of training resulted in limited knowledge regarding the implementation of information security policies within an organisation.

Based on the literature presented above, in order to improve information security management, the organisational factors identified should be incorporated and considered as they are central to organisational success. The factors include: implementing an effective organisational policy that contains clear procedures, communication and documentation, the identification of roles and responsibilities, rewards and sanctions, awareness, envelopment, risk management and regular and appropriate training. These factors could greatly impact on and improve employee compliance with organisational information security policies.

2.5 Human Factors

The world of information technology is constantly developing, hence in order to reduce security breaches it is required to improve information security management. It is crucial for an organisation to understand the critical factors of information security management. Research proves that employees are significant risk due to their behaviour and their lack of knowledge regarding

security issues. As such, Siegel et al., (2006) state that there are higher risks from user errors and accidents than from maliciousness; for instance, accessing offensive or illegal material; downloading attachments from the web or software/applications from unknown sources; users writing down their passwords; and leaving laptops or other devices carelessly unattended in public places. According to Siegel et al. (2006), the results indicated that around 60% of users admit to saving some personal information on their work computer; one in ten confessed to downloading information and applications at work that they should not have; more than half of the respondents (51%) had no idea how to update the antivirus protection on their computer; and, five people stated that they had significant access to areas of their IT system that they should not have. Gehling and Stankard (2005) argue that most users have only vague ideas about the threats and risks relating to conducting their business over the internet. Liginlal et al., (2009) argue that privacy breaches have attracted corporate attention in recent times and that often the overlooked cause of these security breaches is human error, despite the fact that this is potentially the main underlying reason for many attacks on information systems. Russell (2002) and Voss (2001) reiterate this notion by highlighting that human error is often the root cause of most security breaches. Hinson (2003) takes this further by suggesting that the management of the human side of information security should be as carefully considered as the technical side. Human factors have been found to be responsible for between 80% and 90% of organisational incidents, this truly highlights that the behaviour of people plays the most significant role in security breaches (Reason and Hob, 2003).

Many researchers share the belief that information security, on the organisational level, is becoming much more of an employee matter (Hone and Eloff, 2002; Whitman et al., 2005) as they clearly state that employees are the cause of the majority of information security breaches (Kotulic and Clark, 2004; Payne, 2003). These errors not only threaten the integrity of the organisation, but there are also significant losses in terms of information and costs associated with fixing the problems and damage caused to the organisation and its reputation.

Further investigation into the critical issue of information security acted as the main motivator to the researcher of this project. As such, this project acknowledges that there are gaps in the existing literature with regard to the implementation of solutions for the management approach which needs to focus on and address firstly the organisational factors. This study will focus on the discussion of organisational factors to the context of the security policy and the role of people in it. The following sections will address the impact of the critical factors of human behaviour, so as, to evaluate the impact of these factors on the compliance to the organisational security policy and, in order, to identify areas for the improvement of information security management.

Despite the large amounts of effort by organisations to secure their assets, many incidents of data breaches and information loss continue to happen every year due to the reason that organisations typically concentrate on technical and procedural security measures. Although these solutions help improve information security, however, relying on them alone is not enough

to eliminate risk therefore, human, social and organisational factors must be considered critically (Omari et al., 2012).

2.5.1 Behavioural Factors

According to Alfawaz et al., (2010), more emphasis has been placed on technical solutions and little attention has been placed on human behaviour. Few studies have comprehensively modelled or evaluated factors that influence information security behaviour in organisations. Indeed, security breaches occur in various ways across an organisation. Arguably, the most common factor contributing to these security breaches is that of human behaviour, which suggests that changes in employee behaviour can significantly impact the improvement of security in an organisation.

The theory of reasoned action (TRA) was developed by Fishbein and Ajzen (1975); the theory proposes that person's behavior is determined by its behavioural intention to perform it. This intention is itself determined by the person's attitudes and his subjective norms towards the behaviour. Fishbein and Ajzen (1975, p. 302) define the subjective norms as "the person's perception that most people who are important to him think he should or should not perform the behaviour" (Fishbein and Ajzen 1975, p.302). Whereas, the attitude toward the behaviour is defined as the individual's positive or negative feelings about performing certain behaviours. The attitude of a person is determined by his beliefs on the consequences of the behaviour. In contrast, Beliefs are defined by the person's subjective probability that performing a particular behaviour will produce specific results.

In order to identify and investigate the external influences that face an employee to comply and implement the security policy, the existing theory of reasoned action will be used in this research as it helps to provide:

- An understanding of the influences that impact on employees to behave in certain ways
- An understanding of the reasons for employee behaviours
- An understanding of the obstacles that employees face which prevents them from improving their behaviours
- An understanding of the interaction between the factors that impact on employee behaviours
- A means to investigate others factors that might influence employee behaviours

2.5.2 Belief Factor

An understanding of the different factors that impact on an employees' implementation of the organisational security policy, in terms of sustaining appropriate behaviours, is critical if employees are to be allowed to contribute to the improvement of security compliance. Research by Aytes and Connolly (2004) indicates that the gap between knowledge and behaviour can effectively altering an employees' behaviour. Other studies have been conducted in this area, to illustrate, according to Posner et al., (1987), people behave in accordance with their attitudes and beliefs. There are many barriers that need to be identified and considered in order to change peoples' behaviour.

As Galvin et al. (2001) state, information alone is not enough to change behaviour. Therefore, it is essential to think more broadly about how employees actually contribute to the implementation of organisational security policy. By focusing on the outcomes and the results, it is possible to track how employees are applying the skills they have attained in order to achieve the desired goals. Dhillon et al. (2007) and Albrechtsen (2007) state that it is important to understand how people behave, as this knowledge assists in spreading an information security consciousness and awareness. It is also important to identify employee enthusiasm and preference so as to assess how well they are aligned with the strategy of changing behaviour principles. According to Deloitte (2007), it is believed that employees want to change and develop in order to stretch their capabilities; they want techniques and principles that engage their heads, as well as their hearts, and they want to connect with the people and things that will help them achieve their compliance goals.

Furthermore, Alfawaz et al., (2010) confirms that despite knowledge and skills being important, they alone will not assure a positive contribution and impact toward information security. Therefore, it is critical to recognise any other elements that impact on how an employee behaves and complies with the organisation's information security policies.

2.5.3 Attitude Factor

According to Ajzen (1980), attitudes are defined as the first determinant of behavioural intention. It is the degree to which the person has a favourable

or unfavourable evaluation of behaviour and it is an individual's positive or negative belief about performing behaviour. As such, an individual may intend to perform a behaviour when they perceive that other people, who are important to them, would approve or disapprove of their behaviour or performance.

Within the management of information security, the role of motivating employees should also be considered. Employees should be convinced and encouraged to achieve their organisational information security duties, successfully. The identification of an audience is considered to be one of the essential elements for achieving the desired result of changing behaviour. It is important to get to know them by assessing their skill levels and by identifying what they know and what they do not know. It is also important to respect the audience, interact with them and use simple language so as to recognise any barriers to making the change, such as cost, time, technological or skill constraints. Furthermore, the audience needs to be provided with clear feedback and follow-up techniques to ensure that they are motivated to maintain the new behaviours. Williams (2010) believes that the practising of new experiences creates new neural pathways that can change behaviour.

In contrast, Galvin et al., (2001) note that people tend to be persuaded more when messages are emotional rather than logical. For example, personal consideration and consequence messages are usually directly related to elements that people care about, in term of loss rather than gain. According to Yates and Aronson (1983), the provision of a small commitment can lead

to a bigger one and it can greatly influence new behaviours when goals and changes are clearly stated, documented, convenient to perform and when the person can choose whether to commit, as this empowers the person to make an initial change that they believe in. Damrosch (1991) believes that continued contact will help to maintain the new behaviour as it enhances motivation and helps people to practise the skills relating to maintaining the new behaviour.

It is important to motivate participants and support their self-efficacy by preparing them for change, building their confidence and recognition for the need to change. Moreover, the brainstorming of different solutions and work, as a team, can encourage the individual to view the problem from a different perspective. According to Kritsonis (2005), self-efficacy is considered to be an important characteristic that determines a person's behavioural change, because the expected outcomes are filtered through a person's expectations of being able to perform the behaviour. In order to improve self-efficacy in people, it is important to provide clear instructions, opportunities for skill development and training of the new behaviour.

This literature clearly shows the importance of essential elements that impact on improving employee behaviour toward the compliance with organisational information security policies. In addition, the understanding and consideration of these elements will help with the improvement of information security management.

2.5.4 Intention Factor

Ajzen (1980) defined behavioural intention based on the indication of how hard people are willing to try and based on how much effort they apply to achieve the behaviour. Behavioural intention is influenced by the person's attitudes, social pressures and perceived behavioural controls. Control includes both internal and external influences, internal influences include: skills, abilities, information, emotions and stress and external influences include: situation or environmental factors.

It is widely agreed that one of the main threats to information security is as a result of careless employees who do not follow the information security policies within their organisations. An internal security threat does not only cover employee errors, it also covers intentional employee acts that are against the organisation (Hitchings, 1995). The assessment of human behaviour and intention is significant to many researchers focusing on information security. Employees are connected to the internet from the workplace and from their homes, this freedom produces increased security risks to the organisational systems. Therefore, in order to fight against the threat, newly developed effective strategies for protecting the information technologies need to be developed and employees need to be educated so as to improve their attitudes, intentions and behaviours toward information security policies (Zhang et al., 2002).

As has been previously mentioned, information alone will not change peoples' behaviours. Therefore, the next section will evaluate the impact of

training and awareness as a critical factor to enhancing employee compliance to the organisation's security policies, as well as to the improvement of information security management.

2.6 Training Factors

The theory of reasoned action will be used in this study to identify the factors that influence employee behaviour, in order to determine how these factors could be accommodated within information security management and also within the implementation of effective security awareness. Due to the increasing need to improve information security management, many organisations have established information security awareness programmes which aim to ensure that their employees are informed and aware of the various security risks. However, according to Workman et al. (2008), a true understanding of employee behaviours, toward security, have not been fully addressed.

The literature indicates that the lack of knowledge transfer to the job environment is as a result of the majority of training programmes focusing solely on training materials. A recent study by Murphy (2011) critically evaluated organisational training programmes, the research identified that too much instructional material was used even in short training programmes. In addition, despite the increasing number of training and awareness programmes, there is limited evidence to verify the effectiveness of the programmes to the real job environment (Mahapatra and Lai, 2005).

To increase the effectiveness of training and awareness programmes, increase employee motivation is important to consider as this is likely to increase the transfer of skills learned into the workplace. It is therefore important to understand and emphasise the factors that are recognised as being effective rather than ineffective in training. Hwang et al., (2004) maintains that training can help employees to explore the information they need by teaching them deeply effective ideals and manners with regard to how to implement organisational security policy. Gon and Sangjae (2007) indicate that training should be considered an important factor as it can be used to reduce the resistance to change by users – ultimately this would increase the possibility of success of the system adopted. Finally, Cooper (2008) states that training and education must be utilised to change the way people view data as this would generate a change in individual daily habits with regard to data protection.

As a result, the author believes that training programmes could be used to enhance employee perceptions, attitudes, motivations, as well as the transference of skills to sustain new and more appropriate behaviours.

2.6.1 Communication

It has already been established that the development of training and awareness programmes should become a key component for driving the changes that are required for security standards and practices within daily routines. Hinson (2003) suggests that the improvement of security cannot be achieved without skills, knowledge and communication.

Communication is essential as participants need to communicate to become involved during the training. Empirical research, conducted by Mani (2010), agreed that communication skills in the training are considered to be an effective factor that improves employee awareness. Communication allows participants to explain their different perspectives and views by allowing and facilitating discussions between participants which helps them to exchange ideas while also clearly understanding the subject, the facts and the policies. Communication between the participants also allows for them to draw their own conclusions about what they have learned.

Researchers believe that communication is essential for the changing of attitudes (Brinol et al., 2007; Fishbein and Ajzen, 1975; Perloff, 2008). To achieve an effective training and awareness programme, training should incorporate communication techniques which will help to ensure that the appropriate changes in employee behaviours and knowledge are actually transferred into the job place. Furthermore, Noe (1986) states that skill transfer will occur only when trainees have both the ability (I can do), and the intention to transfer their knowledge (I want to do) to acquire and apply new skills.

One of the main challenges affecting information security awareness and training programmes is in the development of a programme that encompasses effective communication techniques that will allow the transfer of knowledge into the workplace (Machin and Fogarty, 2003). Training that utilises effective communication, counselling, feedback, assistance and problem-solving will increase performance which will help to prepare the

individual to make more informed and appropriate decisions. According to Kritsonis (2005), communication and feedback are essential within a training programme as they will also ensure a successful and long-term change. Therefore, communication, within the training programme, is considering an essential element that ensures the success and improvement of information security management.

2.6.2 Learning Motivation

Motivation is consider an essential element of learning that needs to be concentrated on to help participants to learn. It is important to explain clearly the need for the information; to explain this further, Lieb (1991) states that if the participant does not recognise the need or the importance of the knowledge, all of the efforts to learn will be in vain. Participants therefore need to see the advantage of learning in order to be motivated to understand the topic. Various studies suggest that the transference of learning skills will occur when the participant has the motivation and the intention to transfer their own knowledge (Noe, 1986; Tannenbaum and Yukl, 1992).

The review of the literature indicates that there is a positive link between motivation and learning (Mathieu et al., 1992; Quinones, 1995). It is critically important that the individual has the desire and enthusiasm to learn and gain knowledge. A study by Narayan et al. (2007) clearly links the motivation to learn, with acquiring and practising of new knowledge, thus focus should be placed on the benefit of training, and clear and achievable goals should be set as this will help the participant to increase their motivation to learn, as

such this progression will also improve the information security management of an organisation.

2.6.3 Self-efficacy

According to Bandura (1986), self-efficacy is the confidence that a person has in their own capabilities to accomplish a specific task/behaviour successfully. Self-efficacy is essential to increasing a participant's goal to learn, it helps the individual to understand while also diagnosing and dealing with day-to-day organisational problems. Research by Kraiger et al. (1993) concludes that effective training should increase participant self-efficacy; furthermore, positive attitudes and goals should be identified and set in order to accomplish specific tasks in the future. It is important to increase the participant's self-efficacy to enable the individual to believe that they are able to perform a specific behaviour. According to Machin and Fogarty (2003), self-efficacy will help to transfer the knowledge learned in training to the work environment. In addition, their research identified that self-efficacy allows employees to be satisfied in their work which makes them take extra efforts which will ultimately lead to better performance in the work environment. As Torkzadeh and Koufteros (1994) found, self-efficacy has a significant effect on training performance. Therefore, it is critically important to consider and improve upon employee self-efficacy when implementing training programmes, in order to improve information security management.

2.6.4 Satisfaction

The main aim of implementing the above critical elements, within the training programme, is to provide positive feelings and satisfaction in the participant. Satisfaction comes from ensuring that the learner gains positive feelings about their learning experience, throughout the training process. According to Smith (2008), the learner expects certain outcomes and the more effective the outcomes, the more likely the learner is to perform the appropriate behaviour. Motivational strategies, such as: reward, feedback and attention, are likely to increase learner satisfaction (Keller and Suzuki, 2004, p. 232). Bandura (1997) believes that satisfaction allows the learner to participate more actively – they are more likely to work harder, persist longer and act stronger when encountering difficulties. As the literature indicates, it is important to consider the satisfaction of the employee during the training programme as increased satisfaction is likely to significantly improve information security management.

2.6.5 Reinforcement

According to Mani (2010), wasted training is considered to be a common problem in many organisations, due to a lack of appropriate reinforcement of the training. Research conducted by Gupta and Bostrom (2006) indicates that the development of effective training is considering one of the most important methods for enhancing and improving performance. According to Goldstein (and Ford, 2002; Kirkpatrick, 2007), the success of the effectiveness of the training should be based on the transference of the knowledge into the work environment. According to the above literature, the

author believes that effective training techniques should emphasise and improve employee awareness by changing their attitudes and enhancing their motivation to transfer the training knowledge and skills which will improve performance on a daily basis.

It is critically important that a link is established between training, learning, behaviour and performance. Effective training programmes need to be developed that will follow clear guidelines and principles for the employee and the various factors that might affect the training should be taken into account. According to Subrahmanian (2010), effective training should be based on the identification of training needs to determining the forms of training needed, monitoring of how the training is transferred into the work environment as well as a thorough evaluation of the training process should be conducted to truly determine whether it is effective. It is critically important to understand that what makes training effective is not simply the way that the participant feels or how the training programme is evaluated, it should be based on whether it has influenced and changed behaviours toward security. As Laoledchai (2008) states, if a user fails to transfer the skills and the knowledge gained from the training programme then the training has provided no value to the organisation.

2.7 Summary

This chapter has reviewed the literature on information security and the various factors affecting it (see Figure 2-2). In addition (as can be seen in Figures 2-3, 2-4 and 2-5), the literature review has also identified the various

organisational, behavioural and training obstacles that can affect information security.

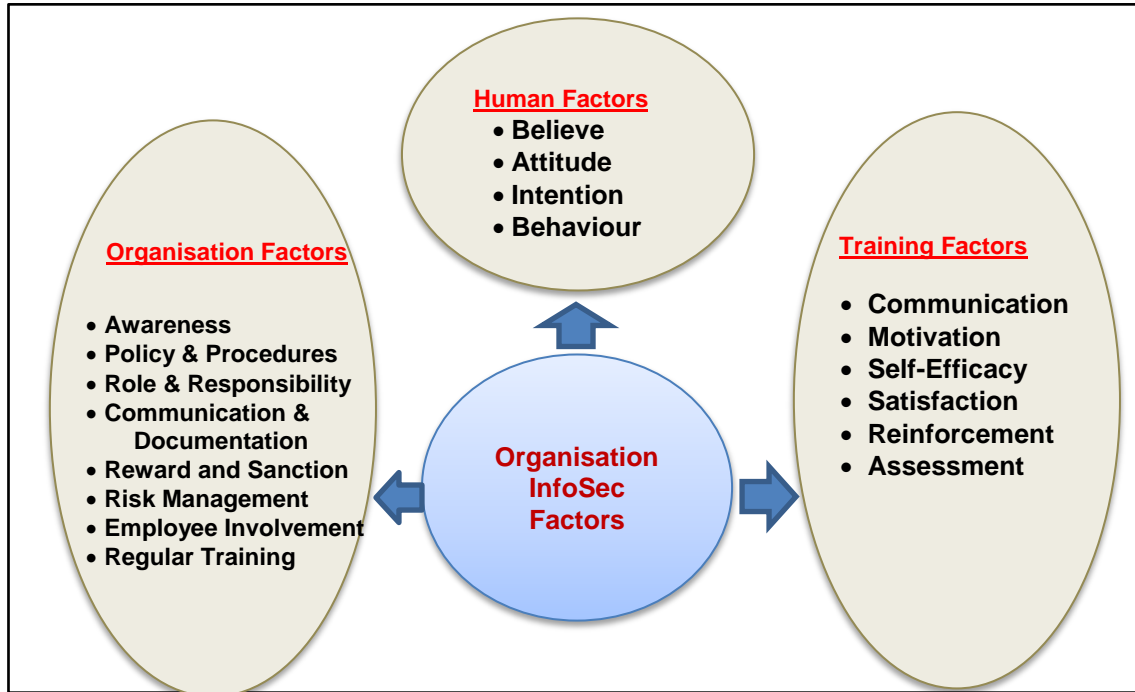


Figure 2-2: The Various Factors Affecting InfoSec

Source: Researcher and reviewed literature

Chapter 3: Research Design and Methodology

3.1 Research Methodology

This chapter will discuss and explain the reasons behind the choice of the selected research strategy and methodology for this study.

There are many different research methodologies, all of which provide means for collecting data from a variety of sources. It is critical to the success of the research to select the most appropriate methods which enable the researcher to conduct high quality final outcomes. According to Steele (2000), it is essential that the best methodology is selected in order to ensure that the research objectives are met and that the findings are validated. According to William (2003), research methods include strategic decisions over the data collection methods, procedures and data analyses.

3.1.1 Qualitative Research Methods

Creswell (1998) defines the qualitative method as the process of understanding a social or human problem, based on a complex or holistic picture, word or report which records information from a natural setting. Neuman (2004) states that the qualitative method focuses on understanding a phenomenon, by explaining the meaning of it. Qualitative methods utilise descriptions and explanations by way of observation and involvement to gather, analyse and interpret data that is obtained through the observation of what people say and do.

Qualitative research is connected to the individuals' account of their own attitudes and behaviours; it can, therefore, provide valuable insight into the reasons behind the way in which people choose to perform a said task, action or behaviour. Qualitative methods are helpful because they provide rich explanations of complex phenomena, as a result of the proposing of hypotheses to understand certain phenomena. The ultimate value of the qualitative research is based on the validity of the information received. To illustrate, qualitative data is obtained through interviews, observations, questionnaires and pilot tests, it is, therefore, accepted as being an accurate report of the participants' opinions and experiences.

A qualitative investigation is the most suitable method for the nature of this research as it provides the researcher with the ability to understand the reasoning behind what leads people to behave as they do towards security.

3.1.2 Quantitative Research Methods

The quantitative method can be described as research involving the use of structured questions, with predetermined response options, that are administered to large numbers of participants (Eisen, 2006). Quantitative methods examine the relationship between variables in order to support various research questions. According to Carr (1994), and Scandura and Williams (2000), quantitative methods provide valid scientific answers about the actions and changes that may have occurred based on the results, that are usually based on larger sample sizes, in order to provide generalisations about the outcome results. According to Neuman (2000), the quantitative

research method is characterised by: the measurement of objective facts, focusing on variables, focusing on the importance of reliability, providing results that are independent of the context, and by, to some degree, being characterised by statistical analyses and statistical results.

Depending on the nature of the problem, a researcher will decide to use the quantitative approach for the following two reasons. Firstly, the use of a quantitative approach allows a good fit for the development of a relationship between the social reality of the research participants and the theories presented. Secondly, it allows for the studying of the cause of employee behaviour and the effect of different factors and behaviours. A good explanation of this was presented by Nettleton and Taylor (1990), they identified that the aim of the quantitative method is to provide the accurate measurement of social action, by explaining the causal relationships that are related to specific events.

Table 3-1: The Strengths and Weaknesses of the Quantitative and Qualitative Methods

	Qualitative analysis:	Quantitative analysis:
Strengths	<ol style="list-style-type: none"> 1. Allows for a complete, rich and clear description. 2. Allows for good insight into the experiences and behaviours of the interviewee. 3. Can be cheaper than quantitative. 4. Can be simpler to undertake. 5. Allows for the ambiguities which are inherent in human language. 	<ol style="list-style-type: none"> 1. Provides higher levels of accuracy. 2. Provides features and result that are more significant and focused. 3. Provides findings that can be generalised to larger populations. 4. Allows for the presentation of graphical analyses. 5. Allows for the margin of error, as missing values can be calculated.
Weaknesses	<ol style="list-style-type: none"> 1. Can be difficult or impossible on qualitative data. 2. Needs a higher level of interpretative skill. 3. Provides a lower level of accuracy in terms of statistical analysis. 4. Is usually based on a smaller sample size. 5. Can mean that it is difficult to generalise as the results are often based on a limited number of cases. 	<ol style="list-style-type: none"> 1. Is slow to complete because it is very time consuming when compared to qualitative analysis. 2. Can be expensive. 3. Is not simple to implement. 4. Usually requires some form of computer analysis.

Source: Based on Ghauri et al. (1995) and Bernard (2000)

3.1.3 Triangulation Method

According to Denzin (1978), triangulation is defined as the combination of methodologies to study the same phenomenon. The triangulation method consists of the utilisation of two or more methodologies to increase the level of validity of the research. Since the quantitative and qualitative approaches carry comparative strengths and weakness (see Table 2.1), it is imperative that the researcher identifies the most appropriate approach that allows for the best result for their research. As Bryman (1995) indicates, triangulation is the most useful method for the study of issues that have not been previously studied, in detail. Moreover, the literature indicates that many researchers are now using the triangulation method in order to provide further clarification

of their finding. According to Jankowicz (1995), there are two main advantages of using the multiple method:

- Firstly, different methods can be chosen and applied for different purposes within the research.
- Secondly, the use of several methods allows for better analyses and triangulation to occur.

Despite the fact that triangulation requires a greater commitment of time and cost, these costs are potentially worthy as they have the ability of removing the biases that are usually associated with the use of one method (Jick, 1979). The use of multiple methods reflects an attempt to understand, in-depth, the phenomenon in question (Denzin and Lincoln, 2000). Many researchers have reported the value and benefit of using both the qualitative and quantitative methods (Neil, 2007; Neuman, 2000; Saunders et al., 2000).

In order to improve the validity and the strength of this research, the researcher decided to use the triangulation approach in order to increase the credibility and validity of the results. Carson and Coviello (1996) recommend that research should be based on the development of a proof of knowledge through the combination and adoption of multiple approaches, as this provides more reliability.

3.2 Research Design

The establishment of the research design is considering to be an important task in any research. The chosen research design needs to define not only the reason for the study, but also the direction of what and why the data will be gathered. As Mouton (1996) states, the main function of the research design is to enable the researcher to anticipate what the most suitable research decisions should be.

According to Rich and Ginsburg (1999, p. 371), no research approach is complete or perfect as all of the qualitative and quantitative methods have both their own inherent strengths and limitations. This supports the concept of combining both the qualitative and quantitative methods within the research to avoid the limitations of each method; thus, providing a balance from the strengths in a way that helps to avoid overlapping the weakness. The utilisation of both approaches will help to produce better outcomes in terms of quality and scope (Tashakkori and Teddlie, 1998; Carr, 1994).

In providing an overview of the qualitative analysis approaches, it is apparent that there are different ways to analyse the qualitative data. The analysis is linked to the level of structure and the procedural requirements that are specified in the research. The qualitative method allows the researcher to collect data in different formats. This guides the researcher to give clear direction into which data should actually be gathered, as well as to the means that it will be gathered by.

This study has adopted the multiple method approach to help with the qualitative analysis in which the credibility and reliability of the data will be processed after its collection from: semi-structured interviews, questionnaires and pilot tests. According to Yin (2003), the qualitative data can be obtained from a document, interview, observation or record.

3.2.1 Interview

An interview is considered to be a flexible technique as it allows new questions to be brought up during the interview, it can also provide great depth from the responses given. Interviews provide the researcher with opportunities to reach their objectives by allowing for the full understanding of a respondents' point of view, rather than simply relying on sweeping statements about behaviours and attitudes toward information security. This research will adopt the interview methodology to enable more freedom and the adaptation of questions in the interview situation. To validate the outcomes from the literature review, interviews will be conducted with a group of people. The interviews will focus on different types of vulnerability for organisations in terms of the security breaches that accrue within organisations. The interview should also obtain feedback from the interviewees which should help to determine their behaviours toward security. This approach also gives people the opportunity to reveal more detailed reasons and explanations for their actions and decisions toward different incidents. According to Yin (1994), an interview is one of the most significant data collection methods because it is essentially a human affair and involves human interactions.

This research project will use the following interview approach:

- Semi-structured interview. This type of interview normally consists of various questions which will be covered and data will be recorded. The interview will use open-ended questions which will start with general questions; interestingly, many of the questions will be created during the interview in response to the answers provided by the interviewee. Semi-structured interviews allow the researcher to probe further in order to gain more information about certain areas – often this will not have been planned for, but it is likely to be of use to the interviewer. In practical terms, the interview is a very helpful method as it can be recorded.
- Face-to-face. A face-to-face approach allows for the obtaining of rich data which will provide further understanding of the area being studied, however they are usually very time consuming.

This research will utilise a semi-structured interview using the face-to-face technique in order to explore different information security issues. The information provided should be detailed and connected to real-life. It will provide an in-depth analysis of the factors that influence individual behaviours toward information security. Furthermore, the development of a positive relationship between the interviewee and interviewer is needed to ensure that the interviewees' attitudes and beliefs are explored openly.

The interview questions were structured and divided into three parts/interviews. The goal of the first interview was to gain insight into the

organisational factors that relate to information security management, as well as thoughts into aspects that may reduce information security breaches. The second interview aimed to explore and use theoretical insight as a reference point to understanding the interviewees' attitudes toward the use of computers in order to analyse the internal and external factors that affect their behaviours. The third interview aimed to explore the impact of effective training and awareness programmes on security management behaviours.

3.2.2 Questionnaire

According to Saunders et al. (1997) and Marshall (2005), questionnaires are considered to be one of the most popular data collection methods among researchers because they can obtain a wide range of information about specific or varied research problems (McMillan, 2000). Questionnaires also provide a relatively inexpensive way of gathering data from potentially large numbers of respondents. Questionnaires are commonly used as they allow researchers to look more critically at peoples' understanding of specific issues while also establishing knowledge that is based on their attitudes and behaviours. Many researchers acknowledge that questionnaires are advantageous as they allow for the obtaining and generalisation of data, while at the same time providing respondents with the freedom to express their own opinions and beliefs (Casewell, 1989).

In order to collect a wide range of information, a standardised questionnaire needs to be developed with clear and concise instructions for all parts and

sections. Each group of questions needs to have a separate and clear title to ensure that it is clear for the respondents to follow.

The researcher decided to use closed questions in order to provide a variety of possible responses to be chosen from. Closed questions are very popular because they provide standardised answers; furthermore, these uniform answers mean that they are easy to code and some critical analysis on the data can be provided.

The questionnaire design will contribute to this research study as data will be collected from different points of view and it will then be critically analysed in order to determine the users' level of knowledge of security management, and to determine the user level of understanding of the different factors that could reduce security breaches and minimise security risk.

This research will therefore conduct on online questionnaire which will explore a variety of factors that affect the implementation of security policies within organisations. Furthermore, it will identify various factors which are deemed to reinforce and sustain appropriate behaviours in employees in order to reduce security breaches and improve information security management.

3.3 Reliability and Validity

Reliability and validity are two fundamental measures that need to be considered when designing a research questionnaire. No matter which

process for gathering information is chosen, it must be examined critically to evaluate the extent to which it is likely to be valid. According to Patton (2004), an instrument is valid if it accurately measures what it planned to measure; thus, it measures what it was designed for. Reliability, on the other hand, includes the extent to which a test or procedure is likely to provide similar results, under consistent conditions, if tested on another occasion (Kalton, 2001).

The conduction of a pilot test is considered to be the first phase in achieving a valid and reliable survey. If it is truly reliable, then if someone re-conducted the study after studying the measurement scale and scope, they should be able to apply the approach reliably in a different time and space. Accordingly, the use of the triangulation method also enhances validity and reliability within a study because it gives depth of meaning to the information by facilitating the exploration of multiple perspectives (Henerson et al., 1988). Finally, the questions presented within the semi-structured interviews and questionnaire were validated and checked for reliability by conducting the following:

- Approval of the questions by an experienced person, who has worked within the field of information security for more than ten years.
- Some modifications were incorporated, as a result of the experienced person critically evaluating the questions, in order to increase clarity, question wording and validity which will ultimately enhance the outcome of the results.

- A pre-test of both research methods to check that the questions were understood in the way they were intended, with a small sample of people before the actual study was conducted. This also allowed the researcher to check: the length of time that would be needed to complete the task, how comprehensive the questions were, and how relevant the themes would be to the research topic.

3.4 Summary

This chapter has identified the methodological approach for this research. The researcher will utilise a combination of qualitative (interview) and quantitative (questionnaire) methods to collect data. The literature shows that each of the mentioned research approaches have their own advantage and disadvantage points. As a result, a combination of qualitative and quantitative research methods will facilitate the researcher to gain the best outcome in order to overcome the weaknesses of each method.

Chapter 4: Qualitative Data Analysis

4.1 Introduction

In order to explore and identify successful factors for the implementation of information security policies in organisations, a qualitative approach was used as the basis of this study. This chapter will not only present the information obtained from these interviews, but it will also analyse them in order to identify the factors that maximise effective information security policy compliance among employees.

The remainder of this chapter will be organised into the following sections. Section 4.2 presents a discussion of the criteria used for selecting the participants for the qualitative research; this will lead into section 4.3 in which a detailed discussion will be given with regards to the choice of questions chosen for the interviews. The following three sections, sections 4.4 to 4.6, will analyse the answers provided for the set questions – this analysis will be divided based on one of three key factors that relate to information security compliance: first, organisational factors; second, behavioural factors; and, third, an assessment of the current training and awareness programmes that employees may be exposed to. Next, section 4.7 will present various lessons that have been learnt as a result of the qualitative data analysis, and finally, section 4.8 will provide conclusions for this chapter.

4.2 Selecting Participants

Before commencing the qualitative data collection, via employee interviews, some thought had to be given into the manner in which individuals would be selected for the interview process. Once selected, the research questions would then be used to collect qualitative data, in order to explore user experiences, behaviours and attitudes toward information security. In order to make the data comprehensive, it was decided that forty interviews would be conducted with both male and female participants that were aged between 25 and 55. The participants were carefully selected to ensure that a cross-section of companies were equally represented from the banking, health, business and education sectors.

4.3 Interview Structure and Format

Each interview was planned to last for approximately one hour. A semi-structured approach was used for each interview in order to encourage a positive relationship between the interviewee and interviewer in order to help the exploration of attitudes and beliefs in the most open way. In addition, the use of semi-structured interviews provided the researcher with more scope to probe and gain more information about certain questions, while also providing for the obtaining of more information into areas that may not have been considered but that the interviewer identified during the interview as being potentially beneficial to the aims of the study. This structure allowed the interviewees to explore their attitudes and behaviours more comprehensively, with guidance from the interviewer. Furthermore, the interviewer is able to complete the objective of the study by fully

understanding the interviewees' point of view, rather than the results being based solely on raw quantitative data and assumptions.

The interviews were arranged based on the interviewees' commitments and they were held in the interviewees' own office to help reduce any inconvenience. A written description of the aims and the objectives of the research study were provided in advance and all of the participants were advised of the ethical considerations which included information about the confidentiality of the data collected. In addition, all of the participants were given the option of choosing to partake or decline partaking in the interview, and they had the option of declining having the interview recorded. All of the participants requested that their information, and the organisation in which they worked, remained anonymous and not named. The request about anonymity was not surprising because of the sensitive nature of information security (Doherty and Fulford, 2005).

The interview was divided into three parts, each of which covered one aspect of information security. The first part was to gain insight into the organisational factors that relate to information security management and the reduction of information security breaches. The second part aimed to explore the existing behaviours and attitudes that individuals had in relation to information security compliance. The final part of the interview focused on the existing training programmes that individuals had encountered with regard to information security, they were asked to identify the good elements as well as to identify elements that they would like to see more of in any future programmes.

The current practices of information security within the organisation were assessed to determine the following:

- Employee awareness of their organisation's security policy;
- Do they understand this policy and are they aware of the purpose of the policy;
- How organisations present their security policy to employees;
- Whether any employees are involved in the development of the security policy;
- Whether the organisation gives training regarding the policy to the employees;
- How the organisation enforces the policy;
- And, whether the organisation reviews the policy with the employee.

Understanding the factors that impact employee behaviour towards compliance with information security:

- How important they feel information security compliance is;
- What their concerns are about their organisations' information security policy;
- What they think they could do to reduce information security breaches;
- And, identifying potential strategies for changing and improving their ability to maintain appropriate behaviour towards information security.

Evaluation of the effectiveness of information security training that their organisations has provided:

- Have those that received training changed their attitude and behaviour after receiving the training;
- Is the training programme successful;
- What were its limitations, if any, how is its success measured;
- And, identification of important criteria for developing an information security training session, in general.

All of these questions relate to the three main themes mentioned above. The participants were asked to elaborate or explore related issues whenever it was felt that additional information would be of value, to the aim of the study, with regard to a particular line of enquiry. At the end of each interview, it was ensured that each of the three main themes of: organisational policy, employee behaviour and effective training on information security had been explored fully and in detail with each participant.

4.4 Employee Views on Organisational Information Security Management

This section will focus on the questions that were asked with regards to the existing security policies and frameworks at each of the interviewees' organisations. The section will be divided into sub-categories which relate to

this theme, and an evaluation of the data collected during the interviews will be given in relation to each category.

4.4.1 Information Security Policy

Does your organisation have a policy on information security management? If so, how effective is it in reducing information security breaches?

As expected, the findings from the interviews show that all of the employees revealed that their organisations did indeed have information security policies which included the core universal elements of confidentiality, integrity and availability. A typical response, in relation to the first part of this question was:

“Yes, we have an organisational information security policy with clear instructions on every single aspect of information security”.

The data gathered also revealed that by actually having a security policy it was seen by employees as being a crucial foundation of their respective organisation. Moreover, although all of the employees from the different organisations illustrated that they had an organisational information security policy in place, most of them also pointed out that there were some barriers affecting the way in which they comply with the implementation of the policy.

To illustrate, typical responses, in accordance with this view, included:

“Yes we have organisational information security policy and I do understand what the purpose of information security is, but there are many employees who

do not understand and I cannot blame them because of their limited knowledge of technology and related problems to information security."

"Yes we have organisational information security policy, however it is not presented effectively to help us to reduce information security breaches."

"Yes we have organisational information security policy, but it is hard to comply with it."

"Yes we have organisational information security policy, but it is not effectively visible and accessible all of the time, just somewhere on the shelf."

From evaluating these answers, it is possible to confirm that employees generally believe that information security is important to them and to their organisation, and they are, indeed, motivated to apply all of the policies. However, there are some barriers to this as employees ultimately feel that the organisation should have clear and concise policies/instructions on all aspects of information security, and on how users can effectively deal with any incidents that they may face, regarding information security.

4.4.2 Awareness

All of the participants strongly agreed that an awareness of the organisational policies was an essential and obvious factor for its successful compliance and implementation. The employees went on to explore the existing barriers which may have contributed to any lack of awareness that they may have regarding their organisational security policy. For instance, one of the employees believed that:

“The policy is too big, [there is] no time to read all the policy and remember it all the time”.

The majority of respondents agreed with this sentiment, this was characterised by the following quote from an employee:

“I am not aware of the policy requirement as I have no time at my work”.

Another recurring view, among employees, was that the policy remained relatively inaccessible to most workers. This obvious barrier to its effectiveness was clearly made by the following statement from an interviewee:

“The policy is not effective because it is not visible all of the time, it is somewhere in a material book in a drawer, which makes it impossible to remember the detail”.

As a result of this inaccessibility, it is no surprise that a large number of respondents were unaware of the implications of non-compliance with the security policy. For instance, one respondent said:

“I am not aware of all of the threat, nor am I familiar with the possible consequences of it”.

The interviewees indicated that the policies are not generally visible all of the time and, in some cases, they are stored in inaccessible locations. This makes it difficult to remember the various aspects of the policies and leads to poor management when incidents occur. The interviewees noted that they had undertaken very few information security actions as they claimed to have

had no time to read and remember the policy; thus, they were not only unaware of the threats, but they were also oblivious of the possible consequences of such security breaches. Finally, a minority of interviewees indicated that an increase in workload would cause a conflict of interest between information security and functionality, as they felt that the documentation is so large that it would be impossible to read it all.

These responses indicate that the majority of employees may fail to comply with the organisational security policy because there are various barriers in the way; therefore, the policy is not effective because it is not visible all of the time and it is often difficult to locate and thus impossible to remember. Ultimately, the lack of effectiveness by an organisation to appropriately present its policy will inevitably lead to a lack of awareness of it.

From analysing the various responses on this area, it is clear that there is a need to present a company's policy in an accessible, prominent and eye-catching manner. Possible examples could include: the placing of images within the policy itself, so that it becomes more memorable; making it more descriptive; physically handing it out to employees; the use of emails; the use of the main points as possible screen-savers, on cards, on discs and on noticeboards. All of these actions would help employees to remember their organisation's policies better as it would help them to apply it all of the time because it would keep it fresh in their minds.

Nearly all of the interviewees suggested there was a relationship between increased awareness and increased compliance of an organisation's policy.

Therefore, in order to help increase the actual compliance to an organisation's security policy, organisations need to adopt a suitable awareness procedure towards it. In other words, the more awareness employees have, the more likely an organisation will have satisfactory and smooth compliance toward their organisation's security policy.

4.4.3 Role and Responsibility

All of the participants agreed that the defining of clear roles and responsibilities is an essential success factor for compliance with organisational information security policy. The participants generally held the view that, by doing this, every employee would know what they needed to do with regards to their organisation's policy; thus, they would be fully aware of their personal responsibilities. The majority of employees claimed to be willing to comply with their organisations' security policy. However, the interviews revealed that the main reason why they failed to comply, which can be added to the ones discussed in the preceding sections, related to a lack of clarity with regards to individual roles and responsibilities. A repetitive theme emerged from the responses which indicated that this lack of clarity often led to laziness and a failure to take personal responsibility when applying organisational procedures. This lack of clarity and responsibilities led to the following three similar responses among participants:

"I think information security is not my job and, therefore, I do not consider it to be my priority".

"My job does not need information security to be its main focus."

“The following of information security policy is not a part of my role, as I just need to do my job.”

In general, there was a widespread belief from the employees that a major factor affecting their lack of commitment to following the policy was, as a result of their belief, that information security was not part of their job which meant that it was not their priority. This highlights how individual beliefs can affect the implementation of organisational information security policies. Consequently, this could lead to risky behaviour and, thus, to an unsafe environment that could lead to an increased number of security breaches within an organisation. One respondent offered a concise summary of this issue:

“I think to be able to consider information security my responsibility, I need to be completely aware of what I need to achieve and what the desired outcome would be”.

Even when employees were aware of their roles and responsibilities toward information security, they often chose to ignore them, for instance:

“I think in order to get things done at work, I need to ignore some of my role and responsibility toward information security”.

Similarly, one of the senior employees held the view that:

“I think being too cautious about my responsibility towards information security will make it impossible to carry out my work smoothly”.

Likewise, another employee stated:

"I think I will ignore some of my roles and my responsibility if I am concerned about getting the job done".

Another very interesting viewpoint, held among employees, was expressed best by one senior employee as:

"I am not familiar and aware of my role and my responsibility of the organisational information security policy because of the fact that any incident that occurs will be handled by security professionals and the fallout and the replacement of the losses will be dealt with by others".

This statement highlights the blinkered approach that currently exists among a minority of employees: the issue of security as another person's problem or, often, as a problem specifically for the information security team. These employees view their role to be exclusively meeting their own job's objectives, and they do not equate information security as being an issue that affects them in terms of meeting their own objectives.

The senior managers, that were questioned, almost entirely felt that the blame for any existing failure to take responsibility stemmed from the fact that:

"We provide good security policy, however employees sometimes do not comply with it due to laziness and irresponsibility".

Most of these senior managers did, however, see this as a big problem:

"Top management believe that if employees do not consider information security policy as their role and responsibility, then that means they are neglecting a core organisational policy requirement".

Some went on to offer suggestions on how to ensure that employees take on more responsibility, to illustrate:

“An organisation needs to develop a reinforcement system that encourages and motivates employees to follow their roles and their responsibility”.

Therefore, it becomes clear from the responses, from senior managers, that there is a concern that individuals are not currently taking responsibility for information security. While some of these managers place the blame for this squarely on the employees' shoulders, others were willing to admit that organisational changes are needed to help instil more responsibility among employees.

To summarise, some employees note that they do not feel that information security is their responsibility and they do not consider it to be their priority as they only have to concentrate on their own working tasks. These employees often feel that if they were to take more responsibility, then it would affect their ability to deliver their work. Furthermore, they believe that if security is in place, then they should not be required to carry out security tasks as they assume them to be the responsibility of the designated security professionals who will handle the incidents and restore any losses immediately. Thus, the effectiveness of employee roles and responsibilities, and the power to reinforce information security actions, is lacking among employees. Finally, the senior managers indicated that they often feel that security measures are adequate and that there are systematic failures among employees which cause breaches and which are not taken responsibility for. To this end,

many senior managers blame the employees entirely for this failure, though some did feel that their organisations need to do more to reinforce responsibility among their staff.

4.4.4 Communication and Dissemination

All of the participating employees strongly agreed that an effective communication system, between employees and managers, is another vital step affecting the successful compliance of an organisation's security policy.

For instance, one response in support of this issue noted:

"I think communication between employees is critical and essential to the effective implementation of information security policies".

Another similar response stated:

"I think regular communication between employees and managers is an effective way to increase compliance with the organisational information security policy".

Specifically, many interviewees highlighted inadequacies in communication between their organisation's IT department and the rest of the company. To illustrate, one employee stated that the reason for his lack of knowledge, concerning security, was because of:

"I do not face and communicate with professional IT people and, therefore, I do not see how they handle and recover any incident – so I am unable to learn from this".

Another employee confirmed this notion by focusing on communication:

"I think regular communication between the IT department and the employee is not effective in our organisation".

A common point, made by most of the respondents, was that more communication was required specifically on the existing security policy. For instance:

"I think regular feedback and updates on information security policy requirements are necessary when implementing the information security policy".

Similarly, another employee noted that:

"I think as employees we do not receive any feedback or updates on information security issues".

This respondent went on to elaborate that it would be helpful if they could receive at least an email to inform of specific things that are being done wrong with regards to information security.

On a more positive note, the majority of employees agreed that if they wanted to be more proactive, then they could easily obtain the information that they need. To illustrate, one interviewee noted:

"It is easy to get information quickly – if I have a query about the information security policy, I know who to contact directly".

However, a general consensus exists among the employees, indicating that more should be done, for instance:

“Having regular workshops/discussions about information security with security experts would help improve compliance with the organisational information security policy”.

This employee went on to note that it is the responsibility of senior managers to not only remind people of the importance of policy compliance, but that these managers should also act as role models because they themselves would then be seen as taking the issue seriously.

The dissemination of the existing policy was also a key issue that many employees felt that their organisations failed upon. Responses on this issue included the fact that this lack of dissemination could lead to complacency:

“I think the reason for not having a copy of the documented policy is that the management does not feel it is important and critical to implement and comply with the policy effectively”.

Employees generally felt that by not actually having a documented policy passed on to them (via email or as a hard-copy), it encouraged them to ignore it. Therefore, there appears to be a pressing need to improve and implement different methods of communication, dissemination and cooperation between the employees and the security experts, in order to better implement the organisational information security policy.

All in all, the interviewees considered communication, or the lack of it, a barrier to complying with information security management. This signifies the important requirement for the sharing of knowledge between employees, managers and the IT staff, in order to increase employee involvement and to

avoid the necessary resolution of security incidents. This will inevitably increase an organisations' capability while also improving individual self-efficiency when practising information security actions.

4.4.5 Rewards and Sanctions

From all of the organisational factors that were explored with the employees, rewards and sanctions seemed to have the strongest resonance. All of the participants strongly agreed that rewards and sanctions are extremely effective in motivating employees to comply with an organisation's security policy. In particular, the threat of disciplinary procedures seems to be the biggest motivator in encouraging compliance.

In terms of rewards, the majority of the interviewees agreed with the sentiment that:

"Rewards, such as increasing salary, title, position, and certificates, would motivate employees to comply with the information security policy".

On the other hand, all of the respondents felt that the use of an enforced, stick, approach would be equally effective. To illustrate, three similar responses confirm this notion:

"I think sanctions (such as re-training, fines, monitoring) would encourage and motivate employees to comply".

"The application of sanctions is the best way of improving employee behaviour towards implementing the organisational information security policy."

“Rewards and sanctions allow a better attitude and create a security culture.”

In general, respondents held the belief that the application of the disciplinary procedure is an essential factor that will lead to improving employee behaviours and changing habits. Thus, the implementation of rewards and sanctions increases interest, performance, motivation and they help to improve employee behaviours toward security. Conversely, the interviewees universally felt that the absence of disciplinary consequences acts as the main reason why employees fail to comply with the organisational security policies, for example:

“I think the fear level and the implication of the consequence is low in regards to information security policy”.

As far as the senior managers were concerned, one held the view that:

“I believe that the cost of cautious behaviour, in terms of time and effort in complying, is seen as being higher than the perceived benefits of cautious behaviour”.

Another senior manager believed that:

“I think the top management level should apply disciplinary procedures by applying it consistently if employees do not comply with the organisational information security policies”.

Interestingly, the employees agreed that:

“I think pressure and threat of discipline raises my effort and allows me to be more focused”.

However, due to the lack of enforceable disciplinary procedures, employees are currently not aware of the consequence of non-compliance. As one respondent noted:

"I am not aware of the consequences of not conforming to the policy due to the lack of the reinforcement procedure, and this will continue unless things change".

Consistently, employees felt that the disciplinary strategy was lacking and that rewards were not in place for those that actually complied with the policy. In general, it was felt that there were worries with regard to the implications and consequences on the lower level which leads to less effort being made to comply with the information security policy across all levels. Hence, they felt that the use of reward and sanction strategies would lead employees to participate more readily by making a concerted and persistent effort to work and achieve the security goals. These strategies would also motivate employees to be stronger when they encountered difficulties. The interviewees also identified various examples of effective rewards, including the use of: bonuses, salary increases, praise, recognition from others, titles, certificates, new responsibilities, extended breaks, more flexible working hours and gifts vouchers, to show the appreciation for their improvement of undesirable habits regarding information security.

4.4.6 Risk Management

The vast majority of respondents accepted that the process of risk management was essential in helping to prevent security breaches. For instance, one respondent stated that:

"I think my organisation conducts risk assessments, and these have reduced security breaches".

From those that were unaware of their organisation's risk management processes, there was still agreement with regard to its potential benefits:

"Applying and following organisational risk management will help to reduce security breaches".

Although the majority of participants agreed on the importance of conducting and applying risk management, many of them indicated that they were not aware or familiar with their organisation's risk management procedure, as illustrated by the following response:

"I think we need to be more aware and familiar with the organisation's risk management procedure".

One of the senior participants elaborated on this point further, by stating:

"I think it is very important that the organisation provides training and awareness to help employees implement risk management effectively".

Another employee, who was more familiar with the risk management process at his organisation, summed up its benefits as:

"I think being familiar with risk management allows me to understand, analyse and respond to any incidents that might occur".

From the interview responses, it is clear that employees understand the importance of being aware and familiar with the risk management procedure,

as a means for reducing risk. This fact signals the need to provide an effective training and awareness programme that enables the employees to respond accordingly to any incident that might occur. One employee felt that the best way to understand the organisational risk management procedure is through communication with the IT professionals:

“Communication and discussion with the security professionals will help me to become familiar with security incident recovery and reporting procedures”.

A similar response also noted that:

“I think communication and discussion with the internal and external professionals will help me understand what needs to be done when facing a security incident”.

Ultimately, there was a general lack of confidence among employees with regard to what needs to be done when facing security breaches, in terms of minimising the impact of these. Most of the respondents noted that if a situation arose, they would contact the security personnel to obtain advice on the situation. In identifying any steps that employees could themselves take to minimise impact, a general view developed that training and communication between employees and security professionals would be hugely beneficial. In this way, a more proactive approach could be utilised to build confidence that any security incidents that were encountered could be managed more effectively.

4.4.7 Summary of Employee Views on Organisational Factors Affecting Security

In the preceding sub-sections of section 4.4, various employee views have been presented and analysed with regards to the organisational factors that the interviewees felt affected information security. Their overriding concerns can be summarised as follows:

- The existing policy does not seem accessible enough to the general employees.
- There is a general lack of awareness of the organisational policy.
- Roles and responsibilities regarding information security are not clearly and adequately defined.
- There is a lack of communication and dissemination of the existing policy.
- There is a lack of reward and sanction in complying with the policy.
- There is a lack of knowledge about risk management and what needs to be done when faced with security breaches, in order to minimise the impact of these risks.



Figure 4-1: Organisational Obstacles Affecting InfoSec

4.5 Employee Views on Behavioural Factors Affecting Information Security

This research aims to understand the factors that impact on user behaviours toward information security; therefore, it aims to identify the different strategies that may be used to change and improve employee behaviours which will ultimately influence an employee’s ability to maintain appropriate behaviours toward information security. It is therefore important to understand how people behave, as this knowledge could be of use when devising a strategy which aims to increase information security consciousness and awareness. In this section, four separate aspects of

behaviour will be highlighted (beliefs, influence of others, behavioural intent and changing behaviours). All four aspects were explored with the interviewees, the results and analysis of their responses will now be presented in the following sub-sections.

4.5.1 Beliefs:

What are your personal opinions on the importance of information security policy, and on your current behaviour towards it?

There was a strong belief from nearly all of the respondents that:

“Having information security policies in the organisation will reduce employee errors that lead to security breaches”.

One respondent explained this further by noting that security policies:

“Will help to reduce human mistakes – if we are ready from inside, it is a great defence for the organisation”.

Despite this, and as discussed throughout the previous section (section 4.4), the majority of respondents were of the opinion that there were a number of organisational barriers that affected the way they behaved towards the existing security framework. One interviewee, for instance, noted:

“I believe complying with the information security policy is very important. However, there are some barriers in place, which are not helping us in sustaining the good behaviour”.

These barriers included: a lack of awareness (*“I am not completely aware of the organisational information security policy”*) and uncertainty about the responsibilities and time constraints (*“I believe that there is no time available in the workplace and I am too busy to think about the organisational information security policy”*). The net effect of these barriers is that some employees are likely to be unable to fully comply with the policy even if they wanted to.

For instance, one interviewee noted:

“I do not get regular reminders on information security procedures which inadvertently makes me think that I am working in the right manner”.

This interviewee did not feel that it was part of his remit to investigate whether the information he was using was up to date – moreover, he felt that he should be updated automatically.

Similarly, others felt that the blame lay entirely with the senior managers. This notion can reduce the importance of their compliance and it can even be used to help justify their lack of compliance, to illustrate:

“The top management teams do not contribute too much as role models and don’t really facilitate the sharing of knowledge and experience”.

Another respondent had an issue with the manner in which the information was dissemination from the senior managers to the employees:

“The top management do not provide the organisational information security policy using effective techniques; it is boring, too long, no reminders are in place and the presentation of it is poor”.

On the other hand, most of the top managers disagreed with the above viewpoint:

“We provide a good influence, as well as regular communication and cooperation with the employees”.

Likewise, another manager acknowledged:

“We provide useful information to all employees by sending emails and leading articles about security breaches”.

The above conflict, between the opinions of the top management team and the employees, shows that there is a lack of agreement with regards to who is to blame for not implementing the right behaviours and habits among employees. Most of the employees point the finger towards the managers by stating that it is because of their failings that the employees can justify their failings in terms of understanding the importance of behaving appropriately/inappropriately in regards to information security. On the other hand, the managers were also very willing to identify any failings towards the employees – it is their failure to comply, their beliefs and their habits that are the problem. In truth, as all of the respondents from the survey came across as honest and trustworthy, it is likely that the blame must be partly in both camps. Some management failings must exist, but this is possibly being jumped upon by employees, who use these failings to justify their behaviours.

Finally, a minority of respondents also felt that their behaviour was exactly what was required from employees within their organisation. Responses from this group of individuals included the following:

"I am familiar with most of the information security procedure and I think my behaviour is roughly the same as that outlined in the documented information security policy".

However, by probing this group further, about the specifics of their organisation's policy, vaguer and more doubtful responses were given, such as:

"I must admit that I am only familiar with aspects of the policy that affect me directly".

Thus indicating that even among this group of individuals, who were confident about their compliance, there was uncertainty regarding the established policy of information security and how they should behave in order to comply with it.

When questioned directly about their beliefs concerning information security, all of the interviewees agreed that changing these would help hugely to increase compliance. The habit attribute, which enables people to deal with any situations that they encounter without paying attention to the environment and the consequence of the behaviour, was also identified. To this end, there was a general consensus that:

"It is important that employees learn good security habits in order to be able to reduce security breaches".

In practice, as this section has highlighted, these habits can only be changed by the changing of existing opinions among employees with regards to the importance of information security. Therefore, employee concerns about: barriers to compliance, communication, management and about information dissemination all need to be tackled.

4.5.2 Influence of Others:

Do colleagues and friends influence your behaviour toward your organisation's information security policy?

Before considering the extent to which employees are influenced by others around them, it is worth noting firstly that all of the respondents agreed that colleagues and friends, and even family, can influence a person's behaviour toward information security. To illustrate, it was accepted by one interviewee that:

"Colleagues, friends and family all have a big impact on my behaviour which is related to all aspects of my work".

Similarly, another response indicated that:

"I believe we are so much affected by others, all of the time".

Although it was acknowledged that the influence of others can be a positive one, often it can be negative, to illustrate:

“My colleagues are not helping me to change my attitude towards information security”.

Another interviewee elaborated on this point further, by stating:

“My close friends can act as barriers for me in complying with security. For example, we share passwords when the need arises and I allow other people to use my personal accounts and logins”.

The majority of the interviewees agreed that employees are affected by their colleagues and friends, and that they have a large impact on the way they behave with regards to information security. Therefore, it is critically important to raise the awareness level by acknowledging the consequence of social influencers. This was a surprising admission, but it was repeated by a handful of others, to illustrate, another interviewee indicated:

“I do not see any problem sharing my password account to only my best friend and colleagues, they also use my computer at work if that is what the job requires”.

Furthermore, it was not only in the sharing of passwords that the problem existed, many individuals admitted to doing exactly what their friends and colleagues did in regards to security compliance, even if this was obviously in conflict with the organisational policy. This was clearly explained by one interviewee as follows:

“Because me and my colleagues are best friends, we trust each other, and I think we really influence each other’s behaviour”.

As a result, these employees are obviously affected by social norms, which together influence their behaviour towards complying with the organisational information security policy. It was also admitted by many respondents that these influencers stop them from analysing their existing behaviours as it stops them from fully engaging in any changes proposed by the organisation to improve attitudes.

Finally, respondents also felt that the managers could be doing more to counteract the often negative influences from friends and colleagues, on one another. To this end, one interviewee stated that:

"We do not get from the top management consistent direction or an effective awareness procedure. This, therefore, opens the door for my colleagues and friends to influence my behaviour more than perhaps they should in matters of security".

The above responses signal the need for the top managers to be more aware in their application of some of the procedures that might help to reduce the way in which the employees influences each other, this could be managed through: consistent observation, effective reinforcement and increased awareness procedures.

4.5.3 Behavioural Intention:

What do you think you could do, yourself, to reduce information security breaches at work?

This open-ended question led to a huge variety of suggestions into what employees felt that they could do, themselves, to improve their compliance

with security. One suggestion, which was repeated by several respondents (and was discussed in more detail in the previous sub-section), referred to the influence that colleagues can have on behaviour:

"I think that if I stop been influenced by my colleagues, I can reduce information security breaches".

More specifically, this respondent then added:

"I need to think more about the implications of practices such as: sharing my password details".

A number of others also identified the existence of a high level of trust between employees as being problematic to security. To illustrate, most of the respondents agreed that there needs to be increased awareness regarding this issue, such as the introduction of an:

"Effective awareness programme that shows clearly the consequences of social influence on security breaches".

It also appears as though a minority of respondents seemed to share the notion that they all needed to take the existing guidance from management and security professionals much more seriously. However, the interviewees argued that the advice and guidance they received needed to be clearer, more frequent and more assertive in order to help them to enforce it. For instance, one respondent stated:

"I think that if management were to take the issue more seriously, then I would make more effort to reinforce the information security policy. This will definitely help to reduce security breaches".

A similar response was:

"If given encouragement and good support from managers, I would completely focus on security issues and concerns".

It appears as though this minority of interviewees were willing to change, but it is accepted that employees may need an occasional push in the right direction – be that from management, security staff or from training sessions which remind employees of the necessary behaviours.

One further suggestion that the majority of respondents pointed to was the need for awareness sessions that would actually help to enforce the reality of the security implications, within the employees' minds. One interviewee summarised this as a need for:

"Connecting the risk and the consequence of breaches to real-life everyday scenarios would be a big help."

This implies that the employees interviewed are, in general, struggling to connect the security implications with their working life; they could therefore do with a method of connecting the theory with the current working practices.

A similar point was made by the following interviewee:

"I believe I need to think more about the benefits and consequences of my behaviour towards security compliance, perhaps by attending training and awareness".

Another possible aspect, which was suggested by one interviewee, focused on the need to:

“Discuss current problems and breaches, and consider recommendations on how to avoid these in future”.

Finally, a few respondents also identified the issue of confidence, both in their own ability to react appropriately to avoid potential breaches as well as within the organisational security policy. One interviewee summarised this as:

“It would help if I started to believe more that information security is critical to the organisation and that it is easy to implement”.

Another interviewee agreed with this statement, by illustrating what they felt they needed, on a personal level, in order to start following the procedure better:

“I need to be more confident that I can personally make a difference to security, because I currently see it as being handled by others”.

This point of view suggests that any potential awareness or training sessions needs to not only help raise confidence levels in the policy, but also in the ability of the individuals as being significant in the fight against breaches.

4.5.4 Changing Behaviours:

What do you think would make you change your behaviour towards information security management at work?

The sub-section above considered the views of employees in terms of what they could themselves do to elicit a change. In contrast, this section will focus on the areas that the employers felt they could influence to elicit change and to help instil better behaviours regarding security compliance within their organisation. Once again, the open-ended nature of this question encouraged a range of suggestions, some of which will now be highlighted and explored in detail.

In general, most interviewees agreed that it was necessary for the company to take measures that would help to change employee habits. A wide range of suggestions on how this could be achieved were given, but one theme remained central among the responses – organisations need to motivate their employees better, towards compliance. One respondent clearly illustrated this point as follows:

“I need more motivation and inspiration from my organisation, and especially from my manager. This can take the form of simple vocal encouragement, or be more formal, such as having the threat of discipline hanging over people who don't listen”.

Another similar response presented a reflective view that was held by the majority of employees, in particular:

“The organisation I work for needs to increase my desire to change. They also need to praise and recognise my successes if I do manage to improve my behaviour”.

Thus, most respondents seemed to agree that a push was needed in the right direction; however, there were variations in the opinions from employees with regards to the form that this push should take.

Reinforcement, awareness and training were also identified by many employees. An example of what this should include was given by the following interviewee:

“I think a regular awareness course is needed. This should include clear consequences of security breaches. Examples of these breaches would also be helpful”.

In support of this, another response identified a similar element:

“Consistent reinforcement is needed that will help me to change my habits and my routines, in case they need to be changed”.

Another benefit of having some kind of training and awareness was pointed out by another employee, who felt that:

“It would be good to have somewhere where I can practice the skills and knowledge that I already have regarding security. This would help keep my skills relevant and it would also improve my motivation to behave appropriately”.

A final more obvious factor which was identified by the interviewees was the need for additional rewards for good behaviour, within their organisations.

One employee was quite specific about the exact form of benefits that would help:

“Promotion and recognition from the top management, such as being given extra holidays, certificate, gifts, or even an increased salary”.

In general, when pressed on the issue, it was clear that nearly all of the interviewees believed that being given some form of recognition for compliance was something that their organisation was failing to adequately do; thus, improvement in the area of recognition would most likely improve employee behaviours toward compliance.

4.5.4 Summary of Employee Views on Behavioural Factors

All of the interviewees indicated that they believed that information security is very important to them and to their company. However, the vast majority agreed that there were certain factors that were affecting their current behaviours which were stopping them from developing good habits with regards to security. Quite often, the interviewees generally believed that the cost of cautious behaviour was higher than the perceived benefits of cautious behaviour, and this was, in itself, preventing compliance. On the other hand, a minority of interviewees felt that they were currently fully complying with the policy; although when probed further they became vague and unsure of the specific elements to the policy. This identifies complacency or perhaps a lack of feedback, updates and reinforcement.

The interviewees also acknowledged that they were often influenced by others in terms of their behaviours toward security. Many accepted that this can be a negative influence, and a large number identified the fact that more could be done to reduce or remove the link between negative influence, from friends and colleagues, while simultaneously promoting positive influencers. Furthermore, the majority of interviewees felt that the senior management team could act as a perfect positive influencer by acting as role models and deterrents at the same time.

The interviewees felt that there were steps that they, themselves, were capable of taking which would help to improve their behaviour towards compliance, these steps included: consciously stopping any negative influences, around them, from affecting their behaviour; taking any advice given about security more seriously; refreshing their own knowledge through information gathering or training; and, also by improving their confidence in their knowledge and ability to make a difference. On the other hand, the interviewees felt that their organisation could also help to improve things by: sharing information in a better way; exploring the consequences that employees could make in a better way; the conduction of training and awareness; providing rewards for compliance; by providing better feedback, assistance and encouragement; and, finally by provided a setting where new skills could be practised, fine-tuned and improved upon.

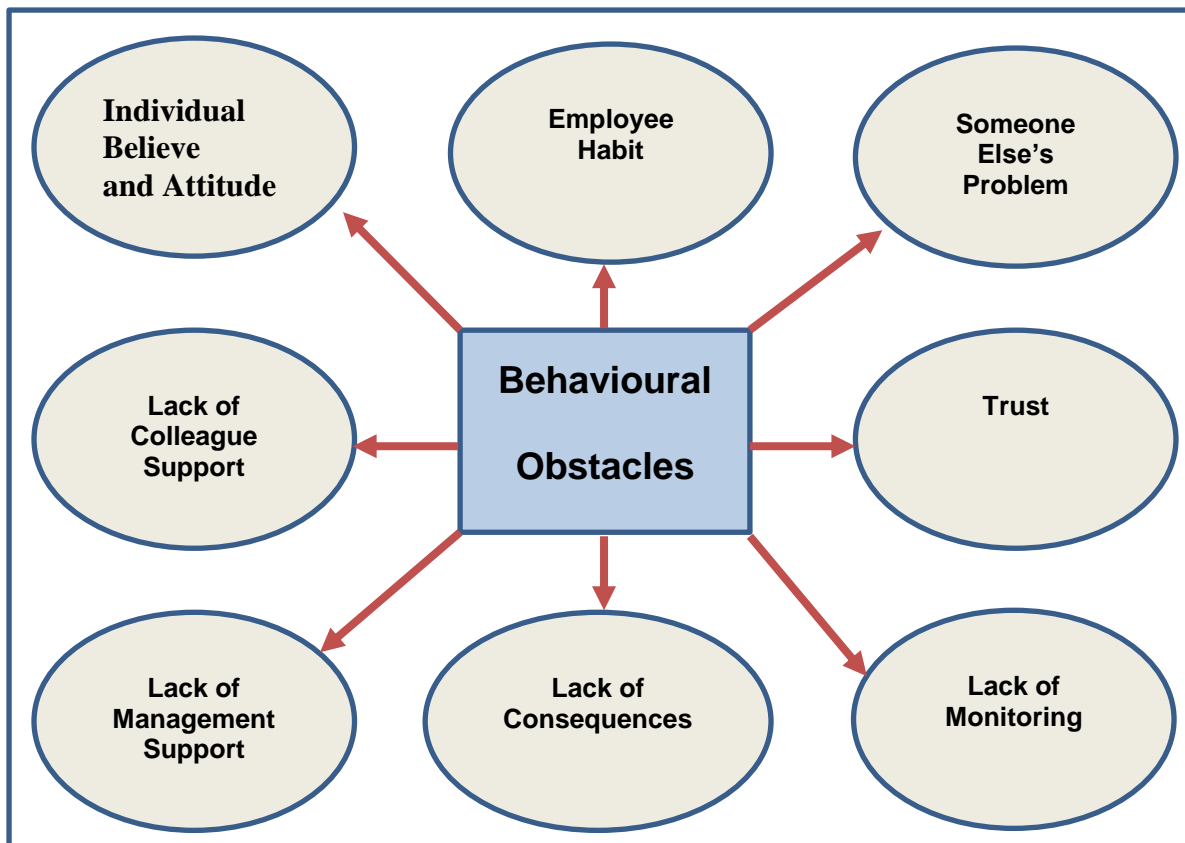


Figure 4-2: Behavioural Obstacles Affecting InfoSec

4.6 Training and Awareness Programmes to Impact on Information Security Management Behaviours

This section will investigate and identify the characteristics of effective training as a tool to help people retain security information for longer, while also working to persistently improve their performance on information security. In order to provide effective training, firstly it is essential to think broadly and deeply about how the users can contribute in order to sustain the appropriate behaviour. Secondly, it is necessary to focus on the factors that are utilised successfully in training and awareness programmes to impact on information security management behaviours. This section will

assess the existing training programmes that employees utilise in order to determine: how effective the employees find them; whether the employees feel that the programmes have helped to improve their behaviour towards security; and, also to determine whether these programmes are seen as being ultimately successful.

4.6.1 How effective do the employees think the current information security training is?

Firstly, it became apparent throughout the interviews that the majority of the respondents were not aware of their organisation offering any form of security training. A typical response to this question was:

“My organisation does not provide us with training and awareness programmes on information security, only a copy of the policy and sometimes an email reminder”.

Out of the majority of respondents, nearly all could see the need for these sessions to be provided, at least annually. A typical response, in support of this, was:

“I think we do need a regular information security training programme. I personally would benefit from that and I would be more confident about security if this programme was available”.

Of the people who had been given some form of training, or for those who were part of an organisation where training was provided regularly, the responses were overwhelmingly in favour of the need for these sessions. However, there seemed to be a consensus among this group that the training

that was being offered was not very effective at retaining the attention of the participants. To illustrate, one respondent noted:

“The information security training programme my organisation provides is boring, and therefore I don’t really learn much from it”.

Even some of the individuals that did not currently attend any of the training agreed that any potential training must be designed to focus the delegates’ attention. In support of this, one respondent, who currently had no options of attend any training, said

“I want to attend information security training but it must be interesting, otherwise I can see my time being wasted”.

Another issue that many of the current attendees of the training sessions had was that there was a lack of user involvement and user participation in the training programmes. A typical response that illustrates this viewpoint, said the following:

“I think there is not enough participation and involvement and feedback from the trainer”.

Similarly, another respondent was more specific on the type of interaction that seemed to be missing:

“I think the current information security training in my organisation has a lack of engagement and reinforcement”.

These statements illustrate the general consensus, among attendees, that in order to motivate delegates to attend and to gain benefits from the security training and awareness programmes, interaction to draw the employees' attention must be provided and encourage through engagement. As one perceptive respondent put it:

"It is essential to allow the users to participate, to present their opinions and to share their experiences as part of the learning process".

A related point that was highlighted by a number of respondents who had attended sessions noted that no assessments were carried out as a benchmark to determine pre- and post-training knowledge. This was seen as a failing by many of the interviewees:

"I think the current information security training in my organisation does not include an assessment of my information security knowledge, and this may have helped me learn better".

By including an assessment of what had been learnt, many of the respondents in this group felt that any learning from the sessions would be enforced better and the training would be more effective if it were assessed, to illustrate:

"A test at the end would ensure that I definitely paid more attention throughout".

A final theme that was recurrent in many of the responses was focused on by those that had attended various sessions, they felt that there was too much information and too many written rules in the documentation that was being

used by the trainers. It was felt that this became a barrier to effective learning within the course; one respondent acknowledged this by stating:

"I think there were so many rules and so much information thrown at us that it was difficult to keep any of that knowledge in your head".

Others felt that the information could have been relayed/delivered more effectively by the trainer; for instance, one respondent felt that:

"The trainer could have highlighted key points better".

To summarise, all of the respondents felt there was a need for training to be provided by their organisation. Of the people that had attended training sessions, there was a consensus that these programmes were not truly effective. Some of the main barriers preventing effectiveness included a lack of engagement by the trainers, a failure to keep the sessions interesting and to keep participants involved, a lack of assessment to review what had been learnt, an overload of information and a lack of effective communication by the trainer.

4.6.2 Have those that received training changed their attitudes and behaviours after receiving the training?

Most of the respondents that had attended any training agreed that the sessions had affected their behaviour in work, post-training. However, the extent to which they felt there was a change varied considerably within the group. One extreme interviewee felt that:

“The training programme completely changed my behaviour towards security... and the effect has been permanent.”

Conversely, on the opposite extreme, a different interviewee said that the training session had led to:

“A small awareness about security policy – but no direct impact on behaviour.”

Reassuringly, most of the interviewees fell somewhere in between these extreme views; a typical interviewee response was as follows:

“My attitudes and behaviours were affected after the training. I think I consider information security policy much more after the training than before it.”

A very common view, held by the vast majority of the individuals who had attended the training, was that their attitudes and behaviours had changed, but only for a short period following the training. For instance, one respondent said:

“I think the training increased my motivation to follow the rules and regulations of the information security policy for a while. After that, if I’m honest, I returned to my old ways of thinking.”

Likewise, a similar response noted:

“I think the information security training improved my knowledge at the time, but I think I have forgotten most of what I learnt now.”

A final element with regards to training that needs to be considered is from the point of view that the behaviours and attitudes of most of the participants were not changed for long enough to influence their long-term habits:

“My behaviour changed and improved, but then I returned to my old habits regarding information security.”

A number of explanations were provided by the respondents with regards to why they thought that the changes in their behaviours and attitudes had been only short lived. One important view, shared by a few, was that their motivation was not affected or permanently changed as a result of the course. A typical response highlighting this was:

“I was not inspired enough during the course to become changed by it. Afterwards, there were no rewards or sanctions in place, so I didn’t change for very long.”

Another important reason cited by a number of respondents was that no reinforcements were utilised in the period that followed the training. One such response which alluded to this issue included:

“I was not able to practice or maintain the skills and knowledge that I picked up, so I ended up losing the knowledge eventually. Some regular reminders may have helped.”

Finally, many respondents pointed to the methods employed during the training as the reason for it not having a lasting effect on behaviours and attitudes. One particularly astute respondent summarised this view the best:

“I didn’t think that training was delivered in the best way to make knowledge stick. There was too much information and a lack of simplicity. There was also a lack of visual-aides, descriptive images, group discussions and real-life examples.”

All in all, the interviewee responses indicate that training can indeed influence attitudes and behaviours in employees. However, these should be backed up with strong reinforcements, regular assessments and reminders, rewards and sanctions. Moreover, in order for the training to have a lasting effect, care needs to be taken in terms of the content and delivery method of the training itself; the training should be interactive, clear, succinct and it should involve tools such as group discussions and visual-aides in order to maximise its effect.

4.6.3 If you help to devise or deliver training, how successful do you think it has been, and how do you think it can be improved?

Most of the individuals who offered their views in this section were either members of the training team that helped to implement or deliver the training sessions, or they were members of the management team responsible for sanctioning and overseeing the training sessions. Unsurprisingly, most of these individuals felt that their training sessions were highly effective. For instance, one manager said:

“I think the training we provide does a great job in changing employee attitudes toward information security”.

Another trainer added:

“Yes, I think we had less security breaches after conducting the information security training”.

This was fairly typical of the view held by this group which included the board, trainers and managers alike. Despite their overwhelming positivity, when pressed, the managers and trainers offered valuable insights into how they thought the training within their respective organisations could be improved. One simple method was via:

“The provision of more regular training instead of the current voluntary training, which is given every few years”.

Another suggestion can be related to the manner in which the training was put together:

“It needs to be more organised and better planned. It is currently too informal and it lacks structure”.

A further suggestion links closely some of the elements identified by participants themselves, in the preceding section:

“I think there needs to be an assessment within the training course, to encourage employees to pay more attention than they possibly do now”.

Finally, one respondent acknowledged the need for the training to be provided in a more professional manner:

“I think we would get better success if we had an external and professional trainer, instead of someone from the IT department”.

A couple of training providers, in their responses, raised an interesting suggestion for the development stage of the training programmes. They noted that it is important to take into consideration the different learning styles of adults in order to cater for all learners. To illustrate, one trainer noted:

“By doing a survey about learning styles at the start of the course, participants can then be split into different groups, depending on their learning style. The training can then be group-specific. Some people respond better to videos, some to role-play, some to discussions, and some to straight-forward classroom learning”.

This was an interesting suggestion and it seems reasonable, as a minimum, to incorporate as many of these tools as possible in any training session that may be devised to cover all learning styles, even if the survey itself is not conducted.

Finally, a group of managers and trainers acknowledged the concept of empowering participants, so that they personally feel more responsible for their company’s information security. To explain this further, one manager said:

“In my opinion employees need to become more self-sufficient at learning about policy. If we could give them the tools to and knowledge about where to find information, and then if we offered rewards for them doing so, then this would be the best form of training”.

This form of self-sufficiency could take the form of employees being given objectives at the start of the training and then, through the use of various resources, the objectives would be fulfilled; in this way:

“Self-learning allows employees and the end-users to be satisfied with their work, as it motivates them to make an extra effort in training”.

To recap, most of the training providers felt that the training that they provided was a success as they felt that it effectively encouraged more compliance among staff. However, they made a number of interesting suggestions about how this type of training could be improved. This included the need for more regular and professionally led sessions, more empowerment to the participants, more learning-style specific training, as well as the programmes being better structured and assessment-based. All of these elements appear to be of importance and they should be incorporated within any training that will be ultimately devised as part of this study.

4.7 Summary of the Criteria to Address When Devising Training

This final section in this chapter will explore further some of the lessons learnt from the preceding qualitative data analyses. In particular, this section will focus on the specific criteria that must be addressed in order to successfully devise a training programme for employees that will cater for their needs, concerns and behaviours. In order to do this, five main broad themes, that have presented themselves throughout this chapter, will now be

considered separately, including: motivation, awareness, communication, reinforcement and training methods.

4.7.1 Motivation

Throughout this chapter, motivation has been mentioned on various occasions as being central in helping to ensure that security policy is fully complied with. Therefore, in order to have a successful training and awareness programme, it is crucial that all of the participants feel motivated by what they see and hear. Furthermore, it is important that their motivation to comply remains maximised once they return to their workplaces.

Throughout this chapter, a number of suggestions have been made regarding how motivation can be passed on to employees, both within a training session and beyond it. The most important and relevant elements have been collated below, they include, but are not limited to:

- Providing rewards for attending sessions and for complying with policy.
- Punishing those that do not attend and who consistently fail to comply.
- Helping employees understand the practical and financial impact of non-compliance.
- Encouraging employees to believe that they can make a difference.
- Empowering individuals, so they feel they are responsible for their own behaviours and for their own compliance to security, by also exhibiting trust in their abilities.

- Setting attainable objectives that employees can work towards.
- Helping employees believe in their capacity to change.
- Providing regular and positive feedback on compliance behaviours.

4.7.2 Awareness

Awareness encompasses a number of facets which relate to information security compliance. The importance of awareness has been highlighted throughout this chapter as a recurring factor mentioned throughout the interviews which were conducted for this research. In order to ensure that all participants have their awareness increased about security implications, it would be imperative to include the following suggestions within any strategy:

- Make clear the implications of non-compliance.
- Make the policy clear and widely-accessible to all.
- Give regular updates of any breaches, of what caused them and on how these can be prevented in the future.
- Any updates or changes to policy should be made clear (through communication or training) to all employees.
- Help to provide an understanding of how best to behave, given hypothetical situations, in order to minimise the risk of security breaches.

4.7.3 Communication

Over the course of the interviews, communication, in its various forms, was continuously cited as being central to effectively instilling security

compliance. In order to optimise the effectiveness of any training session and security policy, it is necessary to incorporate the following list of suggestions that were made over the course of the interviews:

- Communication between trainer and participants should be clear and two-way.
- Regular and positive feedback should be given regarding practices and behaviours of compliance.
- Regular communications regarding policy, and in particular on updates to policy, via emails, intranet, phone conferences, as well as appropriate and regular refresher training.
- Knowledge sharing within the training sessions, and beyond, via the use of forums, meetings and distribution lists.

4.7.4 Reinforcement

Another category that was regularly cited in interviews, which is slightly broader, concerns the need for constant reinforcement both during the training sessions and beyond it, in the months and years that follow. A number of suggestions were made about how best to achieve this:

- Regular reminders of what was learnt during training through communications and refresher training sessions.
- More engagement and hands-on practice during the training sessions.
- Holding assessments at the end of training, in order to ensure that all who take part leave the course with adequate knowledge.

- Holding periodic and regular assessments of knowledge which relates to security, in order to ensure that the knowledge remains fresh and up-to-date.
- Holding quizzes and contests, with prizes for winners, to help reinforce knowledge.
- Allowing familiarity to be built around the policy, through the regular practice of compliance.

4.7.5 Training Methods

As the final part of this summary of qualitative findings within this fourth chapter, it would be useful to collate all of the direct suggestions regarding the training method itself, as employment of the most flexible and appropriate training method would help to make the security training as effective as possible. Although it may be impractical to include all of the following suggestions within any one training session, it would be wise to incorporate as many as possible, or at least to devise a training framework that utilises the main suggestions below:

- Ensuring that there is not an overload of information within the training session.
- Simple, non-technical language needs to be used by any trainers.
- More visualisation, videos and descriptive imagery should be used in the training.
- The use of group discussions, role-plays and scenario creations within the training sessions.

- The performance of a survey of learning styles of the trainee group, so that the training could be tailored to cater for the majority of the trainees.
- Encouraging involvement, participation and discussion among the participants.
- Setting clear learning objectives at the start of the session and working towards these.
- Emphasis to be placed on convincing, rather than top-down persuasion.
- Utilising a mixture of training methods, including brainstorming and role-play in order to keep all participants and learning styles engaged.

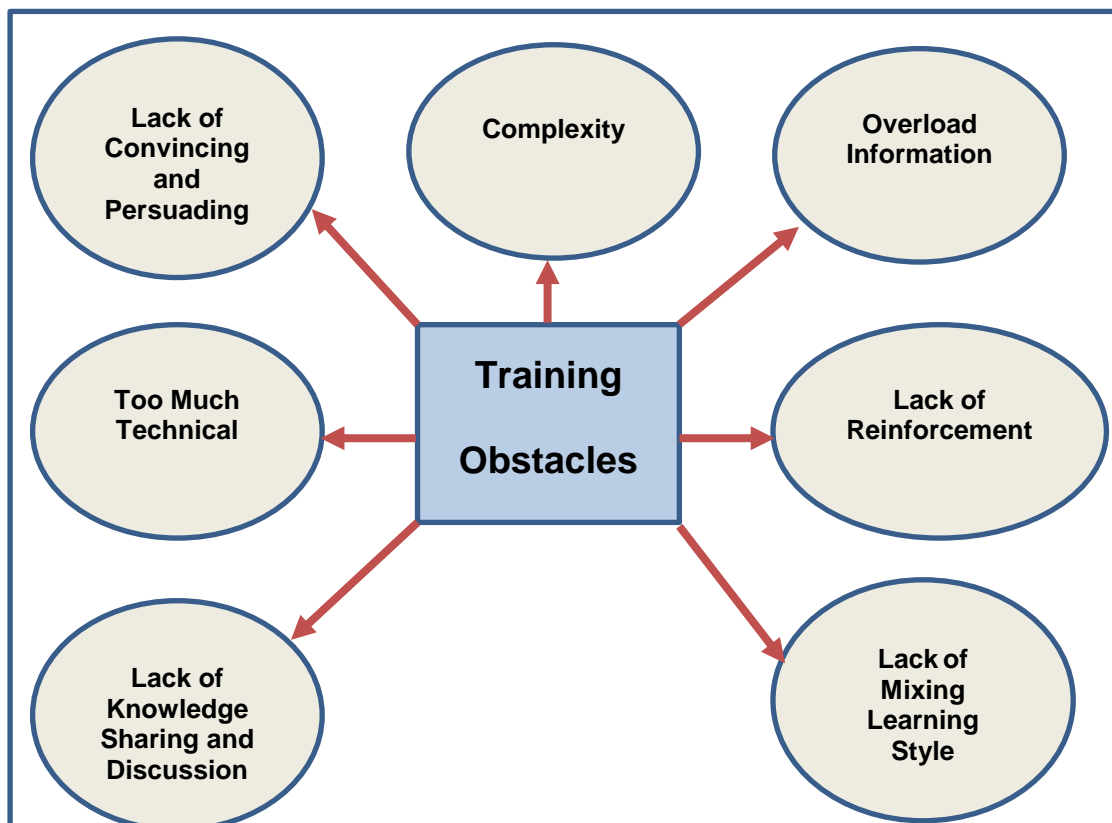


Figure 4-3: Training Obstacles Affecting InfoSec

4.8 Conclusion

As mentioned previously, the world of information technology is constantly developing and evolving; hence, developments in the different technological types has fuelled the requirement for improvements in security management to reduce and mitigate security breaches. In order to help devise the most effective information security, this chapter has presented and analysed the qualitative data collected from the employee interviews. The findings have been dissected based on the organisational factors and deficiencies that have led to non-compliance, along with human behavioural factors and, finally, the effect of the current training and awareness sessions on employees. Consequently, a summary of major findings was present in the previous section (section 4.7 and its respective sub-sections). It is imperative to consider these factors when devising the specific format of the training session. Finally, it is important to note that the next chapter will build on the foundations set out in this chapter by reviewing the quantitative data from the questionnaires.

Chapter 5: Quantitative Data Analysis

5.1 Introduction

This chapter is entirely dedicated to the quantitative analysis utilised in this research. The chapter will be divided into various sections and sub-sections in order to provide a description of the tools and techniques used as well as an analysis for the various factors studied. The use of the quantitative data analysis method allows the researcher to use different figures as well as statistical methods for the purpose of analysing the results obtained for the research problem identified.

The development of a questionnaire was necessary for this research, as this instrument would contribute toward completing the goals of the study. The questionnaire was to be one of the main tools for gathering data in this research. The questionnaire consisted of clear and concise instructions for five separate sections which included: part one which obtained very brief demographic backgrounds about the responders, this would help the researcher to, at a later stage, categorise the results; part two assessed the users level of information security awareness; part three assessed the employees evaluation of the information security policies at their organisation; part four focused on understanding the different factors that influence user behaviour towards information security; and, finally, part five assessed how the training and awareness programmes were evaluated to determine their impact on information security management behaviours.

5.2 Quantitative Research Methods

As a result of the nature of the research problem, the researcher decided to use the quantitative approach for the following reasons. Firstly, the use of a quantitative approach allows for a good fit between the social reality of the research participants and the theories presented. Secondly, it allows for the studying of the cause of employee behaviour and the effect of different factors and relationships. Thirdly, the quantitative approach allows the study to identify the common factors that can then be compared to the various actions that are taken towards security. As Nettleton and Taylor (1990) identified, the aim of the quantitative method is to provide accurate measurements for social actions, by explaining the causal relationships that relate to specific events. Unfortunately, this approach is not without its disadvantages; as such, the quantitative approach utilises sometimes awkward and formal language, and generalisations are made which lead to predictions, explanations and understanding – however, these generalisations can become over-generalised. Furthermore, as the samples that are used are often large to allow for a representative sample, this type of research is often very time consuming (Creswell, 1994, p. 4-9).

5.2.1 Questionnaire Design

Questionnaires provide a relatively inexpensive way of gathering data from a potentially large number of respondents. Questionnaire design is one of the most common tools which allows the researcher to look more critically at peoples' understanding of a specified issue. The design of the questionnaire is an important aspect of the success of the research. For the purpose of

this research and context, it was chosen that this questionnaire would use various closed questions which would be based on the Likert scale. The use of closed questions in the questionnaire allows the researcher to collect more focused and useful information, which helps conclusions to be drawn about the related research and works. It therefore appears as though a questionnaire, using closed questions, and which is designed on the basis of requirements of the Likert scale, would be the most suitable for the context of this research (Rubin and Babbie 2009).

5.2.2 Pilot Test

Pilot tests are a crucial and intensive requirement of such a large sized project. According to De Vaus (1996), it is wise to assess the reliability and validity of indicators before conducting the actual survey with the whole sample. The pilot test was conducted with a small sample of 10 people that were randomly selected; these participants included a mix of men and women that were between 25 and 40 years of age. These people were selected because they worked in different organisational sectors, as it was believed that this would help to provide a diverse range of information from their different experiences. The findings from the pilot test would allow the researcher to identify the strengths and weaknesses of the survey procedure that was to be used in the research.

After obtaining the participants' feedback, the overall response was that the questionnaire was straightforward and easy to complete. However, there were suggestions for change with regards to the order of some of the

questions, as it was felt that this would help the questionnaire to flow better; furthermore, it was suggested that some participants felt that the questionnaire was too long. Changes were implemented to make the questionnaire flow better and some questions were also removed which were a little repetitive to make the questionnaire a little shorter.

5.3 Participating Organisations

5.3.1 Organisation (A)

Organisation (A) represents one of the healthcare institutions in the United Kingdom, it is a public enterprise. The organisation has approximately one hundred staff of which there were both male and female employees and some of which were consultants. This organisation aims to provide medical services and healthcare that is of a highly specialised level, their mission is to seek healthy and satisfied patients.

This organisation follows the formal policies and standard procedures of ISO 27001, which aims to incorporate information technology into everyday working practices. The use of regular training is considered to be part of their strategic plan to improve employee management and to enhance the organisation's ability to achieve high levels of implementation of the organisation's information security policy. The organisation enforces their policy through practical processes and by taking appropriate action against those who fail to comply with the policies. This organisation has also

adopted information security within its main mission and organisational strategy.

Organisation (A) aims to provide its employees with a documented policy that has been designed to provide a framework of control for the security of the information and systems used within their general practice. The managers ensure that equality, feedback with encouragement, motivation, as well as the sharing of knowledge, solutions and trust are encouraged throughout the organisation. Effective security measures have helped to protect against the risk of certain events occurring, by reducing the impact of such risks. Finally, the training requirements within this organisation are reviewed regularly in order to ensure continued awareness and compliance with future system developments and good security practices.

5.3.2 Organisation (B)

Organisation (B) is one of the education institutions in the United Kingdom. It has a comprehensive set of policies, procedures and aims which provide guidance for all staff involved in policy development. Organisation (B) aims to produce effective and independent learning through practise that is innovative, high quality, relevant, flexible, achievable, efficient, engaging and teaching.

Organisation (B) has a vision for their security policy which provides clear guidelines and advice to enable staff to realise their professional roles and responsibilities towards the policy, through the encouragement for the

dissemination and sharing of good practice of security policy implementation. Their policy supports and enhances electronic communication which includes the provision of feedback and documentation of the policy. This organisation provides its staff with complete support for any IT security incident or event that might occur, such as: viruses, password problems, backups and any other IT service. In order to ensure reinforcement, supporting policies have been developed to strengthen the reinforcement of their policy statements.

5.3.3 Organisation (C)

Organisation (C) is considered to be one of the leading consumer goods companies in the UK. This organisation follows formal policies and standard procedures of ISO 27001 which aim to provide clear requirements and tasks that allow appropriate knowledge and skills of the security policy to be transferred; this ensures that all of the policies, processes and procedures reflect this company's commitments.

Organisation (C) has a security policy vision which allows its staff to develop and use good practice with regards to their security policies. They provide a competitive package which rewards employees for what they do; furthermore, they also receive discounts on any goods they would like to purchase. Awareness materials about information security are available electronically and it is the employees' responsibility to ensure that they are aware of: the security risks and their responsibilities to minimise the threats; ensuring that no breaches of information security result from their actions, as this is their role and responsibility; the risks that disrupt day-to-day business,

so that they may be reduced through informing staff about the contingency procedures, backup actions and safekeeping of records; and, to ensure that employees are not only aware of but also report any viruses detected/suspected on their machines, immediately to the computing services department.

5.4 Questionnaire Analysis

5.4.1 Statistical Techniques

The Statistical Package for the Social Sciences (SPSS) is considered to be one of the most intensive and preferred statistical techniques that researchers can use to resolve and analyse complex research problems. The SPSS can provide analyses for the research by enhancing the validity of the results which makes it an extremely practical tool for analysing research data (Foster, 2001).

There are a number of different advantages which drive researchers to use the SPSS techniques for their analysis. For instance, the SPSS is a self-competent computer program which provides statistical analysis of complex data. The user needs only to insert the data into the program which can then produce accurate as well as reliable outcomes for the research. Furthermore, the program also organises the results from the research into a clear and organised format which significantly reduces the amount of valuable time that is needed to be employed by the researcher to accomplish the task; therefore, it is an extremely effective and efficient tool for complex

analyses (Bryman and Cramer, 200). These statistical analyses allow the researcher to achieve reliable and valid results from their researched work.

5.4.2 Data Analysis

A total of 400 survey questionnaires were completed, however only 360 were usable. A summary of the data analysis will now be provided which will include a brief description about the demographic factors which correspond to the participants included in this study. This will be further divided into sub-sections to analyse the participants' age, gender, education level and industry that they are from. The responses obtained from the questionnaires will now be presented using figures and an analysis of the various findings.

5.4.2.1 *Response by Industry*

Based on the analysis of the responses from the surveyed participants, as shown in Figure 5-1, from the 360 participants included in this survey it was found that they came from one of three sectors. To illustrate: 33% of them were working in the business sector, 47% of the participants were working in the education sector and the remaining 20% were working in the health sector.

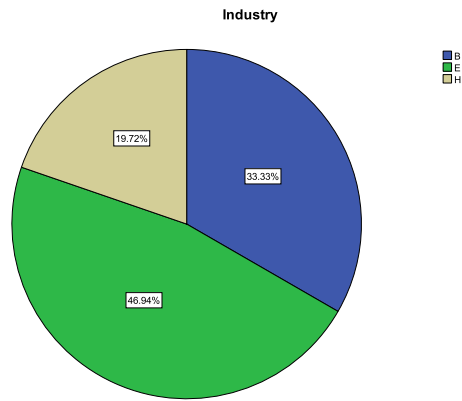


Figure 5-1: Response by Industry

5.4.2.2 Response by Gender

On the basis of the analysis of all 360 surveys, it can be revealed that the split of participants by gender was quite equal (see Figure 5-2); but, the majority of respondents included within the survey were male which represented 52.5% of the sample and the remaining 47.5% were female.

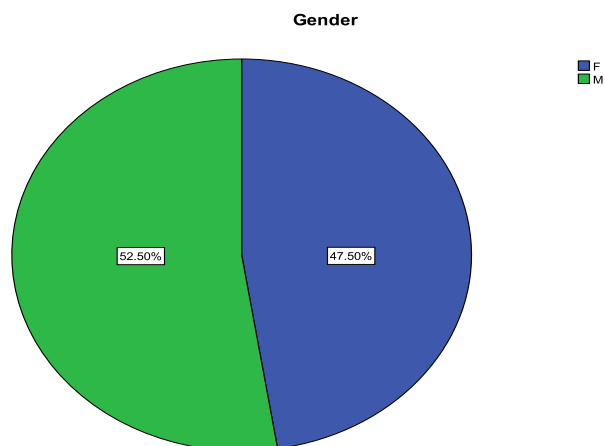


Figure 5-2: Response by Gender

5.4.2.3 Response by Level of Education

It can be seen from Figure 5-3 that the majority of respondents were educated to at least graduate level with 47.78% being BSc graduates, 34.17% of the respondents held an MSc level of education and 9.17% of respondents had a PhD; in contrast, only 8.89% of the participants – the smallest group – had a GCSE level of education.

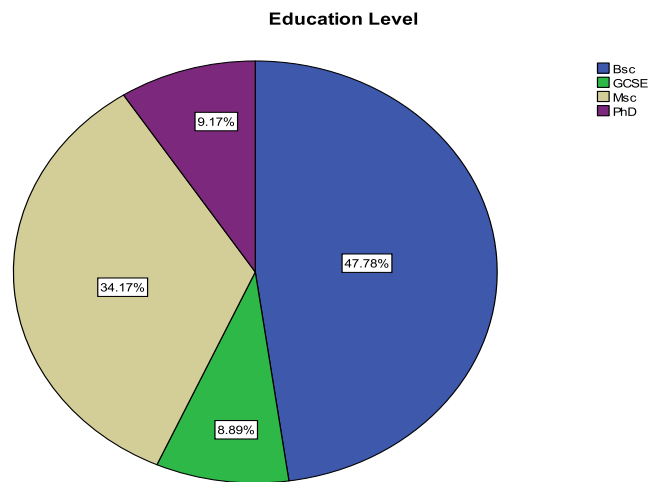


Figure 5-3: Response by Level of Education

5.4.2.4 Response by Age

On the basis of Figure 5-4, it can be acknowledged that the majority of respondents, 48.33%, were aged between 35 and 54. At the second level, 40.83% of the participants were aged between 25 and 34. About 9.17% of the respondents were aged between 19 and 24 and the remaining 1.67% of participants were from the age group of more than 55 years.

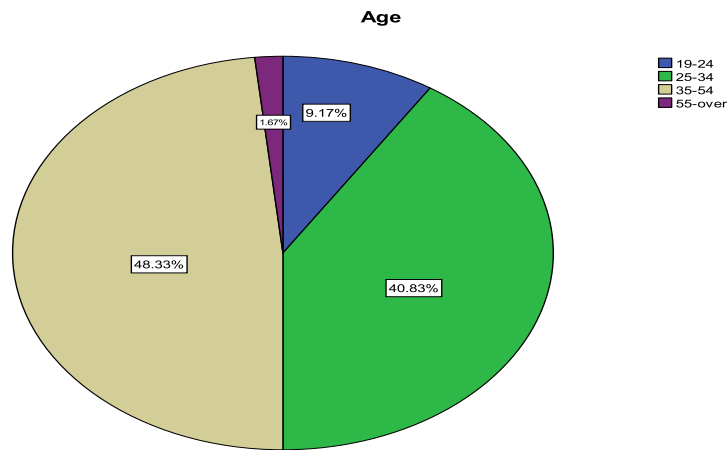


Figure 5-4: Response by Age

5.4.3 Habits of Employees

This sub-section will be divided into a number of further sub-sections in order to provide a description of the analysis of the survey responses in terms of the habits displayed by the employees/participants while working at the various organisations, of the three considered industrial sectors.

5.4.3.1 Receiving Training

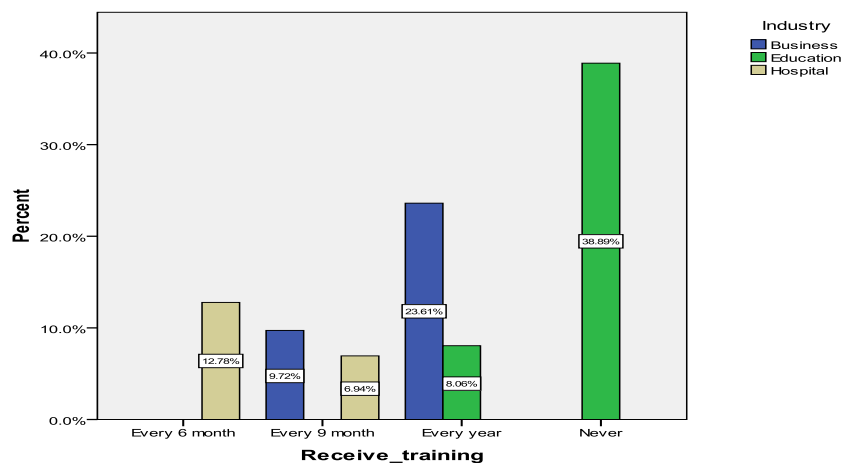


Figure 5-5: Receiving Training

The figure above (Figure 5-5) shows the frequency of training provided to the employees in the different sectors. The figure shows that in the business sector, around 9% of the respondents indicated that they received training every nine months; in contrast, most of respondents, 23.6%, said that they received training once per year. For the education sector, the scenario is quite different, as most of the respondents, 38.9%, said that they never received training regarding security habits. In addition, 8.1% of the participants noted that they received training on an annual basis. For the health sector, 12.8% of the participants noted that they received regular training, every six months; while, 6.9% of the respondents revealed that they received training every nine months.

5.4.3.2 *The Sharing of Passwords*

Figure 5-6 shows the tendency that people have to share their password. In the business sector the majority of respondents, 21.2%, agreed that they shared their passwords and about 13.8% respondents felt that they were neutral about this notion. As such, there were no respondents from the business sector that indicated that they did not share their passwords. In the education sector, similar results were obtained with 21.9% of respondents agreeing that they shared this information and only 5.4% of the participants indicated a neutral response on this perspective. In addition, about 20.9% of the respondents from the education sector strongly disagreed that they shared this information, noticeable 0.3% of the respondents actually strongly agreed with this notion. In terms of the health industry, 1.4% of the

respondents agreed and 16.9% of the participants strongly disagreed that they shared their passwords.

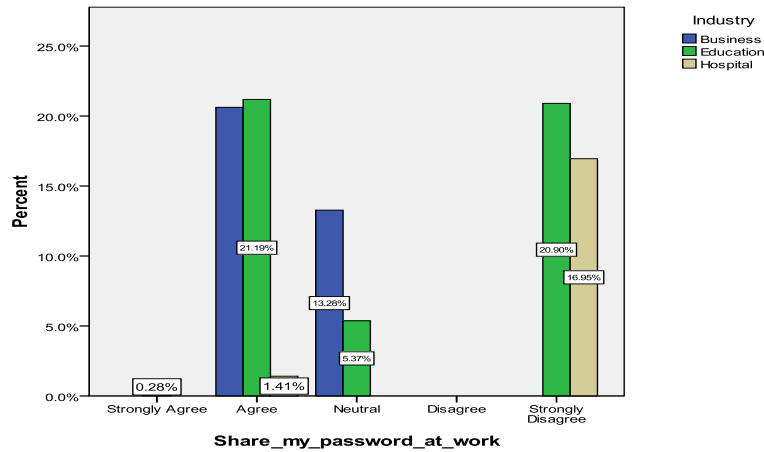


Figure 5-6: Sharing My Password at Work

5.4.3.3 Following Information Security policy at Work

Figure 5-7 illustrates the habits that people from the different sectors had with regards to following their organisation's information security policy (ISP), on a regular basis. In this context, the figure clearly shows a negative response in tendency from the participants. To illustrate, the majority of respondents from the different business industries indicated that they didn't follow the policy (i.e. 15.3% from the business sector, 20% from the education sector and 8.3% from the health sector); in contrast, a nominal number strongly felt that they didn't follow the policy (i.e. 13.6% from the business sector and 13.9% from the education sector). A small number of respondents agreed that they did follow the policy, on a regular basis, but they were few in number (i.e. 3.3% from the business sector, 10.6% from the education sector and 0.3% from the health sector).

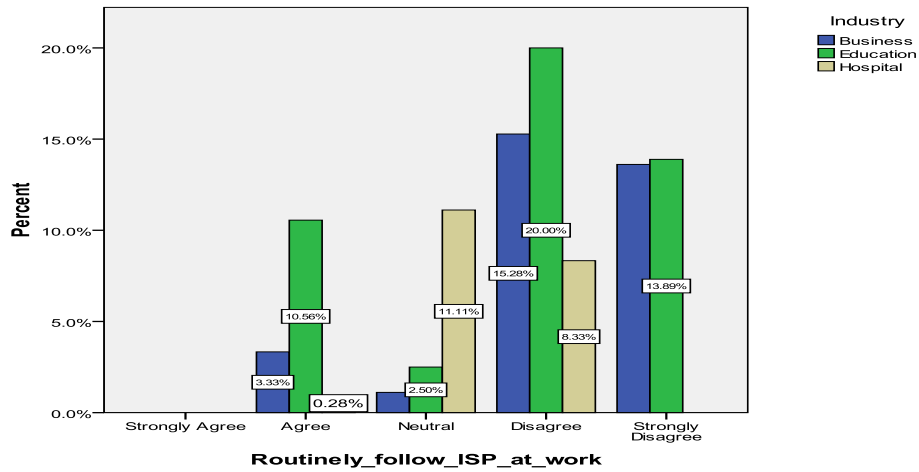


Figure 5-7: Routinely Follow ISP at Work

5.4.3.4 Following Risk Management at Work

Figure 5-8 shows the attitudes from the participants with regards to the following of information security risk management practices. As per the graphical presentation, most of the respondents from the business and education sectors (i.e. 16.7% from the business and 25.8% from the education sector) did not follow, on a routine basis, the information security risk management framework. Furthermore, 11.9% of the respondents from the business sector and 17.8% from the education sector strongly disagreed on this account. In the health industry, the scenario was very different, as 5.8% of the participants agreed that they followed it and the remaining 13.9% were quite neutral on this account.

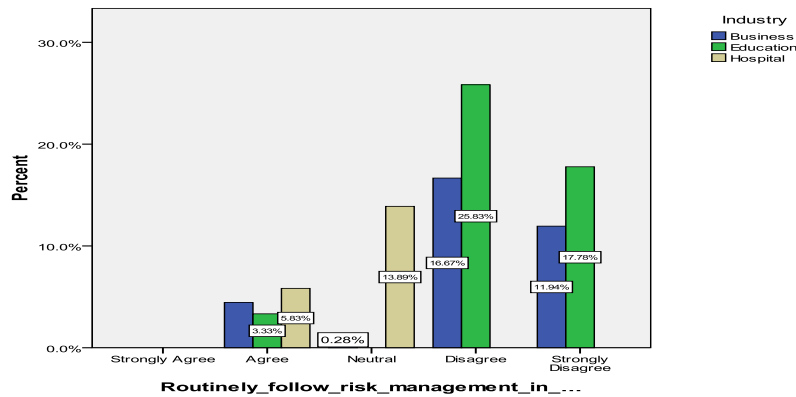


Figure 5-8: Routinely Follow Risk Management

5.5 Barrier and Effective Factors

In order to analyse the survey responses in relation to the individual sectors, a frequency measure needs to be taken into account, this is helpful as it identifies various obstacles, in terms of the organisational, behavioural and training factors that affect the application of information security policy within business organisations. Frequency is considered in terms of it being an agreeable status by the respondents, with respect to their queries. High frequency depicts effective factors and low frequency depicts barrier factors, within the corresponding sectors.

5.5.1 The Health Sector

As can be seen in Table 5-1, below, the influence of the organisational factors on the implementation of information security policy within the health sector are highlighted.

Table 5-1: Organisational Factors on the Health Sector

Variable	Frequency
Communication	69
Risk management	71
Rewards and punishment	68
Roles and responsibilities	46
Incident reporting	15
Motivation	71
Recovery	10
Awareness	41
Feedback	69
Sanctions	9
Satisfaction	47
Regular training	53
Reinforcement	50
Regular assessment	65
Good security habits	45
Attitudes	50

It can be concluded from this table that the majority of the participants considered organisational factors to be important when trying to align their processes with the implementation of information security policy. The key barriers that were found in the health sector appeared to relate to the incident reporting and the recovery of procedures and sanction, which need to be improved significantly. Despite this, the most effective organisational factors that appeared to contribute towards the growth of the health sector, in terms of compliance to the information security policy, were communication, rewards, awareness, motivation, feedback, regular training, reinforcements, and assessments. These participants appeared to have good attitudes because of the strength of the integrated policies within the health sector. These aspects therefore appear to be much stronger when compared to the business and education sectors.

5.5.2 Business and Education Sector

The table below (Table 5-2) summarises the influence of organisational factors on the implementation of information security policies within the business and education sectors.

Table 5-2: Organisational Factors on the Business and Education Sectors

Variable	Frequency (Education)	Frequency (Business)
Communication	145	119
Risk management	40	65
Rewards	157	117
Roles and Responsibilities	14	8
Incident reporting	7	13
Motivation	152	106
Recovery	17	10
Awareness	24	9
Feedback	93	64
Sanctions	5	9
Satisfaction	29	13
Regular training	20	5
Reinforcement	12	24
Regular assessment	3	12
Good security habits	20	35
Attitudes	36	17

On the basis of the above table, it has been identified that the business and education sectors do not have good security habits; furthermore, there is an ineffective alignment of employee behaviours towards compliance with the information security policy's norms and regulations. It can also be observed that the key organisational factors which can be considered as barriers to the implementation of information security policy, include: a lack of commitment to hold roles and responsibilities, a lack of incident reporting, a lack of recovery, a lack of sanctions and a lack of awareness and regular training. These factors act as barriers towards the creation of a positive drive toward

the implementation and following of information security policy within the business and education sectors. These behavioural and training factors are having a direct and negative influence on the security habits because a lack of behavioural awareness is leading to the creation of a gap between employee perceptions and organisational policies. It is therefore essential that emphasis is placed on the utilisation of good security habits, as currently the frequency of its use is very low. Despite this, communication, motivation, rewards and feedback appear to be the most effective factors contributing toward the appropriate application of information security policy.

Finally, it can be inferred that the health sector is doing well in terms of the majority of factors influencing security (including: communication, risk management, attitudes, behaviour, rewards, motivation and regular training); in contrast, the business and education sectors are lacking in some of these areas, as such significant barriers have been created which need to be not only identified but also dealt with effectively. In particular, there are apparent shortfalls in terms of the roles and responsibilities, awareness, appropriate behaviours, rewards, motivation as well as an indication that there is too little regular training being provided. Furthermore, even when the training is provided it appears to be lacking in terms of assessment and reinforcement within the business and education sector. Essentially, all of these shortfalls need to be improved significantly as comparatively the health sector appears to be performing much better in these areas. In spite of this, all three sectors appear to be lacking in terms of the following areas: sanctions, incident reporting, recovery mechanisms and a lack of good security habits, all of

which need to be improved in order to properly align the security norms within the respective policies. Therefore, there is a need for new, stimulating and constructive policies to be implemented if security habits are to be adopted and improved across all of the three sectors.

5.5.3 Statistical Analysis

The results obtained from the survey are summarised in Table 5-3, below, which details the application results of the Kruskal-Wallis test. This test helps to compare the importance of the various organisational factors for encouraging employees to comply with the information security policy.

In total 360 survey responses were fully completed and therefore only the data from these questionnaires was considered for the analysis. In terms of the three sectors, there were 120 business participants, 169 education participants and 71 health sector participants, respectively.

As a result of the chi-squared statistical analysis, which was obtained from the corresponding organisational factors of risk management, incident reporting, recovery and sanction, all of these factors were deemed to be not significant at a 5% level of significance because the p-value for these factors was higher than would be accepted as a significant level.

Table 5-3: Organisational Factors for Encouraging Employees to Comply with Information Security

Variable	Sector	Mean Ranks	Kruskal-Wallis Test (Chi-Squared Statistic)	Significance Probability
Communication	Health	166.45	36.632	0.000
	Business	147.92		
	Education	209.54		
Risk Management	Health	75.65	144.327	0.194
	Business	159.60		
	Education	239.39		
Reward	Health	166.37	3.276	0.000
	Business	178.59		
	Education	187.79		
Role and responsibility	Health	68.02	120.678	0.000
	Business	219.62		
	Education	199.98		
Incident Reporting	Health	72.87	117.022	0.154
	Business	183.18		
	Education	223.81		
Motivation	Health	168.52	4.465	0.000
	Business	173.75		
	Education	190.33		
Recovery	Health	69.04	135.104	0.147
	Business	174.71		
	Education	231.44		
Awareness	Health	79.68	99.675	0.000
	Business	206.39		
	Education	204.47		
Feedback	Health	107.68	53.042	0.000
	Business	201.01		
	Education	196.53		
Sanctions	Health	178.01	11.309	0.004
	Business	160.03		
	Education	196.08		
Believe	Health	149.65	11.737	0.000
	Business	195.18		
	Education	183.04		
Attitude	Health	61.54	138.687	0.000
	Business	207.28		
	Education	211.46		
Intention	Health	76.74	101.565	0.000

On the basis of the analysis shown in the above table, which summarises the chi-squared statistics which were obtained from the Kruskal-Wallis test, it was identified that the most effective organisational factors that should be considered as influencing information security policy, across the three sectors, are: awareness, communication, feedback mechanism and

efficiency in managing the roles and responsibilities and behavioural factors. From the table, it is possible to analyse the mean ranks that were obtained from the test, these indicate that the health sector is managing their information security policy much more effectively than the business and education sectors.

All three of the sectors had information security policies; however, it can be concluded, from the above summarised statistical output, that the following behavioural factors, namely: beliefs, attitudes, intentions and the behaviour of employees towards the information security policy, appear to hold a great significance. It is therefore important that all of these factors are considered by the organisations as they could all help to initiate improvement in the policy frameworks with regards to a reduction in security breaches.

5.5.4 Training and Awareness Programme Factors

It can be analysed from the summarised statistical output, presented below in Table 5-4, that the listed training factors are significant. All of these factors are important and should be considered by organisations which are aiming to initiate improvements in their policies and framework with regards to improving information security management through training.

Table 5-4: Training and Awareness Programme Factors

Variable	Sector	Mean Ranks	Kruskal-Wallis Test (Chi-Squared Statistic)	Significance Probability
Awareness	Health	43.68	201.268	0.000
	Business	177.71		
	Education	239.96		
Communication	Health	102.83	63.619	0.000
	Business	219.88		
	Education	185.17		
Motivation	Health	134.00	21.090	0.000
	Business	190.50		
	Education	192.94		
Reinforcement	Health	131.98	49.540	0.000
	Business	225.90		
	Education	168.65		
Satisfaction	Health	96.99	70.972	0.000
	Business	197.10		
	Education	203.80		
Assessment	Health	33.50	156.928	0.000
	Business	168.57		
	Education	218.69		

5.5.5 Correlation Analysis

In order to analyse the significance of the organisational, behavioural and training factors, with respect to the successful compliance of the security policy, it is essential that the strength of the relationship among the considered factors is evaluated. Table 5-5, below, contains Pearson correlation coefficient results which indicate the most effective factors that appear to influence the implementation of security policies in organisations. To illustrate, there appears to be a significant correlation between various factors and the successful compliance of information security policies.

Table 5-5: Correlation Analysis

Variable	Correlation coefficient (Health)	Correlation coefficient (Business)	Correlation coefficient (Education)
Incident reporting	0.562	0.312	0.312
Attitudes	0.749	0.775	0.735
Sanctions	0.321	0.474	0.322
Feedback	0.746	0.767	0.767
Intention	0.995	0.759	0.736
Recovery	0.341	0.441	0.231
Belief	0.787	0.783	0.775
Rewards	0.747	0.776	0.773
Risk management	0.476	0.376	0.306
Roles and responsibilities	0.713	0.716	0.612
Assessments	0.732	0.887	0.887
Communication	0.945	0.994	0.916
Regular training	0.747	0.769	0.734
Motivation	0.890	0.731	0.753
Good security habits	0.746	0.743	0.714
Awareness	0.863	0.981	0.934
Reinforcement	0.735	0.812	0.819
Satisfaction	0.733	0.771	0.763

Significant at 0.01 level

On the basis of a review of the above mentioned correlation coefficient, it has been found that, for all three sectors, the following factors are highly correlated to the implementation of information security policy: regular training, motivation, roles and responsibilities, communication, intentions, good security habits, rewards, assessments, awareness, satisfaction and reinforcement. The majority of these factors are significantly correlated to the adoption of information security norms, this justifies the need to assess their importance. Conversely, risk assessment, recovery, incident reporting and sanctions appeared to not be significantly correlated to the implementation of information security policy.

This thesis focused on the socio-perspective; it aimed to study the factors that impact on employee behaviours towards compliance with their

organisation's information security policy. The study empirically evaluated the obstacles and success factors that affect employee compliance to organisational security policies. It also evaluated the extent to which the socio-perspective impacted on improving organisational information security management. Thus, the focus of this study was on the socio-perspective, not the technical perspective; in particular, it including the relationships and the significance of various effective factors in order to fill the gaps in the literature with regards to the socio-perspective.

5.6 Conclusion

All of the tables presented within this chapter summarise the significant correlation coefficients that have been identified among the critical factors which contribute to the successful implementation of information security policy within organisations. It has been identified that awareness of the security norms and regulations is important for positive attitudes and intentions to occur among the employees as this will influence their decision to adopt and follow the policy frameworks. Furthermore, effective and regular training has also been identified among the critical factors that contribute to the successful implementation of information security policy within organisations, as these companies utilise assessments and reinforcements to align habits within the workplace, this motivates employees to comply with the policy guidelines. Finally, it is important to note the importance of the success factor of motivation which can be used to empower employees, by increasing staff satisfaction and successful compliance with the organisation's information security policy. Despite the

strength of these findings, a number of low correlations were observed between the compliance of information security policy and risk management, including: recovery, incident reporting and sanctions.

In addition, this research conducted a training and awareness programme that incorporated these effective factors in order to improve information security management as well as the awareness of sanctions and risk assessment procedures – this will be discussed in detail in the following chapter. The identification of the factors above has been helpful because the researcher is now aware of many factors that affect how employees follow security policies within their organisations. Furthermore, this analysis has also identified a number of factors that do not appear to impact on employee compliance to organisational information security policies.

Chapter 6: Information Security Awareness – The Training Programme

6.1 Introduction

Training is defined as the process by which participants learn the skills, knowledge, attitudes and behaviours that are needed in order to perform their work effectively (Subramanian, 2010). It is important to understand and place emphasis on the factors that are recognised as being effective rather than ineffective in terms of the training. It is therefore more important to categorise the factors that influence training rather than simply to investigate how these factors can contribute to better training results. This research is likely to provide a significant contribution as it aims to clearly identify and emphasise the characteristics of effective training which will lead to improved employee security behaviours; it will also examine their appreciation of sustaining such behaviours in the long-term.

According to Jaspersen et al., (2005) most of the developed training programmes are often wasted as the participants do not transfer their learned skills or their newly developed/appropriate behaviours into their work environment. Based on this research finding, this sixth chapter will identify the effective training techniques that can be implemented to improve user awareness, change attitudes, while also enhancing their motivation to transfer the new training knowledge and skills to improve performance within their role. According to Kirkpatrick (2007), the success of a training session is based on the successful transference of knowledge into the workplace.

6.2 Training Effectiveness

According to Mani (2010), wasted training is considered to be a common problem in organisations. In a recent study by Grossman and Salas (2011), they note that despite organisations investing billions of dollars in training every year, many trained competencies are reportedly not transferred into the workplace. The issue of knowledge transfer into the workplace remains a critical issue that faces organisation today.

This chapter will introduce the learning and training techniques which should be used, it will also look at the human factors as these principles can help to explain how training and the gaining of knowledge should be appropriate to the individual participant as this will then allow effective training to occur. In order to achieve effective training, it is important to understand how adults learn. Managing how an adult learns involves the utilisation of some basic principles which should be considered across various elements/functions of the training. Adults have different and special requirements and characteristics that need to be identified; therefore, it is essential to address and concentrate on the various learner style preferences when preparing the training materials.

Within this context, the importance of training can only be appreciated when a clear understanding of its impact on employee behaviour is obtained. It should also be remembered that an improvement in employee attitude will also lead to an improvement in company performance.

Training itself involves various processes of planning and organising activities through the use of delivered skills and techniques to employees which will ultimately assist them to establish and maintain the required skills for their future. The researcher believes that effective training should help the participant to develop their own personal skills, knowledge and abilities which will change their attitudes which will help them in the future, while also helping the organisation with its goals.

6.3 Training Objective

It is critically important to understand exactly what it is that makes training effective. As Laoledchai (2008) states, when users do not transfer the skills and the knowledge that are gained from the training programme then there is no value of it to the organisation.

It is also essential to recognise the contribution that these training programmes make to improve both individual and organisational performance, in order to understand how to focus on and gain benefit from such training programmes. To answer these questions, it is, firstly, essential to identify the effective factors that influence the success and impact of the training as these will affect the participants as individuals. Secondly, it is important to investigate how, when implemented, these factors contribute to better training outcomes and long-term sustainability. By focusing on these elements, it will enable the delivery of more effective training programmes that take into account the participants' motivations, communication through effective feedback, the promotion of training transfer with effective

reinforcement, regular assessment and ultimately an improvement in organisational performance.

6.4 Training Strategy and Plan

Initially, in the first stage, the actual training and awareness programme was piloted with a number of random participants. This pilot training programme aimed to gain effective feedback that could be incorporated to improve the training. The feedback gained from the participants, upon completion of the training programme, addressed the following elements: quality of the training, the scope of the training, the development method, as well as the level of difficulty, the ease of use, the duration of the training and suggestions for modification.

The aim of the developed security awareness programme was that it could be implemented within any organisation to make employees more security aware. As mentioned previously, in order for a security awareness programme to be effective, the individuals' attitude towards information security must be changed. It is also important to measure the sustainability of behavioural changes to ensure that actual attitudes have changed as this will help to enforce long-term change. The previous two chapters provided an overview of the most effective factors that need to be considered when implementing a training programme. Research acknowledges that information security issues need to be not only investigated and tackled, but that change must occur in order for people to truly act differently as behavioural change, on its own, isn't enough.

6.5 Implementation of Effective Training Factors

Based on the findings of this research, a specific set of factors have been identified as being influential and effective in affecting training – these factors have been analysed using both qualitative and quantitative methodologies. This section will identify how these different techniques will be implemented in the proposed training programme. The aim is that a conclusion will be drawn to identify how this study has contributed to the existing research through the suggestion of a comprehensive solution to improving organisational information security management.

6.5.1 Communication Mechanism

For the purpose of enhancing communication, within the training programme, the trainer needs to undertake various works and deploy numerous strategies. In this regard, the use of some tools and technologies, for the purpose of enhancing communication, would be beneficial. The more ways, in which, a trainer presents the information, the more the participant is likely to learn and retain the information.

In this context, the trainer should utilise a variety of teaching strategies, such as: group discussions and group problem-solving, while also using different graphical images, include: symbols, diagrams, photos and illustrations to attract and maintain the participants' attention while also explaining the issue effectively. It is also important to allow the participant to connect their own experiences with knowledge that is relevant to the topic, in order to make it more familiar and to increase motivation and knowledge retention. It is also

essential that the information/learning is regularly summarised in order to recap and to allow for clarification before a new subject is started. The trainer should provide the participant with questions which incorporate various communication techniques, in order to not only attract their attention to the subject, but also to maintain concentration and attention. According to Fallowfield (2003), the participant should feel involved in the training as this will allow them to draw their own conclusions about what they are going to learn.

6.5.2 Motivation Mechanism

Cameron and Pierce (2002) believe that the required behaviour will only be achieved if motivation is part of the teaching and learning process. The use of motivation, on a regular basis, will help the participant to remember what they have learned which will help them to maintain the new behaviour. It is therefore critical to understand the management principle of effective learning in order to accomplish better attitudes and better performance from the participants.

The trainer should use motivation as a method for increasing the participants' interest in understanding the issue, as this will help to increase the participants' engagement and belief in the issue. It is also paramount that the benefit of such a policy is explained and understood in clear, effective and easy language. Moreover, the trainer should aim to motivate the participants by enforcing the notion that they themselves can make a difference within their organisation by protecting it from security breaches.

By ensuring that the participants are aware that information security is their responsibility, they are likely to be more motivated to take more ownership and to put more effort and commitment into making the necessary changes. The trainer should also explore the notion of the importance of human factors as these can influence their attitudes towards compliance with their own organisation's security policy; furthermore, this also helps to show an appreciation of individual values and beliefs. As Smith (2008) notes, if the trainer satisfies all of the participants' needs, through the use of clear instructions, they will develop positive feelings about their learning experience which is likely to have a significant effect on their learning and transference of the learning into the workplace.

6.5.3 Feedback Mechanism

Goldstein and Ford (2002), suggest that the provision of feedback to the participant helps with their progress as it reinforces their learning experience. The provision of feedback can act as an important advantage to the participants' performance as it keeps them interested, engaged and motivated to attend the training, to learn and to sustain the new information. Effective training will provide the participant with prompt feedback which will allow for them to reflect on what they have learned, what they need to know and how to assess themselves at that point as well as in the future. The provision of feedback allows the participant to actually see a reward from the learning process, this can also help to keep them interested in the subject.

Within this context, the trainer can spend time focusing on understanding the participant and their beliefs and opinions, their reasoning, discussion through the use of questions and group problem-solving. This also gives the participant an important opportunity to explore their own opinions and beliefs freely by exploring the various benefits and tools that they need to learn to be able to achieve the goal of changing their behaviour towards security.

6.5.4 Reinforcement Mechanism

The provision of practising of the new skill ensures that the participant not only understands, but can also apply the new knowledge/skill in their role effectively. According to Kirkpatrick (2007), in order to obtain the true benefit of learning, it is important to interpret and apply the new skill and knowledge as this will maintain the desired performance. Therefore, it is important to allow for the practising of the new information immediate as this will help the participant to be more motivated as they will feel that they can put their learning investment into practice immediately.

Within this context, in order to facilitate permanent learning, the participant needs to make the learning part of themselves; the trainer, therefore, needs to allow the participants to talk about what they learn, write about it, relate it to past experiences and apply it within the training, as this will make it more relevant, reflective and permanent. Recent evidence suggests that once a new skill has been learnt, the participant should reinforce its acquisition by applying their knowledge right away. In recent years, there has been an increasing amount of literature stating that learning-by-doing is the basic

principle that fundamentally helps participants to change their actions into a new way of working that is based on the knowledge taught (Kirkpatrick, 2007).

6.5.5 Awareness Mechanism

Recent evidence also suggests that the use of clear explanations, guidelines and instructions can be more persuasive to the subject when they are supported by real facts and observations. It is also important to gain respect from the participants, as belief and respect for the trainer and the trainer's knowledge will allow them to gain more insight into the details and messages provided by the training. According to Subrahmanian (2010), training should be based on the identification of the training needs which will help with determining and designing the training material; finally, it is important to evaluate the training process to ensure that the training and learning is really transferred into the job environment.

The trainer therefore needs to provide facts, observations, the advantages and disadvantages, and guidelines, in order to allow the participants to focus their attention on the issue at hand. The researcher believes that it is critically important to establish a link between training, learning, behaviour and performance and that the development of an effective training programme, that will follow clear guidelines and principles of adult learning, will take into account each and every factor that might affect and have an impact on its success.

6.6 Designing an Awareness and Training Programme

The literature clearly indicates that training is considered to be one of the most important ways of providing learners with the initial skills and knowledge that are needed to cope with new challenges. For the purpose of this study, a security awareness and training programme will be developed which will incorporate the various methods, techniques and knowledge that are required to maximise security awareness and to manage and minimise security risks for individuals and organisations. A summarised process, of the proposed training programme is illustrated, below, in Figure 6-1.

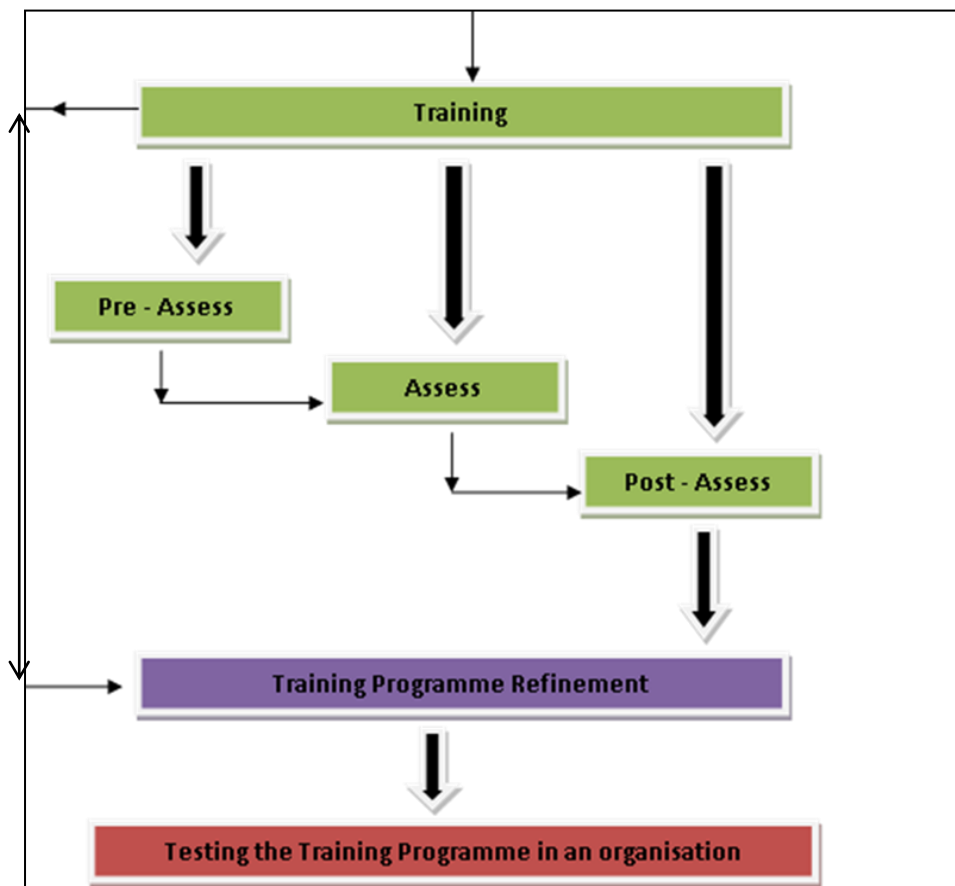


Figure 6-1: The Security Awareness and Training Programme

The training programme will be devised, different stages and different assessment levels will be used to evaluate understanding through these different stages. To illustrate, a pre-assessment level will be used to determine the employees' level of understanding of security management; training will then be provided in response to this for a certain period of time. For the post-assessment, the different stages and levels will be examined to determine whether the training programme achieved its aims.

6.6.1 Contents of the Security Policy

Various topics should be included and addressed by the security awareness training programme – the content should consist of the existing organisational policies. It is essential that the awareness and training programme supports the business needs of the organisation by illustrating why security awareness is vitally important. It is important that time is allocated to exploring the procedure as this will help to identify why it is so important to prevent incidents from happening, as well as providing an understanding of actions that should be taken if incidents occur. Furthermore, the content should use simple language to explore the topic of information security the use of bullet-points to highlight the activities that participants need to perform to ensure that the security controls actually meet the organisation's objectives.

6.6.2 Physical Security

Physical security focuses on physical actions that should be taken to protect buildings and property, including the: locking of doors, desks and filing

cabinets. Physical security includes the protection of personnel, hardware, computer programs, networks and data, from physical circumstances and events that could cause serious losses or damage.

6.6.3 Desktop Security

It is important to:

- Lock your doors, desks and filing cabinet drawers when you away from them.
- Not remove any computer equipment or media from the institute, unless you are authorised to do so.
- Add screensaver timeouts if you are away from your computer for more than five minutes.
- Use a password protected screensaver.
- Shutdown your computer at the end of the day.

6.6.4 Password Security

Password security should be focused on as a password should consist of a strong, secure password or passphrase, to illustrate:

- Some of the methods and examples that are explained include the use of a combination of letters and numbers which are joined together to make a password, such as: “too late again” could be spelled out as: “2L8again”.
- Another example would be through the use of the first letter of a combination of words in a sentence that can be used to form a strong

password, for example: “we spent too much at the fair last night”, could be constructed into the following password: “ws2matfln”.

- As a minimum, it should be a requirement that passwords should comprise of the following:
 - Numeric characters (1, 2, 3, 4, 5, 6, 7, 8 ...);
 - Special characters (/, [, -, +, =, \$, # ...);
 - Lowercase characters (a, b, c, d, e, f ...);
 - And, uppercase characters (A, B, C, D, E, F...).

6.6.5 Phishing

In terms of phishing:

- Phishing involves the act of sending an email on the pretence that it is from an online store (amazon, eBay, banks) or an internet service.
- Phishing hackers use this technique to obtain personal information such as credit card numbers, bank pin numbers and social security numbers.
- Be very careful of web links that are provided in an email.
- Do not submit banking or password information via email.
- Install good antivirus software packages that protect against phishing attempts.

6.6.6 Hoaxes

- Hoaxes come in many forms, including in the form of warnings about different viruses that can delete your hard drive or important system files.
- Hoax hackers use this technique to get you to forward a potential virus on to everyone in your address book to warn them about the viruses – without you realising that the actual email you are forwarding may contain the virus.
- To help to protect yourself from hoaxes:
 - Never open an attachment from someone you don't know.
 - Never open unexpected attachments from someone that you do know.

6.6.7 Malware

- Malware is software that is designed to secretly access a computer system without the owner's informed consent.
- Malware includes: viruses, worms, trojans, spyware and adware.
- There is a difference between real and fake malware: malware and fake anti-viruses are quite annoying, they are usually colourful and they start randomly.
- Most real internet protection software is Microsoft certified and a real update programme will download only with the owner's permission.

6.6.8 Viruses

- Viruses spread from one computer to another when users send files over a network or the internet; they can also be carried on removable mediums, such as a floppy discs, CDs, DVDs and flash drives.
- Interestingly, recent statistics show that unprotected computers can be infected with a virus, worm or trojan in less than five minutes after it is placed on a network.
- The installation of antivirus software is important, and it should be kept up-to-date all of the time.
- It is important to do it yourself, never assume that a system or application is always going to update itself.
- All downloads from websites and emails should be scanned first.
- Backup any important data you cannot afford to lose to an external drive, regularly.

6.6.9 Spyware and Adware

- Spyware and adware work by collecting personal information from websites that you have visited.
- Spyware can interfere with the user controls of a computer by installing additional software and by changing computer setting which can result in slower connection speeds.
- Spyware can be simple annoying pop-ups that are used for advertisement purposes that are meant to distract you, or they can even be used to attract you to a malicious site.
- Never click on an unwanted pop-up, instead shut them down.

- It is worth installing a pop-up blocker from Yahoo or Google.
- It is also worth installing and keeping updated, anti spyware.

6.6.10 Firewall

- Firewalls are devices that are designed to permit or deny network transmissions, they work based upon a set of rules.
- Firewalls are used to protect networks from unauthorised access. They prevent the unwanted sharing of files and computer resources, they also prevent applications on your computer from connecting to the internet. They also decrease the chances that a hacker will be able to access your computer.
- Always set Windows Firewall to be on.
- When you connect to a public network, in a hotel or airport, you will need to block all incoming connections to protect yourself.

6.6.11 Backup and Restore Data

- A backup is a copy of file that is stored in a separated location from the original.
- Backups are used to recover data when data has been lost, deleted or corrupted.
- You should back up anything that would be difficult or impossible to replace.
- Regularly back up files that you change frequently.
- Manually back up your files at any time, or set up automatic backup systems.

6.6.12 Encryption

- Encryption is a way of protecting folders and files from unwanted access.
- Encryption is a feature of windows that allows you to store information on your hard disk in an encrypted format.
- Encrypt employee personal information, such as: emails, financial information, budgets, bank account information and reports.
- The first time you encrypt a folder or file, you should back up your encryption key too.
- Whenever and wherever the key is stored, it must also be protected.

6.6.13 Software Copyright

- Software is like any other property. The software company who develops the software keeps their copyright with it and distributes it through chargeable costs.
- When you purchase commercial software, you are paying for a licence to use the software.
- Never install software when you do not have a licence to use the copyright.
- It is illegal to make copies of software without the owners' permission.
- Penalties for software copyright include: fines and up to two years of imprisonment.

6.6.14 Risk Assessments

- This process provides a report that describes the various threats and vulnerabilities, by measuring the risks and providing recommendations for control implementation.
- Risk assessments allow actions to be taken in an appropriate and timely manner, to any incidents.

6.6.15 Disciplinary Procedures

- An exploration of the importance of the disciplinary procedure enhances employee satisfaction by increasing their interest and motivation to improve their behaviour (Stanton, 2005).
- Examples of reward could include: increased salaries and bonuses, extra breaks, recognition by managers, certificates, trips, promotions and extra administrative rights and responsibilities, as well as good records.
- Examples of sanctions could include: reduced salaries, reduced break times, bad records, extended working hours and tasks, more responsibilities and more monitoring.

6.7 Observation

One of the main aims of the training was to allow for the observation and monitoring of participant behaviour. The following table, Table 6-1, identifies the various observation techniques that were used during the training.

Table 6-1: Observation Scenario

Task	Scenario	Target
Disclosing password	Leaving paper in the middle of the table with their usernames and passwords on it.	Observe whether they enter or write their private data.
Password behaviour	In the handout, an empty slide was left for their username and password.	Observe whether they enter their private data in their handout.
Safeguarding password behaviour	During the training, participants were asked to share their handout with another person.	Observe whether they share their private data with others.
Safeguarding password behaviour	When they create their password.	Observe whether they write the password anywhere else to remember it.
Access control behaviour	Going for a break.	Observe the participants' awareness of turning their computer off, or using lock or sleep modes.
Physical and environment security behaviour	Going for a break.	Observe whether they bring drink or food close to their computer.

The first technique was used to assess the participants' behaviour toward complying with the security policy through the use of the observation method. The researcher chose to use the observation method because it is very informative and can lead to understanding of a participants' natural behaviour; furthermore, this method allows the researcher to record and report findings that are deemed to be a true representative of the topic at hand. The researcher used the results from the participants' behaviour to develop communication channels between the participant and the trainer. This observation method aimed to assess the attitudes and factors affecting how employees think and behave in order to gain understanding of how to make improvements and positive changes.

6.8 Assessment

The researcher believes that the conduction of assessments are a fundamental element affecting the success of any training process and

programme. Assessments allow for the measurement of behaviour before and after the training; they can therefore confirm whether the training has had any lasting impact. Training assessments should be part of an ongoing process which continually gathers data before, during and after the training in order to truly determine what training needs exist and whether they have and are being met. According to Brown (2002), there are three main reasons why training need assessments must be completed as part of the development stage of any training programme. This process allows for the identification of: specific problem areas, the current training needs, any gaps in employee skills, as well as the identification of any new skills that are required to increase effective performance.

Within this context, the training firstly placed emphasis on the pre-assessment technique as this can help to provide the participant with feedback on their performance – the participant can also use this information as a benchmark for improving their own achievements.

Table 6-2: Knowledge, Attitude and Training Evaluation

To assess knowledge	To assess attitudes	Training evaluation
Passwords should contain both upper and lower case letters.	I think I am aware of information security policy?	This training helped me to understand the need of implementing the organisational information security policy?
As long as I do not share my password, I don't need to change it.	Security policy is important to protect the information in my organisation?	This training will help me complying with the information security policy in the future?
If the systems administrator calls me asking for my password for system maintenance, it is OK to give it to them?	Good security policy is a key to good information security management?	Because of this training I will comply with the organisational information security policy in the future?
Switching off, locking or using a screensaver protects my computer when I am away from it?	Security policy is important to raise employee's awareness of security?	Because of this training I have the knowledge to apply the organisational information security policy in the future?
I will only check websites or download any software when I am not familiar with the source?	Information security policy can reduce security breaches?	
I backup my data, daily if necessary?	Security awareness plays important factor in implementing security policy?	
I am aware that when I am connected to a public network in a hotel or airport, I need to block all incoming connections?		
I am aware of the difference between real and fake malware messages?		
I think I have the ability to take appropriate action to any incidents that relate to information security policy at work?		

A secondary emphasis was placed on the provision of training that aimed to change participant attitudes toward compliance with their organisational information security policy. Ultimately, the aim was that participants would improve their performance in their roles while also increasing their knowledge of security awareness so that they could be influential in reducing security breaches within their organisations.

The third emphasis was on the conduction of the post-assessment technique. This would be implemented three months after the training in order to determine whether the participant had made improvements and sustained and implemented the new knowledge successfully into the workplace.

Skill assessments can be used to measure learning as they can determine whether employees are meeting the required performance standards. One of the main objectives is that the security training and awareness programme will aim to improve behaviour toward compliance with the organisational security policy through the reinforcement of good security practices. The training programme was delivered to 15 participants from the business, health and education sectors.

The first section of the assessment tested the participants' existing knowledge about the principle of information security policy. For example, as shown in Table 6-2, through enquiries into password requirements, the safeguarding of password, backups, viruses and information security incident management behaviours.

The second section of the assessment aimed to assess the participants' attitude toward information security policy, as showing in Table 6-2. In particular, this focuses on questions regarding their level of awareness, the importance of security policies and the benefits that could be obtained from using these policies.

Finally, the third section aimed to evaluate the training by assessing the participants' level of understanding, commitment and level in which they were applying the learning.

6.8.1 Pre-Assessment

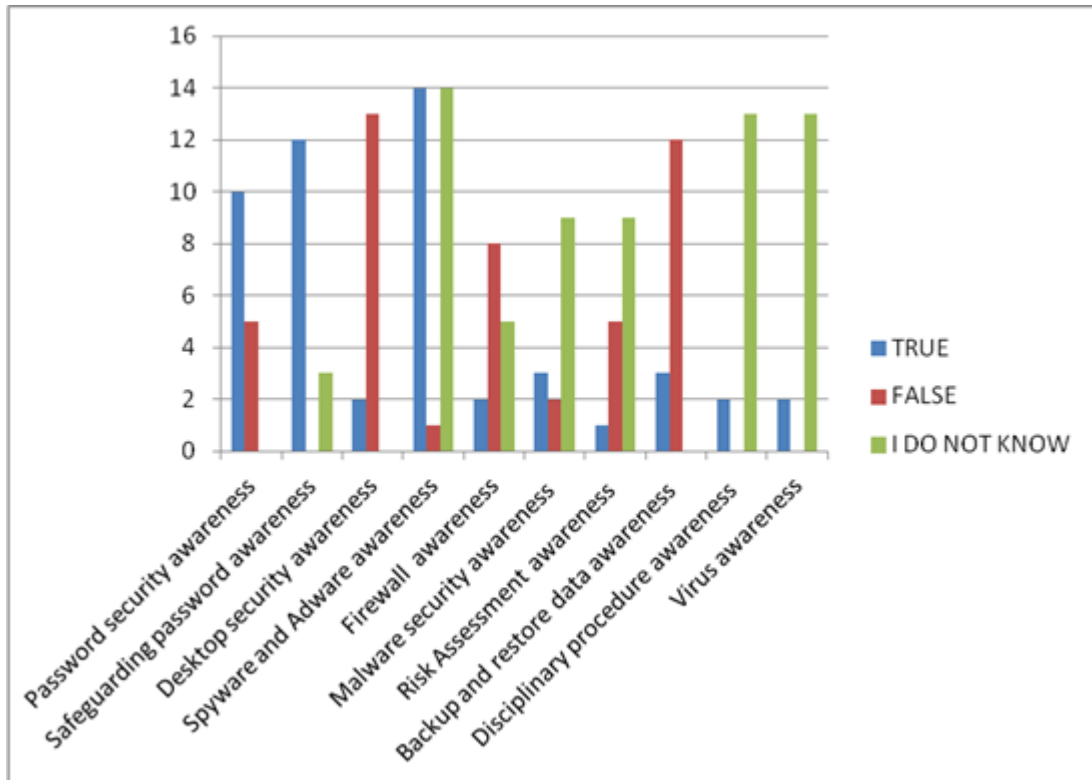


Figure 6-2: Pre-Assessment: Knowledge

The above figure (Figure 6-2) shows the participants' level of knowledge regarding their organisation's information security policy. The results from the pre-assessment show that the participants were generally lacking in terms of their skills and knowledge regarding organisational security policy topics. To illustrate, this was with regards to the sharing of passwords, backups, leaving PCs unattended and also the sharing of sensitive information, as well as a lack of awareness and knowledge toward viruses, copyright issues and risk assessments.

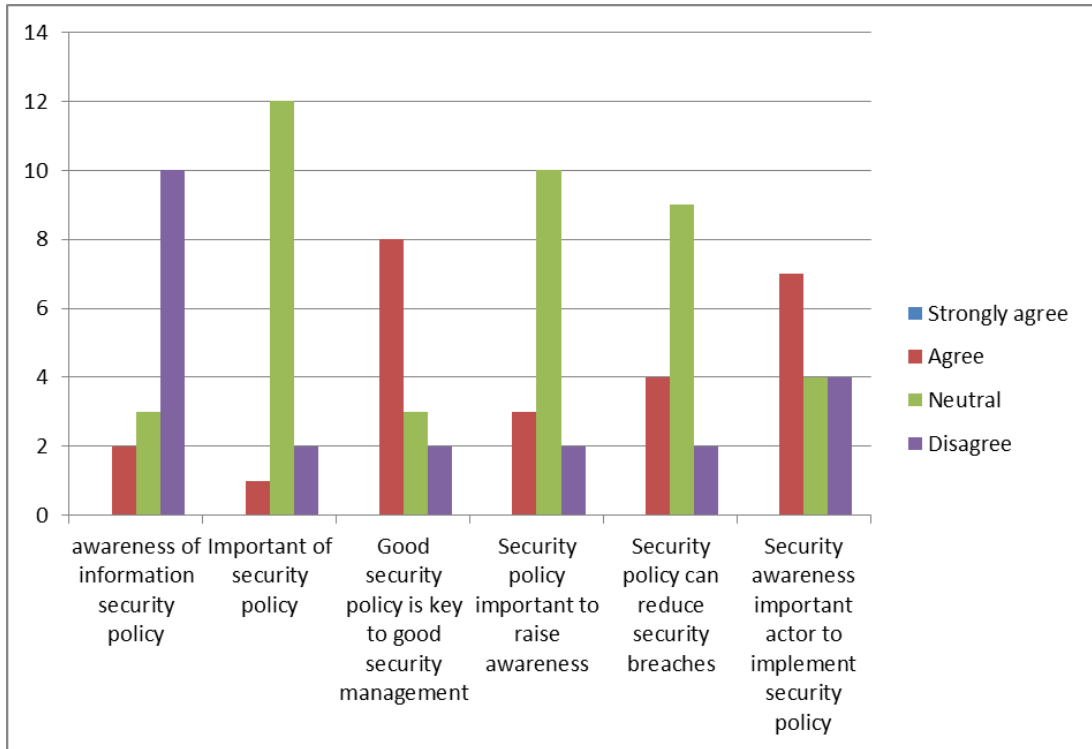


Figure 6-3: Pre-Assessment: Attitude

The figure above (Figure 6-3), illustrates the extent to which the participants agreed or disagreed with the importance of security policy, as well as their attitudes toward the impact of security training to raise security awareness. The results show that participants that were lacking in their attitude toward complying with the organisational information security policy generally lacked an understanding and belief in the importance of, as well as in the benefits and impact associated with organisational policy and security awareness.

6.8.2 Knowledge Reinforcement

The second phase of the training programme aimed to utilise the knowledge reinforcement technique – this should occur prior to the post-assessment stage. The reinforcement technique can be successfully used to motivate

and remind the participants, through appropriate communication, to make changes and improve upon their knowledge.

Upon completion of the first assessment, which should determine the participants' level of knowledge, training and awareness, learning and training should be implemented to improve participant awareness and to improve their behaviour toward compliance with their organisation's information security policy. In addition, after three months a further post-assessment stage should be conducted to determine whether the participants' knowledge and attitudes toward information security have been transferred and sustained into their work environments. Before conducting the post-assessment, effective knowledge reinforcement should be implemented as a reminder of the expected behaviours. These reminders are beneficial because they can help to effectively improve participant knowledge and motivation to perform and apply the newly acquired skills. According to Higgins and Silverman (1999), reinforcements have been shown to be particularly effective at motivating and achieving behavioural change.

6.8.3 Post-Assessment: Knowledge

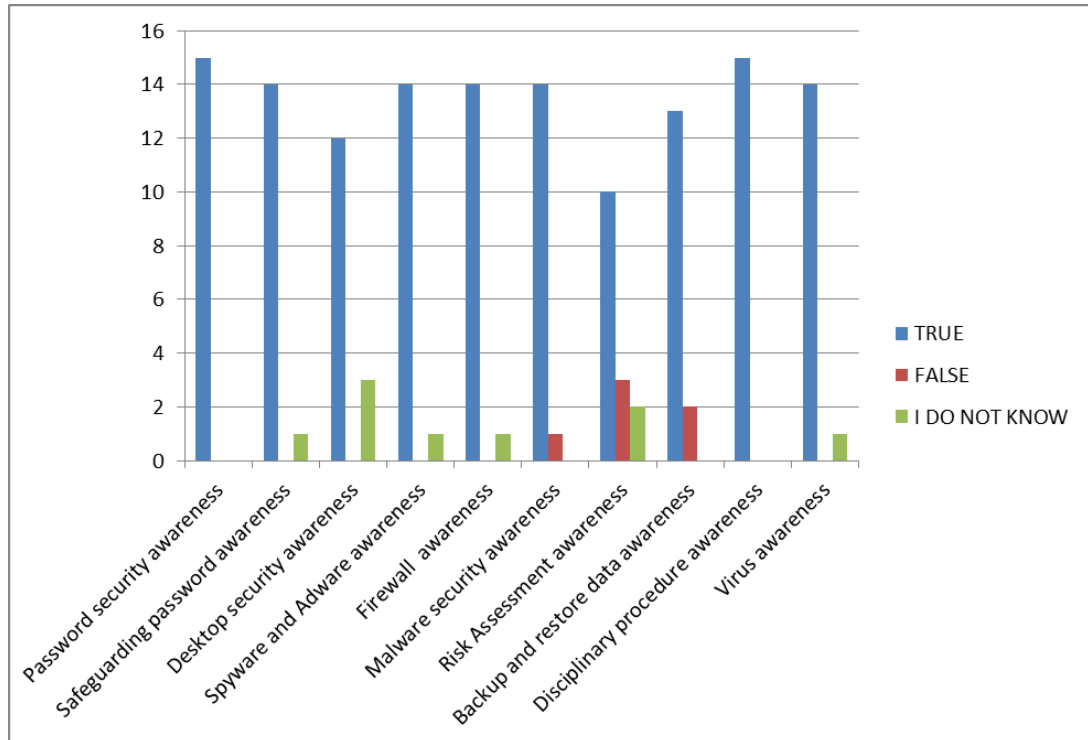


Figure 6-4: Post-Assessment: Knowledge

The aim of conducting post-assessment for the training is to allow follow-ups to determine the long-term effects of the training. The post-assessment should be conducted three months after the actual training.

The post-assessment results showed that there was a significant difference between the pre- and post-assessment results. The figure above (Figure 6-4) shows the improvement in participant knowledge; this was evidenced by an increase in the test scores from the post-assessment. This figure also confirms that the participants appeared to have a better understanding of their roles and responsibilities that related to complying with their organisation's policy.

6.8.4 Post-Assessment: Attitude

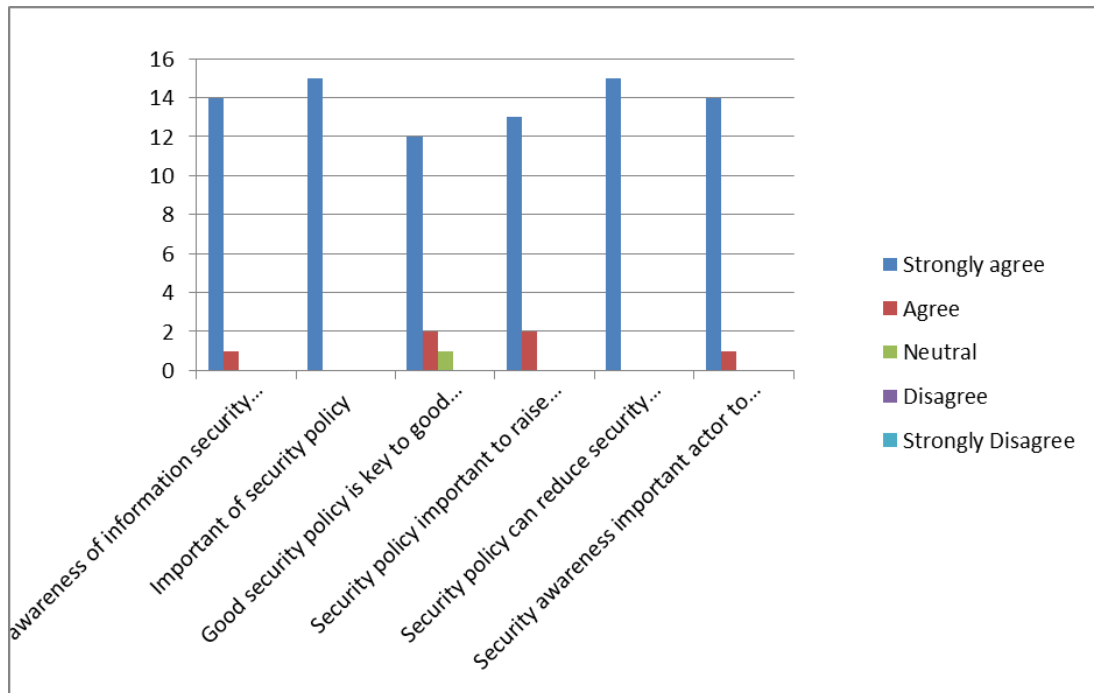


Figure 6-5: Post-Assessment: Attitude

Furthermore, there was also a clear improvement in the attitudes recorded from the pre-training to the post-training (see Figure 6-5 above). It was therefore apparent that the measures implemented by the training helped the participants to understand the need to comply with their organisation's policy, while also maintaining the knowledge they applied to the organisational policy. The results indicate that the participants improved their intention to change their behaviour. Furthermore, the figure also shows an increase in the appreciation value for the importance of, and benefit of, organisational policy and security awareness.

6.8.5 Evaluation Assessment

The results of the evaluation assessment demonstrate the effective impact of the training and awareness programme. Furthermore, the participants understood the need to comply with their organisation's security policy. In addition, there was an increase in interest to change their habits and improve their intentions to comply with the policies. Finally, it is worth noting that, there was an improvement in the participants in terms of their ability to perform and apply the required skills with a real aim of sustaining the newly acquired appropriate behaviours.

6.9 Conclusion

In terms of the utilisation of the evaluation method, the researcher can conclude the following findings. Clearly there are some critical factors that influence the behaviour of the employees attending the training programme; the findings from this research indicate that there are some significant factors that can increase training effectiveness, each of which will now be detailed. Firstly, the motivational technique can be used to lead the participant to improve their efforts and to gain knowledge. Secondly, communication and feedback techniques can be used to improve employee behaviours as they help to highlight the actual influence of their intentions and habits. Thirdly, the effective awareness technique should be utilised to ensure that understandable language is utilised during a course to ensure that the content is not too technical in nature. Fourthly, knowledge reinforcement techniques should also be used to improve the participants' level of satisfaction as this will help them to retain and maintain the organisational

security policy knowledge, in practice. Finally, the assessment technique should be used to determine the improvement stages and the suitability of the participants' knowledge.

Chapter 7: Discussion of Key Findings

7.1 Introduction

This chapter will provide a comprehensive discussion of the findings from this study. The contributions that this study has made will also be presented in the sections and sub-sections which are to follow.

It is apparent that there are many failures in terms of the implementation of information security and organisations are therefore increasingly under pressure from various security threats. A better understanding of what these threats are, and information on how to manage them, will help organisations to improve their business capabilities (Gupta et al, 2006). There are many different types of security breaches affecting organisations, as illustrated in the literature review. Furthermore, many efforts have been made in recent years to examine the problems, and numerous security issues have been addressed through research studies in an attempt to identify the main reasons for security breaches. However, most of these studies focus on technical aspects rather than on security management itself. To illustrate this point further, Hinson's (2003) research proves that studies which concentrate on the identification of technological solutions, to prevent vulnerabilities and security breaches, unfortunately tend to overlook the socio-technical aspects affecting the same vulnerabilities and breaches.

The literature review identified and explored the different research studies that had been conducted into the causes of security breaches; as such, the

researcher gained an understand of the critical factors affecting not only the current situation, but also the future vision of information security and its management. A recent study by Veiga and Eloff (2010) stated that an organisations' approach to information security should focus on employee behaviour, as the organisation's success or failure effectively depends on the things that its employees do or fail to do.

An investigation into the literature on information security brings with it many questions about good practice of what is needed for the good implementation of information security management. In particular, it became apparent that the following question had not been fully answered by the existing research: why are organisations, after working with security for such a long period of time, continuing to struggle to achieve good information security? The researcher decided to focus this study on the gap in the literature; the researcher therefore chose to concentrate on this area by investigating the actual implementation of information security policy as being central to the success of information security management. At this stage, the researcher acknowledged that there was a need for more research to be done into information security management as this could help organisations to achieve better information security implementation.

To explain the reasoning behind this research further, a recent study by Kraemer and Clem (2009) noted that human and organisational factors appear to play a significant role in the development of computer information security vulnerabilities. They emphasised a clear relationship between the complexities of human and organisational factors. Another study by

Beautement and Wonham (2009) indicated that a significant number of security breaches result from employee failures to comply with security policies. Furthermore, many organisations have tried to change or influence security behaviour, but they have found it extremely challenging. This literature clearly indicates that the management of information security policy is one of the major concerns of any successful organisation as many organisations have policies in place but the employees are not complying with them.

This research therefore aims to study the critical factors (CFs) that impact on employee behaviours toward compliance with their organisation's information security policy. The researcher will now, in the next sections, explore and validate firstly the obstacles and then the success factors with regards to the organisational and human dimensions.

7.2 The Main Obstacles of Complying with the Information Security Policy

The researcher used suitable methodologies which, in this case, combined the use of qualitative and quantitative methods. In order to explore and identify successful factors for implementing information security policies within organisations, a qualitative analysis was conducted on a number of interviews – this formed the basis for the study. The interview was divided into three main sections. The goal of the first interview section was to gain insight into the organisational factors that relate to information security management and also to reducing information security breaches.

As mentioned previously, in the literature review, the most common factor contributing to security breaches is employee behaviour towards security; thus, suggesting that changes in employee behaviour could have an impact on improving security. The second interview section aimed to analyse, in addition to the organisational aspects, employee behaviours as their behaviour is often neglected. The theory of reasoned action was used as a reference point for understanding employee attitudes – an analysis was then conducted on the identified factors that appeared to influence employee behaviours toward compliance with their own organisation's information security policy.

7.2.1 Security Policy

The results identified that security policies are not always visible, all of the time, and they are sometimes stored at inaccessible locations. Thus making it much more difficult for employees to remember the various aspects of the policies, as well as poor management of incidents being observed as and when they occur. As Post and Kagan (2007) indicate, visible information security policies help employees to understand good security behaviours; however, if the policies are no visible then employees may try to find ways around the security controls – this will ultimately affect their performance.

7.2.2 Work Pressure

The majority of individuals appeared to be implementing very few of the information security actions as they claimed that they had too little time to read and remember all of the elements in the policy. They also felt that the

documentation was too large, there was too much information and it was over complex. According to Doyle (2004), organisations cannot achieve excellent compliance because of the complexity of the policy. These results indicate that when there are time pressures to a job being done by a specific time, then employees often fail to comply with the security policy and an increase in workload will also cause a conflict of interest between information security and functionality.

7.2.3 Someone Else's Problem

Some employees believe that information security is not even part of their responsibility – they, therefore, do not need to consider it to be their priority as they only have to concentrate on their own working tasks. Furthermore, they assume that security is being implemented by the security professionals who manage any incidents by restoring any data losses, immediately.

7.2.4 Lack of Communication

The employee considers communication, or the lack of it, to be a barrier to complying with information security management. A lack of shared knowledge, between employees and managers, reduces the employees' involvement and commitment to avoid or resolve any security incidents. Therefore, the security management department needs to be visible in order to encourage communication, shared knowledge and role modelling behaviour through the use of regular updates for employees and frequent and recognisable reminders about the standard rules of information security.

7.2.5 Lack of Disciplinary Procedure

The result shows that there is a lack of clarity within the disciplinary strategy, as reward and sanction systems were not in place. Therefore, employees do not fear any consequences, on the whole, meaning that they made little effort to comply with the information security policies. The use of reward and sanction strategies helps to lead employees to participate more readily and make a more concerted and persistent effort to work and achieve the identified goals. These strategies also help to motivate employees to be stronger when they encounter bigger or more complex difficulties. The policy should clearly state that violations and non-compliance with the security policy will result in certain defined consequences. For example, any breaches of this security policy will be investigated and result in the individual being subjected to the organisation's disciplinary procedure.

7.2.6 Lack of Awareness

Some of the finding which related to non-compliance were linked to a lack of awareness and understanding of the actual policy. The findings suggest that many employees were not aware of any consequences, nor did they appreciate or understand the need of the policy. In particular, there were inconsistencies and problems with: the actual identification of clear problems or solution, the stimulating of clear advantages, disadvantages, benefits or the consequences of behaviour that were influencing an employee to not comply. Ultimately, if an employee had no knowledge or motivation to comply with the security policy, then the employee was unlikely to comply (Neal and Griffin, 2002).

7.2.7 Lack of Effective Training

The results indicate that the employees were not utilising and maintaining the gained information for long, so it was not improving their behaviour toward compliance with the security policy in the long-term. The results indicate that there were various reasons for this, including: the size of the training materials, the complexity of the training, a lack of visualisations and no group discussions. Furthermore, a lack of interaction, reinforcement and motivation reduced the importance level of the knowledge gained.

7.2.8 Lack of Roles and Responsibilities

The employees which showed the least effort toward complying with the information security policy appeared to act in a way that was just good enough rather than acting in a way to avoid security breaches. Without effective motivation, it is unlikely that there will be increased organisational performance or the coordination of positive efforts.

7.2.9 Individual Beliefs and Attitudes

In general, the majority of employees believe that even if security breaches occur, they will only affect the organisation rather than affecting them on an individual level. It became apparent that negative or poor attitudes, the influence of friends, colleagues and habits, as well as a fear to change, can all impact on an employees' compliance. In addition, the findings show that employees believe that the cost of cautious behaviour is higher than the perceived benefit of cautious behaviour.

7.2.10 Employee Habits

The results indicate that employee habits are the strongest factor that influences employee behaviour. Firstly, it became apparent that employees were not well-informed in terms of the security actions that they should take. Secondly, there was a fear of breaking their normal work routines in order to respond appropriately to the new situations or routines. Thirdly, the work environments were generally not supportive in helping the employees to change their habits as there was little or no observation or monitoring of security behaviours and the influence of friends and colleagues was also not accounted for. These findings highlight the importance of considering attitudes and habits as essential factors for explaining employee behaviour.

7.2.11 Trust

The findings show that employees often break the rules and fail to comply with the security policies, as a result of the level of trust among employees therefore, act as key challenging factors that can significantly influence employee behaviours in the work environment.

7.2.12 Lack of Top Management Support

The results show that acceptance, support and commitment, from the management teams, are essential in helping employees to comply with the security policies; furthermore, the necessary resources and budgets should also be provided for as this enforces the organisations' commitment. Furthermore, they also need to enforce the security policy, through continual monitoring and the provision of an adequate budget for an approved and

appropriate training and education programme. Furthermore, the top management team needs to review the currently implemented policies and strategies to ensure that any flaws or defects in the strategy are not only identified but also resolved. These actions will demonstrate visually how the management teams are willing to change in order to change the attitude of employees which will ultimately lead to a more favourable compliance with the security policies and strategies.

7.2.13 The Main Problems Summarised

Based on the literature review and the research findings from this study, many organisational information security policies appear to contain all of the required elements, however many employees are not complying with the policies because of the various reasons highlighted above. As mentioned previously, Puhakainen and Siponen (2010) found that the major threat to information security arises from careless employees who fail to comply with their organisation's information security policies and procedures. In addition, the literature review and the findings above show that the above factors are essential and they should therefore be incorporated and implemented within the information security policy. To illustrate, the policy must be enforced to make it effective, without enforcement a policy might as well not exist (Kenneth et al., 2009). Furthermore, the users' feedback of using and implementing the policies and procedures is essential in order to improve the effectiveness of them. Kim and Lee (2007) proposed that if employee involvement is not viewed as part of the overall transformation, the result will not accomplish the expected level of security. As such, Scott et al. (2009)

stated that when individuals are not motivated to follow certain procedures to protect information then security will fail.

Based on these findings, it is apparent that there is a need for effective awareness techniques to increase the participants' goals to learn as this will help them to understand and respond to security incident more effectively. Furthermore, by allowing the employees to participate by presenting their opinions and sharing their experiences in the learning process they will, themselves, learn to consider the most effective approach for improving their information security knowledge and awareness. In order to provide effective training, it is also essential to take into account each of the factors that might affect the training. Participants should be encouraged to maintain the new knowledge effectively in order for them to sustain the newly acquired and appropriate behaviour toward complying with their organisation's information security policy. As laoledchai (2008) states, when a user does not transfer the skills and knowledge that they have gain from a training programme, then there is no value of it to the organisation. According to the literature, it is therefore critically important to understand not only what makes training effective, but also what factors impact on the participants' ability to transfer the learning into their own work/job environment.

The finding from the interviews illustrate that there are some barriers affecting the success of the various training programmes. In particular, the main element needing attention concerns the lack of user involvement and user participation in the training programme. To illustrate, when there is too much information and too many written rules in the documentation then it

usually leads to a lack of communication and a lack of shared knowledge between the participant and the instructor. Furthermore, the findings indicate that there are often a lot of sources available for the gaining of knowledge; however, many employees fail to actively seek knowledge of information security as a result of a lack of engagement, a lack of reinforcement and problems concerning the method of training.

7.3 Critical Factors in Complying with the Organisation's Information Security Policy and Improvement of Information Security Management

After conducting the interviews to explore the obstacles that influence an employees' decision to not comply with the organisation's information security policy, further investigations were conducted using the quantitative survey approach. The findings from this questionnaire would reinforce and validate the findings from the qualitative stage and provide further details of critical factors (from the organisational, human and training perspectives) to improve information security management by providing guidelines for developing effective training programmes. Furthermore, the findings will then be used to propose a guideline for improving future information security management.

This study examined and investigated the critical factors influencing compliance with organisational information security policies. With reference to the information presented in the literature review (in chapter two), a list of critical factors were identified. The aim was that these factors would be

validated further through the use of research using more than one methodology, in particular the qualitative approach using interviews (see chapter four for more information), the quantitative approach using a survey questionnaire (see chapter five) and, finally, the implementation of an experimental training programme (see chapter six).

The remainder of this section, through the use of a number of sub-sections, will now be dedicated to the critical factors of information security through the proposal of various solutions and techniques. Each of these factors will be based on the analyses of the interview and the questionnaire that were conducted for the purpose of this study.

The researcher is pleased to conclude that this study has identified that there are success factors that can be critical in determining the success of information security management. In order for organisations to focus on improving employee compliance with their own information security policies, the following factors should be considered:

7.3.1 Awareness

The findings indicate that awareness of information security actually affects compliance toward information security policies. The results revealed that, in order to obtain the best from the awareness process, the information security policy must be quickly accessible and that the amount of information presented must be sufficient for the employees' needs, it should not be too long or too complex.

The findings from this research also suggest that it should be written in easy to understand language so that all employees can interpret the security policies; furthermore, regular reminders should be given to enforce and maintain awareness, through the use of messages, seminars, posters and articles in newsletters to disseminate such information. Based on these findings, employees not only have to be aware of, but also comply with their organisation's information security policies and procedures; therefore, organisations need to provide training and awareness programmes that include both organisational and human factors, including attitudes, normative beliefs and habits, to ensure that the knowledge is transferable and that the benefits are recognisable as beneficial to the employee and to the organisation.

7.3.2 Communication

Communication between the different parties helps to make policies and strategies more effective and more compatible with the various procedures and changes needed. On the basis of the analyses of the data presented in the earlier sections of this research, the level of communication within the organisation appears to influence the level of compliance with the organisational information security within an organisation; for instance: low communication results in poor compliance and good communication results in better compliance. For the purpose of enhancing the level of communication within an organisation, the management need to utilise certain efforts and strategies. The findings indicate that it is essential that the managers establish either direct or indirect contact with its employees to

ensure that awareness levels, regarding the security policy, can be enhanced by a significant level. In addition to the findings presented in this research, frequent meetings, seminars, conferences, discussion time and regular training are also important aspects and a requirement for successful employee compliance and effective organisational security management.

7.3.3 Employee Involvement

Employee involvement should encourage employees to be involved and engaged in suggestions for amendments and changes in the policies. This involvement will encourage more commitment from the employees, in terms of them using their gained knowledge. Moreover, employee involvement allows employee learning and development to occur which will ultimately improve and enhance the individuals' personal values. Within this context, the organisation needs to adopt various steps in order to encourage and spread employee involvement in the future. For this purpose, the managers should disseminate, dedicated and written, guidelines for the employees, so that they have the opportunity to discuss and share their changing needs and requirements.

7.3.4 Reward

The findings indicate that reward systems are a critical part of any organisations' policy to encourage the adoption and retention of certain behaviours. Reward systems form one of the most important critical factors, as they help to motivate employees to comply with organisational security policies; in particular, high reward levels generally lead to high satisfaction on

an individual level. Essentially, organisations should implement reward systems to promote employee enthusiasm and compliance efforts.

The findings from this research show that the rewarding of employees can be used to stimulate and reinforce the positive behaviours needed for effective compliance with organisational security policies. Therefore, based on these findings, reward strategies need to have clear aims and objectives as this clarity helps to inform employees of what it is actually expect of them. Finally, this study proves that rewards can have a significant effect on an employees' intention to comply with information security policy.

7.3.5 Beliefs and Attitudes

The belief from the employee with regards to values and attitudes is an important aspect that can enhance the level of security policy compliance. In particular, the appreciation of individual values can act as an essential factor for improving behaviour. Through empowering individuals, they will have more freedom and opportunity to innovate and explore new possibilities and approaches. Furthermore, employees should also be permitted to query the existing practices as this will enable them to share their beliefs and values towards compliance with the organisational policy. Furthermore, when an employees' beliefs and values are considered, they are more likely to want to take on extra responsibilities to resolve organisational problems; as such, they will be more open to learn new attitudes which will eventually lead to them being more competent and compliant. Employee attitudes and

normative beliefs and habits all have a significant effect on an employees' intention to comply with their information's security policy.

7.3.6 Habits

The findings indicate that habits affect an employees' intention to comply with information security policies. This study also shows that the changing of employee habits is considered to be one of the most essential requirements of successful and effective compliance to organisational information security policy. The process of changing habits, and the impact of these changes towards compliance with the security policy should be measured to determine whether the necessary improvements occurred. Furthermore, there should be constant rewards and recognition for best practice behaviours within organisations. The results from monitoring any changes can be used to demonstrate the value of knowledge; furthermore, this can be used as a motivator. To illustrate, the changing of habits can be used as a motivator when an employee can clearly see the contribution that they have played – as a significant role – in changing employee habits toward complying with security policy. This study also noted that, in order to change employee daily habits towards organisational security policy practices, their daily work routines and their workflow need to be monitored in order to determine whether change has really occurred.

7.3.7 Intention

Intention also plays a significant role in the success of organisational security policy. This study indicates that employee attitudes, normative beliefs and

habits all have a significant effect on an employees' intention to comply with information security policy. Furthermore, the stronger the intention to comply with the security policies, the more likely the individual is to actually comply. In this context, and for the purpose of changing the intention of the employees, the managers need to undertake a number of crucial and intensive steps. In this regard, the persuasion method will be the most suitable method for influencing change. In particular, the managers need to implement a programme or event by which they can communicate the different specifications and advantages of the proposed policy to the employees. Reward can also be utilised here to significantly affect the intention to comply with information security. These steps will help to persuade the employees to be positive in their intention towards the successful implementation of organisational information security policies.

7.3.8 Motivation

It is important that relationships are built to help to motivate employees within the organisation as this will help to facilitate a more proactive and open knowledge sharing process. Furthermore, if there is a low degree of motivation then employees are more likely to withhold their knowledge which will be negative as it will constrict the flow of knowledge because motivation requires individuals to come together to interact to exchange ideas and to share knowledge with one another. Thus, the better that employees are connected with each other, the better their performance and their motivation will be to comply with their organisation's security policy.

7.3.9 Reinforcement

The reinforcement of employee behaviours is crucial for the success of an organisation. Higher levels of reinforcement are linked with higher levels of employee compliance – this positive relationship, between reinforcement and compliance will increase the chances of success within an organisation. For the purpose of enhancing the compliance of employees, the managers need to provide various intensive and dedicated reinforcement techniques; such as: monitoring, reward, training, quizzes, assessments, reminder emails, etc. The making of mistakes should be viewed as an investment and learning process for the employee, because it can be a key source for creation in learning organisations. Furthermore, when employees leave the training, they should take their knowledge with them as this is essential for the retention of employees and the maintenance of loyalty from employees to their organisations.

7.3.10 Satisfaction

The satisfaction level of employees is also crucial to the success of any implemented policies within organisations. Importantly, the satisfaction level of employees is directly associated with the benefits availed by them; to illustrate, there is a positive correlation between increased advantages from the system and higher levels of satisfaction from employees. In order to enhance the level of satisfaction in the employee, proper and appropriate training and development plays an important role. During the training, employees must be given opportunities to identify the potential benefits from

using the system, so that they feel personally interested in the new system and its policies.

7.3.11 Assessment

Assessment is also an important training factor as it can help to determine the proper implementation of the organisational policies. Regular assessments should be utilised to determine the effectiveness of the process as this is one of the most crucial requirements for successful compliance. The assessment allows the managers to identify the problems and flaws within the processes; but, this requires intensive efforts from the management of the organisation. As such, the managers should undertake measures to determine employee awareness levels and compliance levels to their organisation's security policy. Within this context, the management of the organisation should not only make assessments, but they should also set, in accordance with these assessments, performance standards in order to allow for the identification of areas that need further improvement.

7.3.12 Training

This thesis has implemented an effective training and awareness programme that has been theory-based and empirically evaluated. The training programme focused on creating a link between training, knowledge and behaviour in order to attempt to modify employee attitudes toward their organisation's information security policy. As Puhakainen and Siponen (2010) state, there are many different security policy compliance approaches, but training is deemed to be the most commonly suggested in

the literature. However, very few of these studies into training actually promote information security policy compliance with the application of theories about learning principles. This research therefore focused on the effect of user compliance with information security policies to the implementation of appropriate training that provided empirical evidence for its practical effectiveness. Consequently, there is an essential need for information security training approaches that are theory-based and empirically evaluated.

Finally, the researcher concluded that it was important to understand that security awareness and training programmes should be formulated as one of the key requirements for improving employee compliance toward organisational information security policies. This conclusion was based on a number of elements, which will now be discussed in turn.

The literature demonstrates that employee non-compliance toward information systems security policies is a key concern for the majority of organisations. If employees do not comply with the information security policies, then the security solutions will lose their efficacy. This research presents the fact that there is a need to ensure employee compliance with the organisation's security policy. Compliance plays a major role in making practical and realistic organisational plans. The more compliance with the organisational policy, the more likely the organisation will have a satisfactory outcome with increased performance. Furthermore, compliance will be beneficial as it increases and enhances efficiency, quality and the reputation of the organisation.

Compliance with the organisation's security policy also improves employee behaviour which also contributes to organisational performance. Furthermore, compliance can help to ensure that all of the employees use the company's IT facilities in an effective, efficient and ethical manner. Ultimately, these actions will also help to reduce the risk to the company, company data and company equipment, by adequately protecting it against any action that could adversely affect the organisation. Finally, it should be noted that compliance with the organisation's security policy will ensure that all staff and employees are aware of the relevant legislative requirements and they will therefore conduct their day-to-day duties in a manner that routinely implements information security within the performance of all of their tasks.

7.4 Summary

The author of this thesis has built upon the empirical data, information and knowledge gained within this project in order to conclude that the implementation of a training programme, that is relevant and transferable in to the workplace, should be considered to be one of the most critical success factors that can greatly impact on and enhance employee compliance with an organisation's security policy. This study can conclude that many organisations are not putting enough effort into helping their employees to comply with their organisation's information security policies. In general, the employees are repeating the same mistakes, time and time again, rather than learning from them; this fact highlights that many critical aspects of

security management are being left behind, rather than being proactively and responsibly managed.

The developed training and awareness programme should incorporate techniques that aim to improve employee perceptions, attitudes and motivation as this will help to improve organisational information security management. The outcome and achievement target aimed to assure the sustaining of knowledge that would ultimately improve, permanently, employee security behaviours. This target was achieved through the combination and implementation of the most effective factors that were found to contribute to this research which included the influence of the following factors:

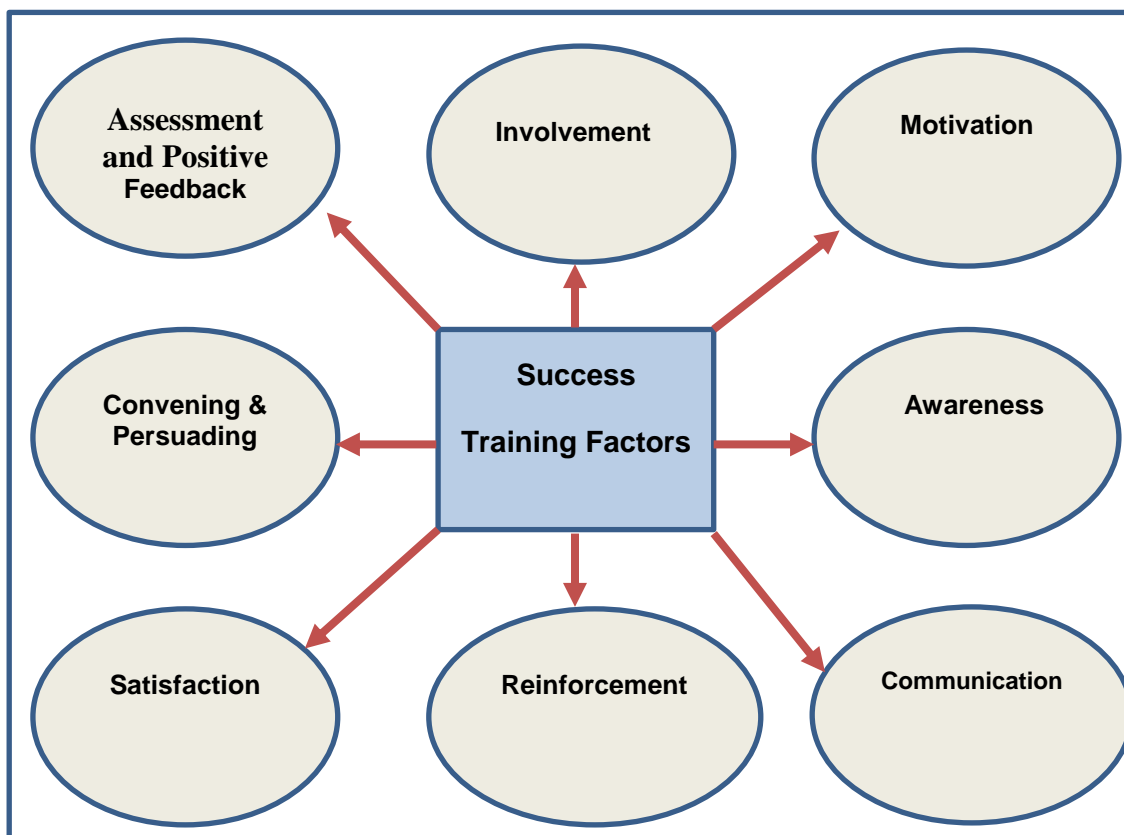


Figure 7-1: Success Training Factors of Compliance to InfoSec Policy

This chapter has discussed in detail the findings from the study and the critical success factors have been highlighted based on the impact that they have on employee compliance toward organisational security policy. Finally, the true impact of the training and awareness programme has been discussed in terms of how information security management could be improved through appropriate training.

In the next chapter, conclusions for this research will be presented, as well as a look at any limitations of the study and suggested areas for future research.

Chapter 8: Conclusions and Future Research

8.1 Introduction

This chapter will highlight the theoretical and practical contributions achieved from this study. Furthermore, the limitation of the study will be provided as well as conclusions and recommendations for future research, at the end of this chapter.

8.2 Theoretical Contributions

The aim of this thesis was that it was twofold, both theoretical and practical. From a theoretical perspective, this study contributes knowledge into the factors which influence employee behaviour towards compliance with organisational information security policies. This research also attempted to overcome many of the problems and inadequacies displayed in previous studies in order to truly provide improvements for the field of information security management.

The study therefore aimed to contribute to this area of research and practice. It adopted the organisational perspective in order to review a large body of literature, concerning many issues around organisational encounters and regarding compliance with information security policies. Based on this review, a number of critical factors affecting organisational information security policy were identified.

The finding of the effective factors that impact employee compliance with the organisational information security policy directed the researcher to investigate further to understand human factors. Various factors have been explored and studied in order to understand the employee behaviour perspective. As a result, various explanations have been included in an attempt to explain employee behaviour in terms of any obstacles affecting the implementation of organisational information security policy.

The study also contributed toward the identification of effective success components that would influence the delivering of effective training and awareness programmes. This enabled an evaluation of the impact of these factors in order to investigate and identify the characteristic of effective training that allow participants to maintain their knowledge effectively through the sustaining of appropriate behaviours toward complying with their organisation's information security policy. The outcomes presented in this study will therefore be of importance to scholars in this area because this study examined and investigated the critical factors that must be carefully considered to ensure successful employee compliance toward an organisation's information security policy and to ultimately, in the long-term, improve information security management.

This study aimed to investigate the management of information security by placing focus on three separate mechanisms: organisational factors, behavioural factors and training factors. Each of these mechanisms affects a different aspect of the information security problem. The study has provided comprehensive solutions to the improvement of organisational information

security management through the use of a combination of all three of these mechanisms. From this study, the researcher can derive a better understanding of the factors that impact on and greatly influence employee behaviours toward the improvement of information security management.

As a result, the researcher believes that information security management cannot be explained by a single frame, as every issue in information security is linked to another. Therefore, many organisations need to redesign their security policies to be in line with the guidelines and training that are given to their employees, as this will make the training and awareness more relevant and transferable into the workplace.

The findings are essential in assisting both the public and private sectors as the study has provided clear guidelines, in the form of a list, of the critical factors which must be considered to ensure the successful improvement and implementation of information security management.

8.3 Practical Contributions

The study also offers suggestions for the implementation of an effective training programme, based on the findings in the study. The aforementioned training programme aimed to enhance the employees' perceptions, attitudes and motivations in order to improve organisational information security management. The experimental approach was utilised to validate and confirm the findings of the study. Moreover, this research should help to improve employee awareness by equipping employees with the knowledge

to handle security decisions, now and in the future, in a manner that will help them to sustain and comply with their organisation's security policy in a comfortable way.

In addition, to the practical training gained from the study, which will help IT managers to improve the information security climate within their organisations. The feedback presented from the managers, from the studied sectors, concluded that the proposed training programme helped to improve the motivation of their employees. Feedback indicated the need for improving information security management by focusing on the socio-organisational perspective by firstly identifying and emphasising the obstacles and the reasoning behind what influences employees to comply with their organisation's security policies. Secondly, the training and awareness programme should be utilised effectively to modify employee behaviours toward compliance with the organisation's security policy. Moreover, agreement was obtained from each sector that participated in the study that guidelines could now be formed for the improvement of information security management that were built on a reliable understanding of the issues from the employees' perspective.

There is no evidence, from the previous literature, of the role that awareness programmes can play in making a difference to employee compliance to organisational information security policies. Therefore, this study has contributed to fulfilling this gap in the literature in terms of an identification of the importance of the various success factors and the implementation of them.

8.4 Limitations of the Study

As with all research projects, this study has a number of limitations which need further discussion. The presented data was obtained from three organisations within the UK, in the form of case studies, and can therefore not be taken to be completely generalisable.

This study was not only set in the UK, but in one specific region of the UK. Therefore more focus could be given to the study of several organisations, in different sectors and in different countries, in an attempt to obtain further understanding of the issues and in an attempt to validate the impact of the findings further.

In addition, although the quantitative study, presented in this research, was strengthened with findings from a qualitative study, it should be noted that qualitative studies are also not without their weakness. The limitations generally are concerned with the small sample size which has created a situation in which the findings are unlikely to be generalisable to other populations.

Furthermore, the methodology used in this thesis was applied from the socio-perspective setting in the UK; thus, the findings may not be applicable to organisations outside the UK.

Finally, this study conducted an experiment to validate the findings however this was conducted with only a small number of participants, over a short

period of time. The generalisations from the experiment are therefore limited, as such they would need to be repeated every three months for one year with a larger number of participants in order to truly measure the retention of knowledge and the sustainability of the employees' abilities to comply with their organisation's information security policy..

8.5 Future Research

As with all research, this research has raised further questions that could be addressed by additional research and work. Although this study covered a broad area of research, there are many directions in which future research could be adapted. For example, firstly it would be interesting to apply and implement the critical factors into different contexts of information security management using different cultures by using international sample surveys and compare them as this could add further value to the current study by providing generalised results.

Second, with regards to the implementation of the training and awareness programme, it would be useful to complete a more longitudinal study monitoring a group of participants for longer periods of time (after the training) which would allow for assessment on degree of employee compliance every three to six months, for one year. This would provide more information about retention of knowledge over time and the influence on employee behaviours. This could be extended further to investigate the impact of reinforcement (length and type of training), assessment, motivation and knowledge retention and compliance.

8.6 Conclusions

This study has presented an integrated review of the critical success factors of information security. Firstly, a review of the relevant literature was conducted and then a study was designed which utilised empirical research to conduct both qualitative and quantitative research. An analytical interview survey of 40 participants was conducted and a questionnaire survey was distributed to 400 participants. This study focused on three different sectors: the health, business and education sectors. The empirical data was then used to focus the study on the socio-technical aspects of organisational information security management.

The research used an empirically based investigation of critical factors to establish a connective body of knowledge and to overcome the gap in the existing literature of information security management. The study provided a necessary step by not only indicating but also examining the critical factors for the successful compliance with organisational information security policies. This research also further explored and investigated the implication of the obstacles and reasoning behind employee behaviours and attitudes toward compliance with the policy through the use of the theory of reasoned action. Furthermore, the study provided a training and awareness programme which incorporated various techniques to enhance employee attitudes, motivations and to improve their compliance with their organisation's information security policy.

This chapter has summarised the various contributions of the study conducted for this thesis, it has also identified the limitations and areas that would warrant future research.

References

- AbuZineh, S. (2006) *Success Factors of Information Security Management: A Comparative Analysis between Jordanian and Finnish Companies*. MSc thesis, The Swedish School of Economics and Business. Administration–Hanken
- Ajzen, I. (1980) *Understanding the attitudes and predicting social behaviour*. Englewood Cliffs, New Jersey: Prentice-Hall Inc
- Albrechtsen, E. (2007) A qualitative study of user's view on information security. *Computers & Security*, 26(4), pp. 276-289
- Alfawaz, S., Nelson, K., & Mohannak, B. (2010) Information security culture: a behaviour compliance conceptual framework. In: *Australasian Information Security Conference (AISC)*, Brisbane, Australia
- Aytes, k. & Connolly, T. (2004) Computer Security and Risky Computing Practices: A rational choice perspective. *Journal of Organizational and End User Computing*, 16(3), pp. 20-38
- Bandura, A. (1986) *Social Foundations of Thought and Action: A Social Cognitive Theory*, Prentice-Hall, New Jersey
- Bandura, A. (1997) *Self-efficacy: The exercise of control*. New York: Freeman
- Barne, S. (1997) "A Cause Map Approach to Assessing IS Implementation and Evaluation in the UK Health Sector". *Proceedings. Fifth European conference on Information Systems*, Cork, United Kingdom.
- Beautement, A., Sasse, M. A., & Wonham, M. (2009) The compliance budget: managing security behaviour in organisations. *In Proceedings of the 2008 workshop on New security paradigms*, (pp. 47-58). ACM
- Bernard, H. (2000) *Social Research Methods: Qualitative and Quantitative Approaches*. Sage Publication Inc
- Blakley, B., McDermott, E., & Geer, D. (2002) Information Security is Information Risk Management. *New Security Paradigms Workshop*, pp. 97-104
- Brinol, P., Valle, C., Petty, R.E., and Rucker, D.D. (2007) The Effects of Message Recipients' Power before and after Persuasion: A Self-Validation Analysis. *Journal of Personality and Social Psychology*, 93(6), pp. 1040-1053
- Brown, J. (2002) Training Needs Assessment: A Must for developing an effective e training program. *International Personnel Management Association*. 31(4)
- Bruque, S., & Moyano, J. (2007) Organisational determinants of information technology adoption and implementation in SMEs: *The case of family and cooperative firms*. *Technovation*, 27(5), pp. 241-253

- Bryman, A. (1995) *Quantity and Quality in Social Research*. London, Routledge
- Cameron, J. & Pierce, W. (2002) *Rewards and intrinsic motivation*. Westport, Conn: Bergin & Garvey
- Carr, L. T. (1994) The Strengths and Weaknesses of Quantitative and Qualitative Research: What Method for Nursing? *Journal of Advanced Nursing*, 20(4), pp. 716-721
- Caswell, F. (1989) *Success in Statistics*. John Murray Publishing, London
- Cooper, M. (2008) Information security training: lessons learned along the trail. *Proceedings of the 36th annual ACM SIGUCCS conference on User services conference*. Portland, OR, USA, ACM
- Creswell, J. (2003) *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*. Sage, Thousand Oaks, CA
- Creswell, J. W. (1998) *Qualitative inquiry and research design: Choosing among five traditions*. Sage, Thousand Oaks, CA
- Damrosch, S. (1991) General strategies for motivating people to change their behaviour. *Nursing Clinics of North America*, 26(4), pp. 833-43
- De Vaus, D. A. (1996) *Surveys in social Research* (4th Ed.), UCL Press Limited, London.
- Deloitte, R. (2007) *It's Do you know where your talent is? why acquisition and retention strategies don't work*. Geneva, Switzerland: Deloitte-Touch Research Report.
- Denzin, N. (1978) *The Research Ac*. New York, McGraw Hill
- Denzin, N. and Lincoln, Y. (2000) *the Handbook of qualitative Research* (2nd Ed.), Sage Publications, Thousand Oaks, Calif and London
- Dhillon, G. & Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11, pp. 127–153
- Dhillon, G. & Torkzadeh, G. (2006) Value-focused assessment of information system security in organisations. *Journal compilation Blackwell publishing Ltd, Information Systems Journal*, 16, pp. 293–314
- Dhillon, G. & Tejay, G. & Hong, W. (2007) Identifying Governance Dimensions to Evaluate Information Systems Security in Organisations. *Proceedings of the 40th Hawaii International Conference on System Sciences*.
- Dhillon, G. (2001) Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, 20(2), pp. 165-172
- Doherty, N. F., & Fulford, H. (2005) Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal*, 18(2), pp. 21-39
- Doherty, N., Anastaasakis, L. & Fulford, H. (2011) Reinforcing the security of corporate information resources: A critical review of the role of the

- acceptable use policy. *International journal of Information Management*. a Loughborough University, The Business School (31), pp. 201-209
- Dourish, P. & Bellotti, V. (1992) Awareness and Coordination in Shared Workspaces, in *Proceedings of the ACM Conference on computer supported cooperative work (CSCW'92)*, Toronto, Ontario. ACM Press. pp. 107-114
- Earl, M. J. (1993) "Experiences in strategic information planning". *MIS Quarterly*, 17(1), pp. 1-24
- Ebrahimi, A. & Naini, P. (2012) Exploring the Type of Relationship between Information Security Management and Organizational Culture. *International Journal of Information, Security and Systems Management*, 1(1), pp. 21-28
- Eidrn, D. L. (2006) *The healing effects of art in paediatric healthcare: art preferences of healthy children and hospitalized children*. Texas A&M University, USA
- Fallowfield, L. Jenkins, V. Farewell, V and Trapala, I. (2003) Enduring impact of communication skills training. *Cancer. Research UK*. 89(8), pp. 1445–1449
- Farahmand, F., Navathe, S., Enslow, P. and Sharp, G. (2003) Managing vulnerabilities of information systems to security incidents. *Proceedings of the 5th international conference on Electronic commerce*. Pittsburgh, Pennsylvania, ACM. 50, pp. 348-354
- Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior : An introduction to theory and research*. Reading, Mass.; Don Mills, Ontario: Addison-Wesley Pub. Co, p. 302
- Fulford, H., & Doherty, N. F. (2003). The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation. *Information Management & Computer Security*, 11(3), pp. 106-114
- Galvin, D. (2001) *Changing Behaviour*. Local Hazardous Waste Management Program in King County. Washington
- Ge, X., Paige, R., Polack, F., Chivers, H. and Brooke, P. (2006) Agile development of secure web applications. *Proceedings of the 6th international conference on Web engineering*. Palo Alto, California, USA, (pp. 305-312). ACM.
- Gehling, B. and Stankard, D. (2005) ecommerce security. *Proceedings of the 2nd annual conference on Information security curriculum development*. Kennesaw, Georgia, ACM. pp. 32-37
- Ghuri, P., Gronhaug, K. & Kristianslund, I. (1995) *Research Methods in Business Studies: A Practical Guide*. Prentice Hall, London
- Glisson, W., McDonald, A. and Welland, R. (2006) Web engineering security: a practitioner's perspective. *Proceedings of the 6th international conference on Web engineering*. Palo Alto, California, USA, ACM

- Goldstein, I.L., and Ford, J.K. (2002) *Training in Organizations: Need Assessment, Development, and Evaluation*, (fourth ed.). Wadsworth
- Gollmann, D. (2010) Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2(5), pp. 544-554
- Gon, K and Sangjae (2007) Factors affecting the implementation of electronic data interchange in Korea. *Computers in Human Behavior*, 24(2), pp. 263-283
- Gonzales & Sawicka (2002) A Framework for Human Factors in information Security. *Presented at WSEAS Int. Conf. on Information Security*, Rio de Janeiro.
- Grossman, R., & Salas, E. (2011) The transfer of training: what really matters. *International Journal of Training and Development*, 15(2), pp. 103-120
- Gupta, S. and Bostrom, P. (2006) End-user training methods: what we know, need to know. *In Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research*. ACM, New York, NY, USA, pp. 172-182
- Gurpreet, D. and B. James (2000). Technical opinion: Information system security management in the new millennium. *Commun. ACM*, 43(7), 125-128
- Hare, C. (2007) Policy Development. In H. F. Tipton, & M. Krause, *Information Security Management Handbook*, pp. 475-497
- Herath, T. & Rao, H. R. (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European journal of information system*, 18, pp. 106-125
- Hinson, G., (2003) Human factors in information security; Innovative information security awareness programs [online]. Available form: www.infosecwriters.com/text_resources/pdf/human_factors.pdf [Accessed: 10th Jan 2012]
- Hitchings, J. (1995) Deficiencies of the Traditional Approach to Information Security and the Requirements for a new Methodology. *Computers & Security*, 14(5), pp. 377-383
- Hitchings, J. (1996) A practical solution to the complex human issues of information security design. In: *Information Systems Security: Facing the Information Society of the 21st Century*, Katsikas, S.K. & Gritzalis, D. (eds), pp. 3–12. Chapman & Hall, London, UK
- Hone, K., & Eloff, J. H. (2002) What Makes an Effective Information Security Policy? *Network Security*, 20(6), pp. 14-16
- Hwang, H. G., Ku, C. Y., Yen, D. C. & Cheng, C. C. (2004) Critical factors influencing the adoption of data warehouse technology: a study of the banking industry. *Decision Support System*, 37, pp. 1-21
- Islam, S. and Dong, W. (2008) Human factors in software security risk management. *Proceedings of the first international workshop on*

Leadership and management in software architecture. Leipzig, Germany, ACM

- Jankowics, A.D. (1995) *Business Research Projects* (2nd ED.), Chapman and Hall, London
- Jasperson, J.S., Carter, P.E., and Zmud, R.W. (2005) A Comprehensive Conceptualization of Post-Adoptive Behaviors Associated with Information Technology Enable Work System. *MIS Quarterly*, (29)3, pp. 525-557
- Jick, T. (1979) Mixing qualitative and quantitative research methods: triangulation in action. *Administrative Science Quarterly*, (24), pp. 602-622
- Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), pp. 815–825
- Karyda, M., Kokolakis, S., & Kiountouzis, E. (2003). *Content, Context, Process Analysis of IS Security Policy Formation*. Security and privacy in the age of uncertainty, pp. 145-156.
- Keller, J.M. & Suzuki, K. (2004) Learner motivation and e-learning design: a multinationally validated process. *Journal of Educational Media*, 29(3), p. 232
- Kenneth, K., Morris, F., Thomas, M. and Anthony, B. (2009) Information security policy: An organisational-level process model. *Computers & Security*, 28(7), pp. 493-508
- Kim, B. G. & Lee, S. (2008) Factors affecting the implementation of electronic data interchange in Korea. *Computers in Human Behaviour*, 24(2), pp. 263-283
- Kim, C. & Ryu, Y. U. (2009) Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28, pp. 816-826.
- Kirkpatrick, J. (2007) *The Hidden Power of Kirkpatrick's Four Levels*. 61(8), pp. 34-37
- Knapp, K., Morris, F., Marshall, T. and Bydr, T. (2009) Information security Policy: an organisational level process model. *Computers & security*, 28, pp. 493-508
- Kotulic, A. G., & Clark, J. G. (2004) Why there aren't more Information Security Research Studies. *Information & Management*, 41, pp. 597-607
- Kraemer, S., Carayon, P., & Clem, J. (2009) Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & security*, 28(7), pp. 509-520
- Kraiger, K., Ford, J.K., and Salas, E. (1993) Application of Cognitive, Skill-Based, and Affective Theories of Learning Outcomes to New Methods of Training Evaluation. *Journal of Applied Psychology Monograph*, 78(2), pp. 311-328

- Kritsonis, A. (2004) Comparison of change theories. *International journal of scholarly academic intellectual diversity*, 8(1), pp. 1-7
- Kritsonis, A. (2005) Comparison of Change Theories. *International journal of scholarly academic intellectual diversity*. 8(1) California State University, Dominguez Hills
- Kritzinger, E. & Smith, E. (2008) Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, 27, pp. 224-231
- Lampson, B. W. (2004) Computer Security in the Real World. *Principles of Computer Systems*, 37(6), pp. 37-46
- Laoledchai, Y.; Land, L.; and Low, G. (2008) "Improving the Effectiveness of End-User Training Outcomes". School of Information Systems Technology and Management. The University of New South Wales Sydney, 2052, 19th Australasian. *Conference on Information Systems*, pp. 532-540
- Lederer, A. L. & Mendelow, A. L. (1993) Information systems planning and the challenge of shifting priorities. *Information and Management*, 24(6), pp. 319-328
- Lederer, A. L. & Sethi, V. (1988) The implementation of strategic information systems planning methodologies. *MIS Quarterly*, 12(3), pp. 445-461
- Liginlal, D., Sim, I. and Khansa, L. (2009) how significant is human error as cause of privacy breaches? Empirical study and a framework for error management. *Computers & Security*, 28(4), pp. 215-228
- Liisa, M., Mikko, S., Seppo, P., Tero, a. and Anthony, V. (2009) What levels of moral reasoning and values explain adherence to information security rules? *European journal of information system*. (18), pp. 126-139
- Lucas, H. Jr., Ginzberg, M. & Schultz, R. (1990) *Information Systems Implementation: Testing a Structural Model*. Ablex Publishing Corporation, Norwood, NJ.
- Machin, M.A., and Fogarty, G.J. (2003) Perceptions of Training-Related Factors and Personal Variables as Predictors of Transfer Implementation Intentions, *Journal of Business & Psychology*, 18(1), pp. 51-71
- Mader, A., & Srinivasan, S. (2005) Curriculum development related to information security policies and procedures. *In Proceedings of the 2nd annual conference on Information security curriculum development*, Kennesaw, Georgia, pp. 49-53. ACM
- Mahapatra, R., and Lai, V.S. (2005) Evaluating End-User Training Programs, *Communication of The ACM*, 48(1), pp. 67-70
- Mak, S. (2001) A model of information management for construction using information technology". *Automation in Construction*, (10), pp. 257-263

- Mani, V. (2010) Evaluating Effectiveness of Executive Training. *International Bulletin of Business Administration*. ISSN: 1451-243X, 9
- Marshall, G. (2005) The purpose, design and administration of a questionnaire for data collection. *The society and college of radiographers*, (11), pp. 131-136. Elsevier Ltd
- Mathieu, J.E., Tannenbaum, S.I., and Salas, E. (1992) Influences of Individual and Situational Characteristics on Measures of Training Effectiveness. *Academy of Management Journal*, 35(10), pp. 828-847
- McMillan, J. H. (2000) *Education research: fundamentals for consumer*. 3th ed. Longman, New York
- Mouton, J. (1996) *Understanding social research*. Van Schaik, Pretoria
- Murphy, L. (2011) Occupational stress management: A review and appraisal. *Journal of Occupational Psychology*, 57(1)
- Narayan, A., Steele-Johnson, D., Delgado, K.M., and Cole, P.A. (2007) Differential Effects of Pretraining Influences on Readiness to Change. *Journal of Psychology*, 14(1), pp. 47-60
- Nau, D. (1995) Mixing Methodologies: Can Bimodal Research be a Viable Post-Positivist Tool? [Online]. Available form: <http://www.nova.edu/ssss/QR/QR2-3/nau.html>. [Accessed 19th Jan 2012]
- Neal, A., & Griffin, M. A. (2002) Safety Climate and Safety Behaviour. *Australian Journal of Management*, 27, pp. 67-75
- Neil, D. and Heather, F. (2006) Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 25(1), pp. 55-63
- Neill, J. (2007) Qualitative versus Quantitative Research: Key Points in a Classic Debate. Research Methods, Qualitative Versue Quantitative Research. [Online]. Available form: <http://www.wilderdom.com/research/QualittiveVersueQuantitativeReseach.html> [Accessed 10th March 2012]
- Neuman, W. (2000) *Social Research Methods: Qualitative and Quantitative Approaches*. 4th ed. Allyn & Bacon, Boston Mass and London.
- Neuman, W. (2004) *Basics of Social Research: Qualitative and Quantitative Approaches*. Pearson, Boston, MA
- Noe, R.A. (1986) Trainees' Attributes and Attitudes: Neglected Influences on Training Effectiveness. *Academy of Management Review*, 11(4), pp. 736-749
- Norris, D. F. (1999) *Leading edge information technologies and their adoption: Lessons from US cities*, in G. D. E. Garson, (ed.) Information Technology and computer Applications in Public Administration: Issues and Trends. Idea Group Publishing, Hershey, PA

- Omari, A., El-Gayar, O., & Deokar, A. (2012) Security Policy Compliance: User Acceptance Perspective. *In System Science (HICSS), 2012 45th Hawaii International Conference on.* pp. 3317-3326. IEEE.
- Payne, S. (2003) Computer Security Education and Awareness. *Computer and Network Security in Higher Education*, pp. 89-104
- Perloff, R.M. (2008) *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*. New York, London: Lawrence Erlbaum Associates
- Posner, B., Randolph, W., & Schtuidt, W. (1987) Managerial Values Across Functions: A Source of Organizational Problems. *Group and Organization Studies*, 12(4), pp. 373-385
- Post, G. V., & Kagan, A. (2007) Evaluating Information Security Tradeoffs: Restricting Access can interfere with User Tasks. *Computers & Security*, 26, pp. 229-237
- Premkumar, G. & King, W. R. (1994) Organisational characteristics and information systems planning: an empirical study. *Information Systems Research*, 5(2), pp. 75-109
- Puhakainen, P. (2006) Design theory for information security awareness. Faculty of Science, *Department of information processing science*. University of OULU
- Puhakainen, P., & Siponen, M. (2010) Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4), 757-778
- Quaddus, M., & Hofmeyer, G. (2007) An investigation into the factors influencing the adoption of B2B trading exchanges in small businesses. *European Journal of Information Systems*, 16(3), pp. 202-215.
- Quinones, M. (1995) Pretraining Context Effects: Training Assignment as Feedback, *Journal of Applied Psychology*, 80(2), pp. 226-238
- Reason, J.T. and Hobbs, A. (2003) *Managing maintenance error: a practical guide*. Ashgate Publishing, 2003
- Rhee, H. S., Kim, C. & Ryu, Y. U. (2009) Self-efficacy in information security: Its influence on end users' information security practice behaviour. *Computers & Security*, 28, pp. 816-826
- Rich, M., & Ginsburg, K. R. (1999) The Reason and Rhyme of Qualitative Research: Why, When, and How to Use Qualitative Methods in the Study of Adolescent health. *Journal of Adolescent health*, (25), pp. 371-378
- Robert, C. S. & Rolf, M. (2003) Operationalizing IT Risk Management. *Computers & Security*, 22, pp. 487-493
- Robey, D., Gupta, S. & Rodriguez-Diaz, A. (1990) *Implementing Information Systems in Developing Countries: Organisational and Cultural Considerations*, in S. Bhatnager & N.Bjorn-Anderson, (ed) Information

- Technology in Developing Countries. North-Holland, Amsterdam. Pp. 41-50
- Rossouw, v. and Basie, V. (2004) From policies to culture. *Computers & Security*, 23(4), pp. 275-279
- Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007) Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1), pp. 56-62
- Russell, R., Bidwell, T., Steudler, O., Walshaw, R. & Huston, L. B. (2001) *Designing and Implementing Security Policies*. Hack Proofing Your E-Commerce Site, pp. 219-260
- Sasse, M. A., & Flechais, I. (2005) *Usable security: Why do we need it? How do we get it?"* pp. 13-30.
- Saunders, M. N., Lewis, P., & Thornhill, A. (2000) *Research Methods for Business Students*, 2nd ed. Prentice Hall
- Saunders, M., Lewis, P. & Thornhill, A. (2000) Using Secondary Data, in *Research Methods for Business Students*. 2nd ed. Prentice Hall, Harlow.
- Scott, B., Laurie, K., Ingo, A., Raymond, S., Wayne, B. (2009) If someone is watching, I will do what I am asked: mandatoriness, control, and information security. *European journal of information system*, 18, pp.151-164
- Siegel, D et al. (2006) IT security: *protecting organisations in spite of themselves*. *Interactions*, 13(3), pp. 20-27
- Smith, A. (1999) Computing in Construction Procurement: Some Experience From Hong Kong. *Australian Institute of Building Papers*, (9), University of Melbourne.
- Soliman, M and Lapointe, L. (2009) Motivational Needs And It Acceptance: The Need For A Richer Conceptualization Of The Perceived Usefulness Construct, John Molson, *School of Business. Faculty of Management*. Niagara Falls. Ontario, ASAC, 30(4)
- Solms, B., (2004) The 10 Deadly Sins of Information Security Management. *Computer & Security*, 23, pp. 371-376
- Stanton, J. M. & Stam, K. R. & Mastrangelo, P. & Jolton, J. (2005) Analysis of end user security behaviours. *Computers & Security*, 24(2), pp. 124-133
- Straub, D. and Welke, R. (1998) Coping with systems risk: security planning models for management decision making. *MIS Q.* 22(4), pp. 441-469
- Subrahmanian, M. (2010) Evaluating Training Programmes in India Post. *Journal of Arts Science & Commerce*, (1), ISSN, 2229-4686
- Sumner, M. (1999) Critical success factors in enterprise wide information management systems projects. *In Proceedings of the 1999 ACM SIGCPR conference on Computer personnel research*, pp. 297-303. ACM

- Swanson, E. B. & Wang, P. (2005) Knowing why and how to innovate with packaged business software. *Journal of Information Technology*, (20), pp. 20-31
- Tannenbaum, S.I., and Yukl, G. (1992) Training and Development in Work Organizations, *Annual Reviews of Psychology*, (43), pp. 399-441
- Tarafdar, M. & Vaidya, S. (2006) Challenges in the adoption of E-Commerce technologies in India: The role of organisational factors. *International Journal of Information Management*, (26), pp. 428-441
- Tashakkori, A., & Teddlie, C. (1998) *Mixed Methodology: Combining Qualitative and Quantitative Approaches*. Thousand Oaks, CA: Sage
- Taylor, B. (1997) The return of strategic planning-once more with feeling. *Long Range Planning*, 30(3), pp. 334-344
- Torkzadeh, G., & Koufteros, X. (1994) Factorial validity of a computer self-efficacy scale and the impact of computer training. *Educational & Psychological Measurement*, 54(3), pp. 813–821
- Tucker, S. N. & Mohamed, S. (1996) Introducing information in construction: pains and gains. *Proceedings of the CIB-W65 Symposium on Organisation and Management of Construction*, Glasgow. pp. 348-356
- Vance, A., Siponen, M., & Pahnla, S. (2012) Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, 49(3), pp.190–198
- Veiga, A., & Eloff, J. H. P. (2010) A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), pp. 196-207
- Voss, B., (2001) The ultimate defence of depth: security awareness in our company
[online]. Available form:
<http://rr.sans.org/aware/ultimate.php> [Accessed: 05th Jan 2012]
- Whitman, M. E., Caylor, J., Fendler, P., & Baker, D. (2005) Rebuilding the Human Firewall. *Information Security Curriculum Development Conference*, pp. 104-106. Kennesaw, GA, USA: ACM
- Wheelen, T. L. & Hunger, J. D. (2000) Strategic management and business policy: *Entering, 21st century global society*. 7th ed, London, Prentice Hall.
- William, Z. (2003) *Business research Methods*. Thomson/South-Western, Great Britain
- Wilson, M., De Zafra, D. E., Pitcher, S. I., Tressler, J. D. & Ippolito, J. B. (1998) Information Technology Security training requirements: *A Role- and Performance-Based Model*. *NIST Special Publication*, pp. 800-816
- Workman, M., W. H. Bommer, et al. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), pp. 2799-2816

- Yates, S. M and Aronson, E. (1983) A social psychological perspective on energy conservation in residential buildings. *American Psychologist*, 38(4), pp. 435-44
- Yin, R. (2003) *Case Study Research: Design and Methods*. Sage, Thousand Oaks, CA& London
- Zhang, P., Benbasat, I., Carey, J., Davis, F., Galletta, D. & Strong, D. (2002) human-computer interaction research in the MIS discipline. AMCIS 2002 panels and workshops I: *Communications of the Association for Information Systems*, 9, pp. 334-355

Appendix A: Interview Information

A-A1: Letter

My name is Nesren Waly, I am currently doing a PHD at the Informatics Department at University of Bradford. My research is to investigate the most effective strategies for developing and implementing a training and awareness programme that will concentrate on changing user behaviour toward security in organisations. There are no right or wrong answers to the questions i ask you and I would like to elicit your opinions and expertise about a number of issues related to security in organisations and strategies for improving employee behaviour.

Just to let you know, we abide by the University of Bradford's ethical policies governing research and data collection and unless you specifically agree otherwise, you as a contributor will remain anonymous and all your personal and organisation's details will remain confidential. The information I collect will be used in my PhD and any subsequent publications that emerge. I will be happy to provide you with a summary once my study is completed.

If you have no objection I will be taping this conversation to make sure that I can pick up on your very valuable contribution.

A-A2: Interview Questions

Section 1: To understand information security user behaviour influences

- 1) How would you rank your knowledge of information security management on scale of 1-10 where 10 is excellent?
- 2) Can you briefly tell me about your information security experience?
- 3) In general what influences your behaviour toward information security?
 - a. (Probe for: Do people around you influence your behaviour toward information: if so who, and how?)
- 4) Have you had any training in information security? Can you tell me about it
 - a. (Probe for: the context (where/when/how; did it change your behaviour; did it make you more aware?)
- 5) In general do you take risks in your life? Can you tell me how?
(probe for examples)
- 6) Do you take risks when you use your computer,? Can you tell me how? (probe for examples)
- 7) What do you think you could do to reduce information security breaches when you use your computer?
- 8) Have you witnessed any information security breaches at work?
Can you tell me about it?
- 9) If you witnessed a security breaches when using a computer by one of your work colleagues, how would you react it?

10) What do you think would make you more likely to change your behaviour towards information security management at work?

Would this be in short term or permanent change? (please explain)

Section 2: Effectiveness of information security policies at work

- 1) In your role do you have any responsibility for information security management: if so how
- 2) On average how many information security breaches do you experience a year at work? Has this improved or got worse over the past 5 years? Please explain why and how
- 3) Does your organisation have a policy on information security management? If so how effective is it in reducing information security breaches?
- 4) Are people in the organisation consulted about the information security policy, to what extent? (probe for who and positions)
- 5) How is the information security policy disseminated to employees in your organisation?
- 6) Is it easy to understand and follow? Why?
- 7) In your opinion what should be included in an information security policy?
- 8) Do you think information security policy is an effective way of changing people's attitude toward security: can you explain?
- 9) Do you think information security policy is an effective way of changing people's behaviour toward security: can you explain?

- 10) Are employees and management equally informed and engaged with the organisation information security policy: can you explain?
- 11) Would a programme of reward and sanction be effective in changing behaviour? (please explain)

Section 3: Training and awareness programmes to impact on information security management behaviour

- 1) Do you provide information security management training to your employees?. **(IF THEY HAVE TRAINING GO TO Q2**

WHY NOT THEN GO TO Q.11,)

- 2) How do you train your staff to avoid information security breaches?
- 3) Do you evaluate training effectiveness: if yes how
1. If not, in your view how would you evaluate it?
- 4) Is the training programme successful, how do you measure its success?
- 5) Do you think this training makes them perform better in their job? (How?)
- 6) Do you cater for individual learning styles please explain
- 7) Have those that received training changed their attitude after receiving the training, if so how?
- 8) Have those that received training changed their behaviour after receiving the training, if so how?

- 9) Do you have any why of reinforcing staff behaviour after training? (please explain)
- 10) In your opinion what would motivate those that have undertaken training to change their behaviour in the long term?
- 11) What do you think are the top five information system security training needs in your organisation?
- 12) If you were designing an information security training programme, what would you include in this in terms of :
- (a) Content
 - b) Motivation technique
 - c) Delivery method
 - d) What reward / sanction would you use?
- 13) Are there any other comments about the training and awareness programme that have not been covered and that you would like to make?

Thank you very much for your contribution it has been most valuable

Appendix B: Questionnaire

I am currently conducting a study to investigate the most effective strategies for developing and implementing training and awareness programme that will focus on changing user behaviour towards information security in organisations. This study forms part of my PhD thesis at the University of Bradford School of Informatics and Computing.

Your contribution to this study would be most valuable and the aims of this questionnaire are to elicit your views about information security and your attitudes and common practices related to it.

In order to be able to use your contribution, I would be most grateful if you could complete all the questions in the questionnaire. This study is bound by the University of Bradford ethical policies governing data collection. Participants in the survey are assured of confidentiality and shall remain anonymous and no personal identifying information will be collected or used. If you have any questions or queries, please contact me or my supervisors (Dr Mumtaz Kamala, or Dr, Rana Tassabehji, University of Bradford, m.a.kamala@bradford.ac.uk; R.Tassabehji@bradford.ac.uk)

By continuing with this survey you are agreeing to take part in this study
Thank you

Page 1 Demographics:

***1. What is your age**

***2. What is your gender**

***3. What is the level of education you have attained (you may tick more than one).**

- Bachelor's degree
- Master's degree
- Doctorate degree
- HND, NVQ, GCSE
- If other, please specify

***4. position in the organisation? Please state your title**

***5. In which industry sector do you work? Please specify**

*** based on your organisation's security policy:**

6. Does your organisation have a security policy

Yes

No

Additional Comments

7. please state the extent to which you agree with the following statements On a scale of 1-5 where 1= Strongly agree 2 = Agree 3= Neutral 4= Disagree 5= Strongly disagree

	1	2	3	4	5
1) My organisation rewards employees for following the information security policy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2) My organisation rewards employees for reporting security breaches	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
3) My organisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

employees for not following the information security policy

4) My organisation punishes employees for unintentionally breaching security

8. please state the extent to which you agree with the following statements On a scale of 1-5 where 1= Strongly agree 2 = Agree 3= Neutral 4= Disagree 5= Strongly disagree

1 2 3 4 5

1) I am familiar with the contents of my organisation's information security policy

2) my organisations conducts effective risk assessment which has reduced security breaches

3) I am aware of my organisation's policy of security incident reporting procedure

4) I am aware of my organisation's policy of security incident recovery procedure

5) I follow my organisation's policy for security incident reporting and recovery procedure

6) I believe that an employee's awareness of risk management will improve employee's behaviour toward security

7) Following my organisation's information security policy is my responsibility as an employee

8) Following my organisation's information security policy is a part of my role in the organisation

9) Every employee in my organisation has a responsibility to ensure that they abide by the information security policy

10) Every employee in my organisation is aware of their responsibility to abide by the information security policy

11) It is important to have regular communication between the IT department and employees to implement the security policy effectively

12) Regular feedback and updates on information security incidents are necessary to implement the information security policy effectively

13) It is easy to get information quickly if I have a system about

the information security policy

14) Having regular workshops/discussions about information security with security experts would help employees implement information security policy effectively

15) Rewards (such as, increasing salary, title, position, and certificates) would motivate me to implement my organisation's information security policy effectively

16) Sanctions (such as re-training, fines, monitoring) would encourage and motivate me to implement my organisation's information security policy effectively

17) My organisation should apply disciplinary procedures if employees do not implement my organisation's information security policy

18) Applying reward and sanction is an effective way of improving employee behaviour towards implementing my organisation's information security policy

Believe that information security policy is good thing

9. **To what extent do you agree with the following statements**
On a scale of 1-5 where 1= Strongly agree 2 = Agree 3= Neutral 4= Disagree 5= Strongly disagree

	1	2	3	4	5
1) Applying my organisation's information security policy will reduce security breaches	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2) Applying my organisation's information security policy will improve employee behaviour towards security management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3) Applying my organisation's information security policy is easy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4) It is desirable for my organisation to have an information security policy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5) Overall, I think it is a good idea for my organisation to have an information security policy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6) I believe having an organisational information security policy is good idea	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7) I believe an organisational information security policy is a waste of time	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8) I believe my organisational information security policy can reduce security breaches

9) Colleagues who are important to me think that implementing my organisational information security policy is important

10) My close friends think that implementing my organisational information security policy is important

11) My family think that implementing my organisational information security policy is important

12) I intend to implement my organisational information security policy

13) I want to implement my organisational information security policy

14) I am confident that I can implement my organisational information security policy

Please answer the following questions based on your behaviour at work

10. please state the extent to which you agree with the following statements On a scale of 1-5 where 1= Strongly agree 2 = Agree 3= Neutral 4= Disagree 5= Strongly disagree



	1	2	3	4	5
1) I regularly switch off my computer when I am away from it at work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2) I regularly change my computer access password at work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3) I would share my password with people I trust at work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4) I change my password if I think it has been compromised at work.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5) I keep a written note of my password stored securely at work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6) I check the source of software before downloading at work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7) It is Important to have antivirus software on my computer at work	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8) I regularly update antivirus software on my computer at work

9) I regularly back up my data at work

10) I would report to the manager if I saw anyone accessing someone else's personal online account at work

11) I routinely follow my organisation's information security policy at work

12) I routinely follow my organisation's information security risk management requirements at work

11. Training you currently receive in your organisation

	Every month	Every 3 month	Every 6 month	Every 9 month	Every year	Never
1) How often do you receive training on information security policy in your organisation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

12. please state the extent to which you agree with the following statements On a scale of 1-5 where 1= Strongly agree 2 = Agree 3= Neutral 4= Disagree 5= Strongly disagree



	1	2	3	4	5
2) We have regular training in how to respond to information security incidents	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3) The current information security training provided by my organisation is very effective	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
4) Every employee is adequately trained by my organisation to abide by the information security policy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5) the current information security training in my organisation provides a regular assessment of the my information security knowledge	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

13. Please state whether you consider these criteria important in developing an information security training session in general where the degree of importance

1= very important 2 = important 3= neutral 4= not very important 5= unimportant

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

6) It is important to undertake regular training to reduce information security breaches

7) Regular training will improve my knowledge to implement information security policy

8) Regular training is important to implement the information security policy effectively

9) Regular training in how to respond to information security incidents will improve employee behaviour towards security management

10) I believe an effective information security training programme will help me to implement my organisation's information security policy

11) I would feel confident about reducing security breaches if I attended information security training

12) Attending an effective information security training on a regular basis will lead to good security habits

13) Sharing experiences between the instructor and the participants in the training session will improve my information security knowledge

14) Understanding how to prevent organisational information security breaches in the training session will improve my knowledge

15) Understanding the practical impact of information security breaches in the training session will improve my information security knowledge

16) Regular assessment of my information security knowledge will improve my retention of it

17) Regular training sessions will help to reinforce my information security knowledge over time

18) Having the opportunity to express my point of view in the training session will help me to reinforce my understanding of information security

19) Regular feedback of my

knowledge in the training session will improve my information security knowledge

20) Using video to learn how to solve security breaches is important

21) Using simulation of information security breaches to show how they impact the organisation is important

22) Having an external IT trainer conducting the training is important

23) Having internal IT staff conducting the training is important

***14. 24) what are the top 3 factors that you would consider to be important in an information security management training programme (this can include content or medium)**

Appendix C: Training Information

A-C1: Letter for the Company for Training

26th April, 2012

Re: Information Security Policy – Training and Impact

Dear Sirs

Following the successful feedback in relation to the questionnaire conducted earlier in the year, I am pleased to inform you that your contribution to this study has successfully helped to achieve the first part of the study aims. Your support and positive contribution is much appreciated.

The initial results have helped to consolidate our understanding of the most effective factors that can help employees to implement their organisational InfoSec policies effectively. One of our findings shows that training is one of the important factors that can directly impact on employee behaviour regarding the implementation of InfoSec policy.

To push the study further and to support this claim, your empathy to permit some of your staff to participate in a carefully designed training programme would be appreciated. Participants will be provided with a complete one hour training programme that provides both; pre and post assessments of their knowledge and attitude towards InfoSec policy implementation. The training programme will be followed by simple assessment on the day then a following up consolidating part will be needed in three months' time. The aim is to confirm our findings and assess knowledge retentions.

The offered programme will be designed based on extensive literature reviews in this field aiming to maximise its effectiveness and knowledge retention. It is anticipated that the training programme will have a long term

positive outcome towards attitude and compliance with your organisational InfoSec policy.

As a thank you for your support and contribution, we will be happy to provide you with our recommendations and findings that can have an input to strategies related to your policies and help to achieve better long term compliance with them.

I hope you will be happy to contribute to the above proposal hence I would appreciate letting me have your existing InfoSec policy (if you have one in place). This will help me designing the training programme around your existing ones to maximise its positive impact on your company.

This study forms part of my PhD thesis at the University of Bradford, School of Informatics and Computing. The study is bound by the University of Bradford ethical policies governing data collection. Participants are assured of confidentiality and shall remain anonymous and no personal identifying information will be collected or used. If you have any questions or queries, please contact me or my supervisors: Dr Mumtaz Kamala, or Dr, Rana Tassabehji, m.a.kamala@bradford.ac.uk; R.Tassabehji@bradford.ac.uk; n.waly@bradford.ac.uk

Sincerely yours,

A-C2: Training Programme

Training Programme

One of the main effective mechanisms factors that the training aiming to establish at the beginning of the training is that generate interactive communication between the participant and the trainer. Allowing the participant to explain their different perspective and views, exchange of ideas and clearly understand the subject Fallowfield (2003).



Providing the participant with questions aiming to incorporate the communication techniques and attract their attention to the subject. Involving the participant in the training allowing them to draw a conclusion about what they going to learn.

Introduction

- ❖ Do you have security policy in your organisation?
- ❖ What is security policy means?
- ❖ Why it is important to have it?
- ❖ When and how to applied?
- ❖ What is the benefit of it?

Training Goals

State the purpose of the policy and the scope of it to motivate the participant to understand their responsibility and what they are required to do (Quinones, 1995). Explain what is the aim of it in order to justify the benefit of such policy in effective easy language.

Goals

- ❖ Take action
- ❖ Reduce risk
- ❖ Response effectively
- ❖ Prevent unwanted sharing
- ❖ Be aware of the consequence

- ❖ Let's change together
- ❖ Let's change our habit
- ❖ Let's be stronger and protective
- ❖ Let's make more effort
- ❖ Let's learn and practice good security habits

```

    graph LR
      A[Attitude towards Act or Behaviour] --> B[Behavioural Intention]
      C[Subjective Norm] --> B
      B --> D[Behaviour]
  
```

Training Objective

To use effective training techniques that will improve participant awareness, change their attitude, habit and enhance their motivation to learn. To transfer the knowledge and sustain information security management practise in the work environment. Satisfy participant needs with clear instruction to allow them to gain positive feeling about their learning experience (Smith 2008)

1. PRACTICE **2. HABIT**

What make our programme effective

3. TRANSFER

- ❖ Understand User believe, attitude and behavioural reasoning
- ❖ Standard policy, procedures objectives and mission
- ❖ Reasoning and logic statement
- ❖ Apply different learning style
- ❖ Fact and a real world example
- ❖ Reinforcement and hand on practise
- ❖ Visualisation, Feedback, assessment and
- ❖ On-going practise
- ❖ Encouragement and convincing techniques

Transfer skill to the work environment

To explore the importance of human factor and what influence their attitude to compliance with organisational security policy to show the appreciation of individual values. (Simpson and Wilson, 1999) To transfer the knowledge and sustain information security management practise in the work environment.

behaviour factors
(1: Believe)

3.TRANSFER

1.PRACTICE **2.HABIT**

- * **Fact:** thousand new malicious code threats coming out every day.
- * **Believe** that Information security is more than just policies
- * It is **on-going process that requires believe and changing behaviour from individual**

6

behaviour factors
(2: habit)

3.TRANSFER

1.PRACTICE **2.HABIT**

- * **Fact:** People remain with routines and habit longer than they should, even when a better or easier solution are exist and available.
- * **How To Break Bad Habits toward using computer!!!**
 - * Interest, challenge, commit, patience, report progress, repeat, and reward

7

behaviour factors
(3: Attitude)

3.TRANSFER

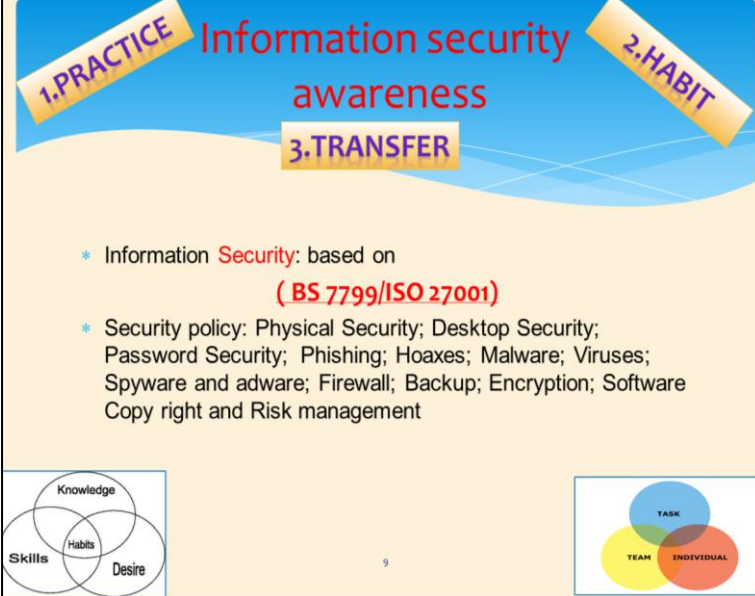
1.PRACTICE **2.HABIT**

- * **What is Attitude :** thinking, feeling, behaving
- * **Fact:** think about positive attitude, and behave in a positive manner to accomplish
- * **How to change attitude!!!**
 - * I can, I want to, I will, I have goal, and I will make effort

8

Content of security policy

Explore in simple language the topic of information security and covers in bullet-point what activities that needs from participant to perform for security controls to meet organisational objective



The slide features a blue header with the title "Information security awareness" in red. Three yellow banners with red text are positioned around the title: "1.PRACTICE" on the left, "2.HABIT" on the right, and "3.TRANSFER" in a central box below the title. The main content area is light yellow and contains two bullet points. The first bullet point states "Information Security: based on (BS 7799/ISO 27001)". The second bullet point lists various security policy areas: Physical Security; Desktop Security; Password Security; Phishing; Hoaxes; Malware; Viruses; Spyware and adware; Firewall; Backup; Encryption; Software Copy right and Risk management. At the bottom left is a Venn diagram with three overlapping circles labeled "Knowledge", "Skills", and "Desire", with "Habits" in the center. At the bottom right is a Venn diagram with three overlapping circles labeled "TASK", "TEAM", and "INDIVIDUAL". A small number "9" is centered at the bottom of the slide.

1.PRACTICE Information security awareness **2.HABIT**

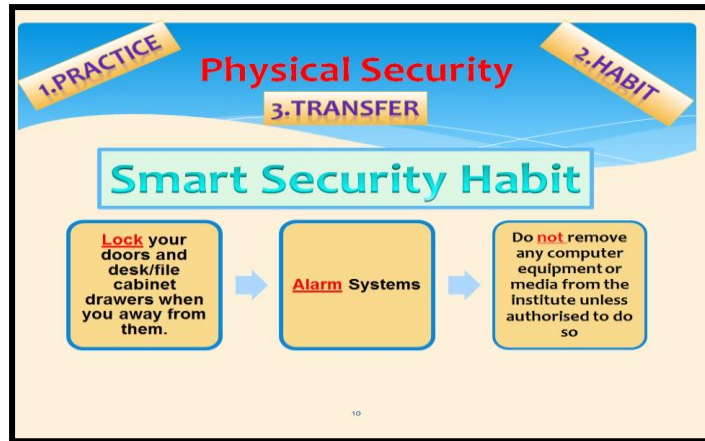
3.TRANSFER

- * Information Security: based on (BS 7799/ISO 27001)
- * Security policy: Physical Security; Desktop Security; Password Security; Phishing; Hoaxes; Malware; Viruses; Spyware and adware; Firewall; Backup; Encryption; Software Copy right and Risk management

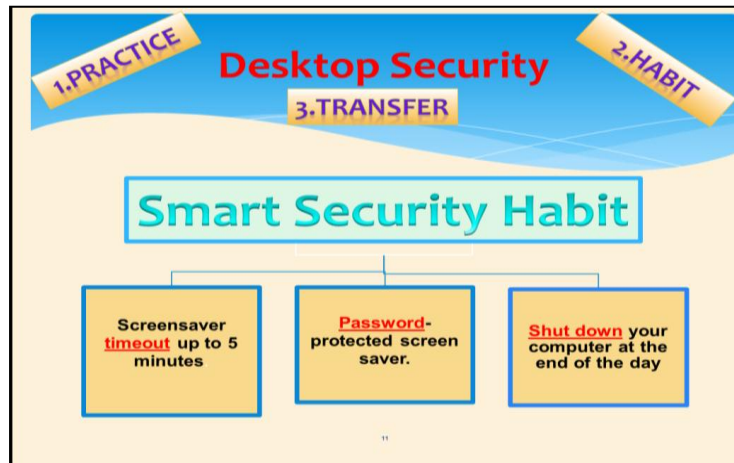
9

Physical security

Physical Security addresses actions you can take to protect buildings, property include locking doors and desk/file cabinet drawers. Physical security includes the protection of personnel, hardware, programs, network and data from physical circumstances and events that could cause serious losses or damage.



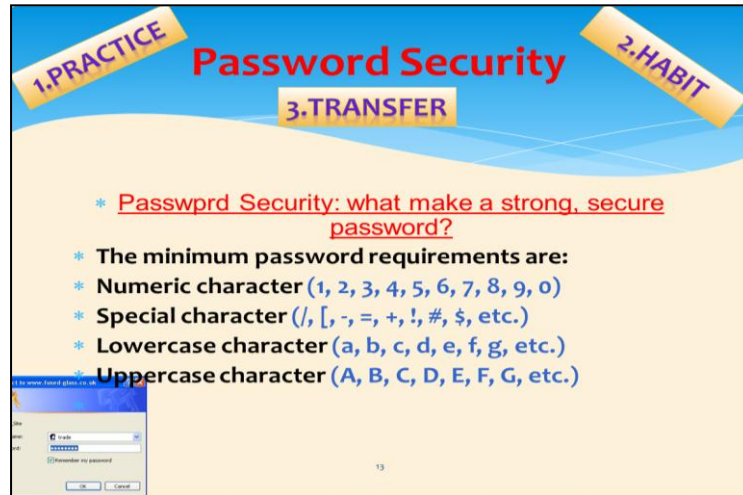
Desktop security



Password security

The password security section should consist of a strong, secure password or passphrase, with an emphasis on passphrases since they are harder to guess and to crack. Some of the methods and examples that are explained are: By taking a combination of letters and numbers and join them together to make password. e.g. Too late again can be spelled out with '2L8again'. Another example is: Using the first letter of each word also help to

build a good password, e.g. 'we spent too much at the fair last night' can be constructed into the password 'ws2matfln'.



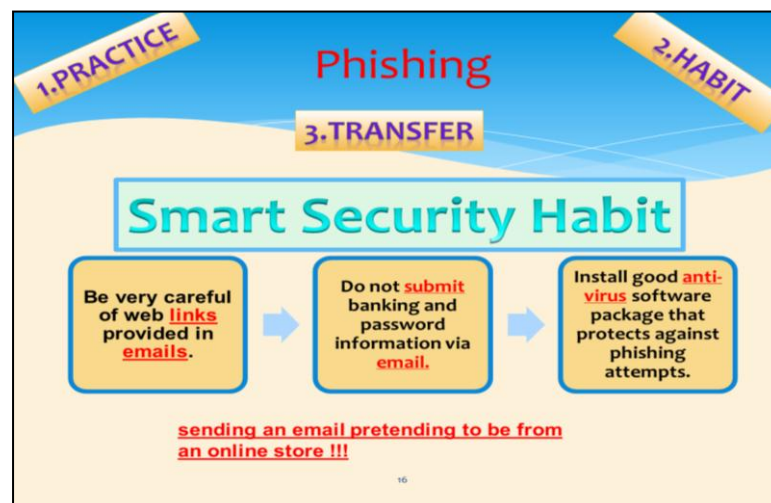
1.PRACTICE **Password Security** **2.HABIT**
3.TRANSFER

- * Passwprd Security: what make a strong, secure password?
- * The minimum password requirements are:
- * Numeric character (1, 2, 3, 4, 5, 6, 7, 8, 9, 0)
- * Special character (/, [, -, =, +, !, #, \$, etc.)
- * Lowercase character (a, b, c, d, e, f, g, etc.)
- * Uppercase character (A, B, C, D, E, F, G, etc.)

13

Phishing

Phishing address the act of sending an email portending to be from an online store (amazon, eBay) or an internet service. Phishing hackers use this technique to obtain personal information such as credit card number, bank pin number and social security numbers.



1.PRACTICE **Phishing** **2.HABIT**
3.TRANSFER

Smart Security Habit

Be very careful of web **links** provided in **emails**.

Do not **submit** banking and password information via **email**.

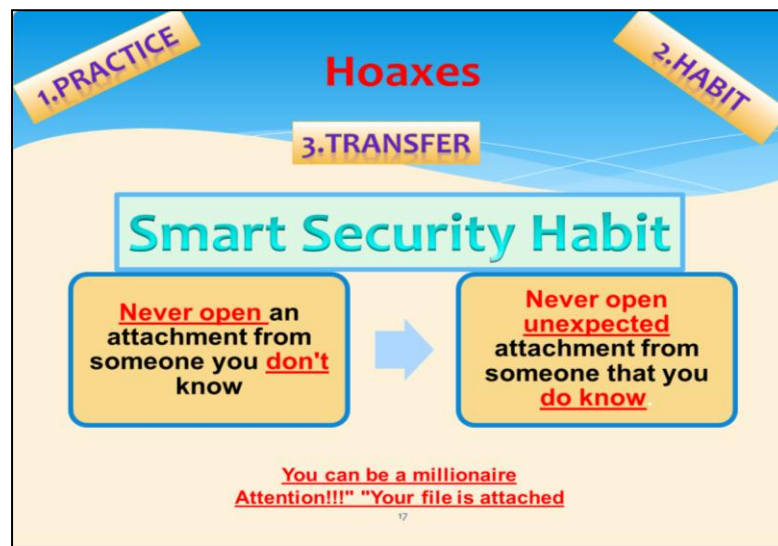
Install good **anti-virus** software package that protects against phishing attempts.

sending an email pretending to be from an online store !!!

16

Hoaxes

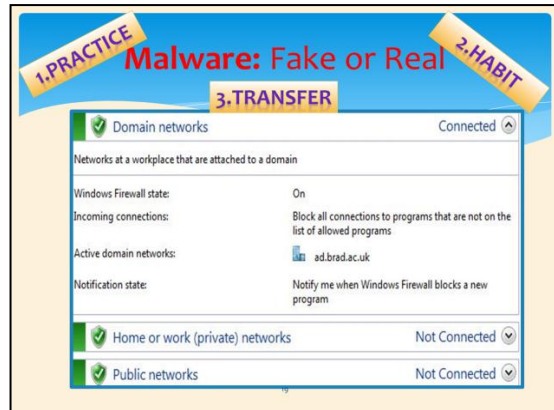
Hoaxes come in the form of a warning about a virus that can delete your hard drive or important system file. Hoaxes hackers use this technique as advertisement to ask you to contact everyone in your address book to warn them about viruses.



Malware

Malware is software designed to secretly access a computer system without the owner's informed consent. Malware include (viruses, worms, trojans, spyware and adware)

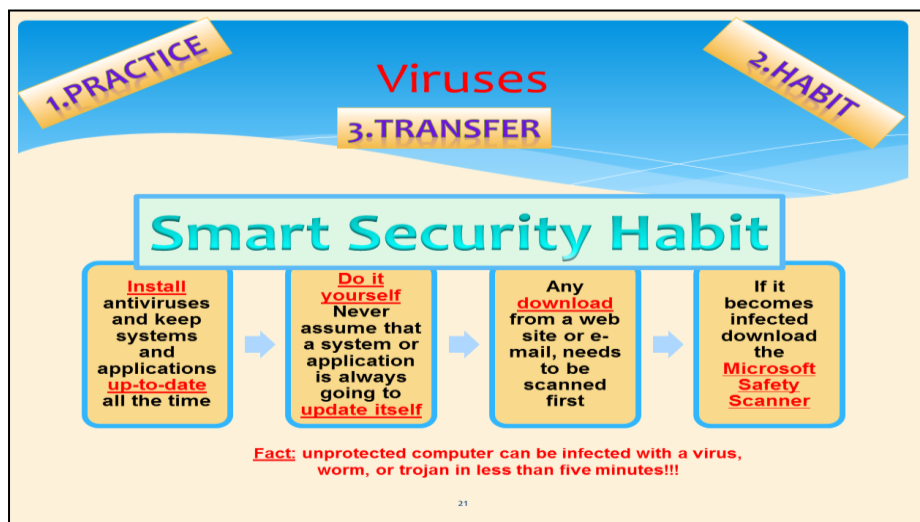
Difference between real and fake malware: Malware and fake antivirus are quite annoying, colorful and start randomly. Most real internet protection software is Microsoft certified. Real update program will download with owner permission.

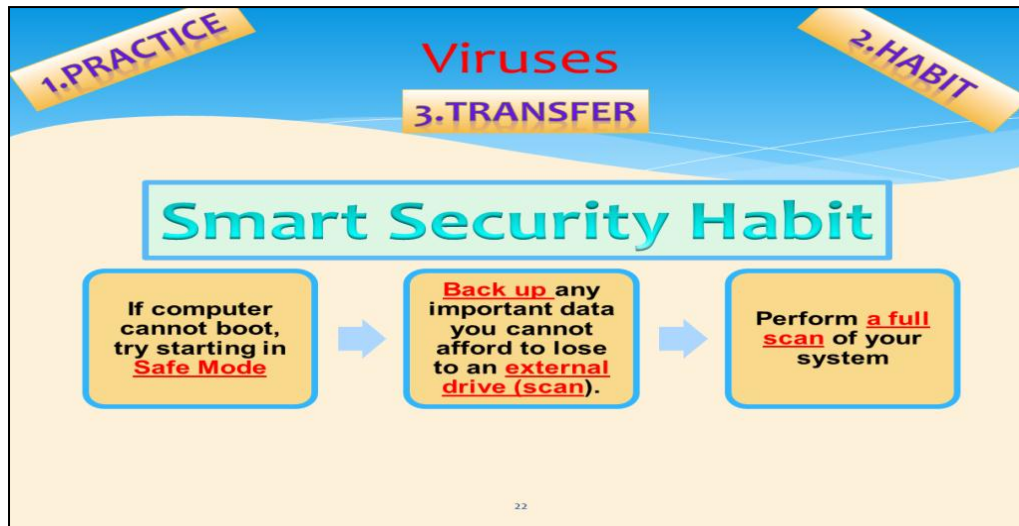


Viruses

Virus spread from one computer to another when user send file over a network or the internet, or carried it on a removal medium such as a floppy disc or CD.

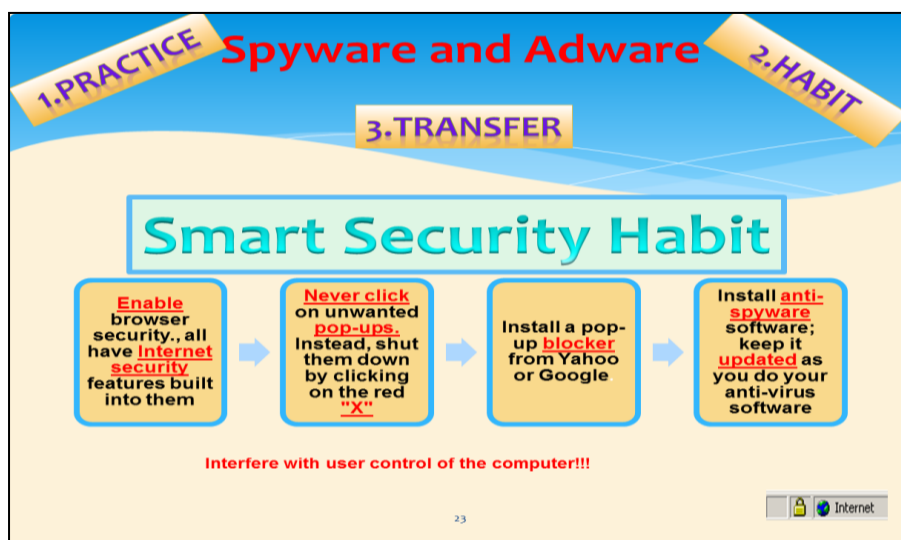
Fact: Recent statistics show that unprotected computer can be infected with a virus, worm or trojan in less than five minutes after being placed on a network (reference).





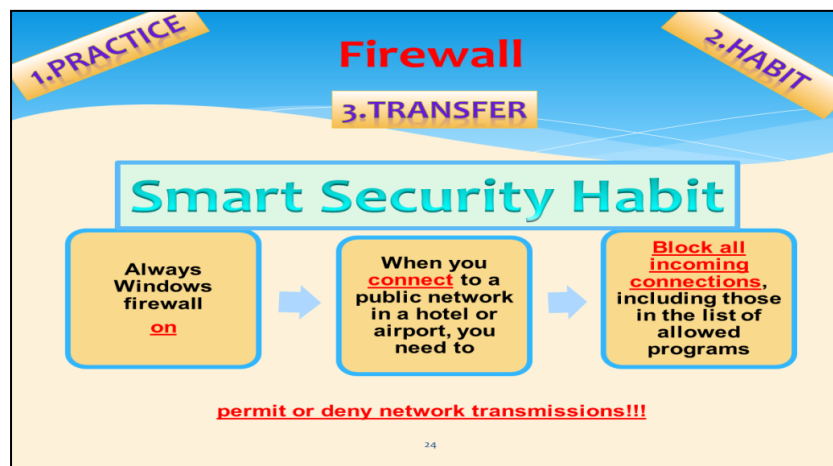
Spyware and Adware

Spyware and adware collect personal information from the site you have been visited. Spyware can interfere with user control of the computer, such as installing additional software, change computer setting, resulting in slow connection speeds. Spyware can be as simple as annoying pop-up that are meant to distract you or attract you to malicious site.



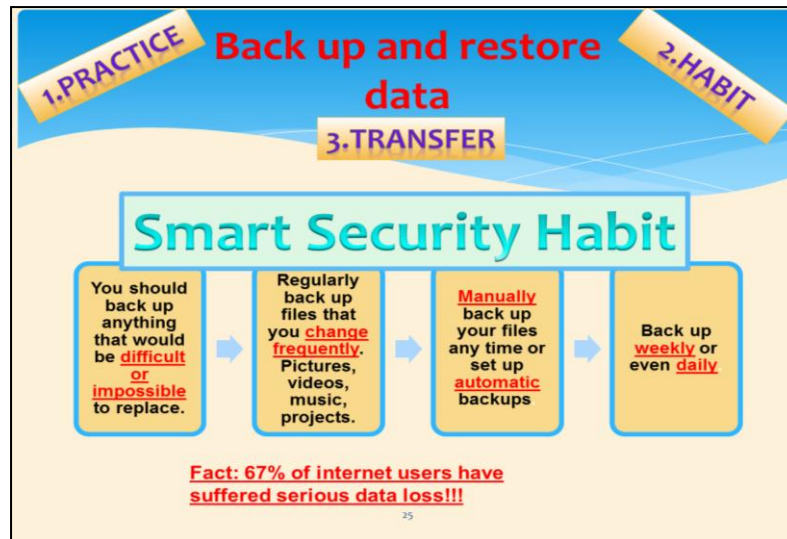
Firewall

Firewall is a device designed to permit or deny network transmissions based upon a set of rules. Firewall used to protect networks from unauthorized access. Prevent unwanted sharing of your file and computer resources. It also prevents applications on your computer from connecting to the internet. It also increases the difficulty for hackers to access your computer.



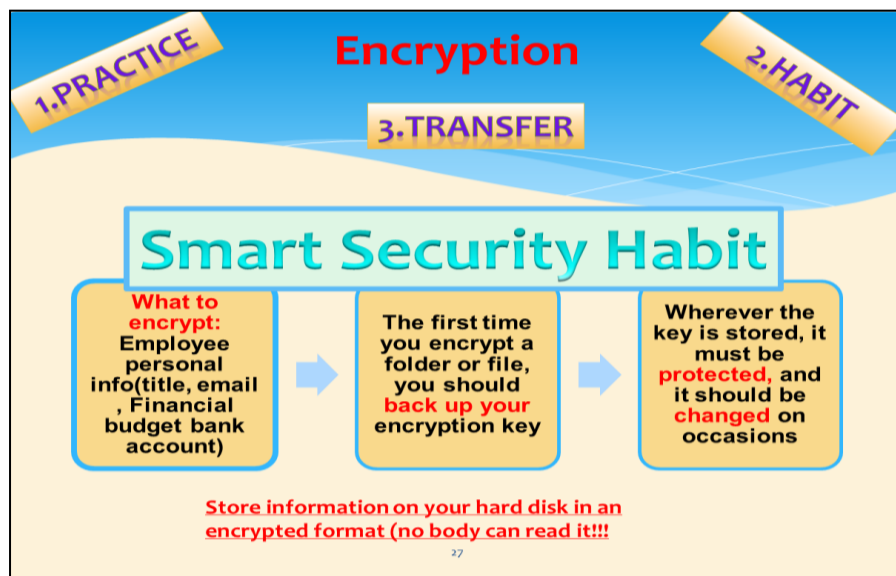
Backup and restore data

Backup is a copy of file that is stored in a separated location from the original. Purpose is to recover data as a reaction to data loss, or data deletion or corrupted data.



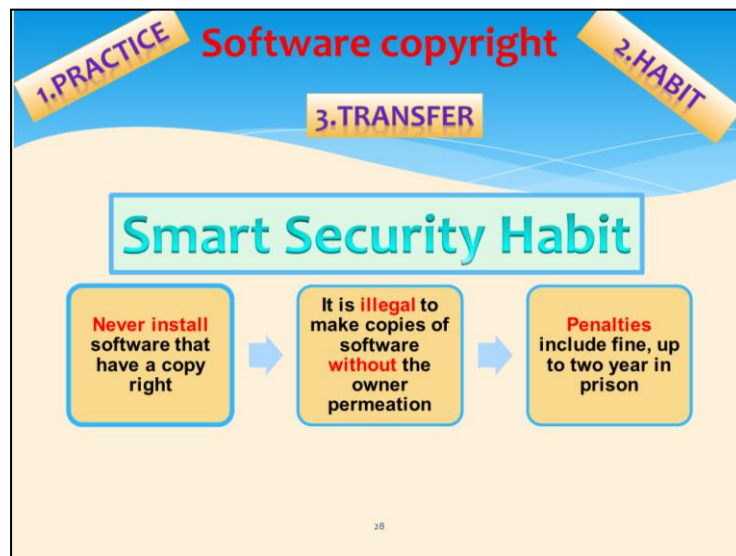
Encryption

Encryption is a way to protect folders and files from unwanted access. Encryption is a feature of windows that allows you to store information on your hard disk in an encrypted format.



Software copyright

Software is like any other property. The software company who develops the software keeps copy right with it and distributes by cost. When you purchase commercial software, you are paying for a license to use the software.




Risk assessment

The process of provides a report that describes the threat and vulnerabilities, measure the risk and provide recommendation for control implementation. It allows the ability to take action appropriately as quickly as possible to any incident.

1.PRACTICE **Risk assessment** **2.HABIT**
3.TRANSFER

- * **Risk assessment:** provides a report that describes the threats and vulnerabilities, measure the risk, and provide recommendation for control implementation.
- * Ability to take action appropriately as quickly as possible to any incidents



29

Disciplinary procedure

Exploring the important of the disciplinary procedure enhances their satisfaction to increase interest, motivation and improve participant behaviour (Stanton, 2005)

1.PRACTICE **Disciplinary procedure** **2.HABIT**
3.TRANSFER

- * **Example of reward:** Increase salary; bounce; extra break time; recognition by the manager; Certificate; trip; higher position; extra administrative right; good record.
- * **Example of sanction** Reduce salary; reduce break time; bad record; extend working time and task; more responsibility; monitoring.

30

A-C3: Final Assessment

Section One: Knowledge

1. Passwords should contain of both upper and lower case letters?

True: False: I do not know:

2. As long as I do not share my password, I don't need to change it?

True: False: I do not know:

3. If the systems administrator calls me asking for my password for system maintenance, it is OK to give it to him/her?

True: False: I do not know:

4. Switching off or locking or using screensaver protected my computer when I am a way from it?

True: False: I do not know:

5. I will only check the site of any software to download if I am not familiar with the source?

True: False: I do not know:

6. Backup my data, daily if necessary?

True: False: I do not know:

7. I am aware how when I am connected to a public network in a hotel or airport, I need to block all incoming connections?

True: False: I do not know:

8. I am aware of the different between real and fake malware message?

True: False: I do not know:

9. I think I have the ability to take appropriate action to any incidents that relate to Information security policy at work?

True: False: I do not know:

10. I am aware of the three elements of information security: confidentiality, integrity, and availability?

True: False: I do not know:

11. Do not attach a wireless USB unless permission has been granted?

True: False: I do not know:

12. All software are protected by copyright?

True: False: I do not know:

13. Viruses may be received as attachment, documentation programme or external disc or CD?

True: False: I do not know:

14. Information containing personal detail that no longer required must be disposed off?

True: False: I do not know:

15. Inappropriate use or downloading illegal material from the internet at work will result in disciplinary action?

True: False: I do not know:

Section Two: Attitude

Please state the extent to which you agree with the following statements, on a scale of 1-5 where:

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

16. I think I am aware of information security policy?

1 2 3 4 5

17. Security policy is important to protect the information in my organisation?

1 2 3 4 5

18. Good security policy is a key to good information security management?

1 2 3 4 5

19. Security policy is important to raise employee's awareness of security?

1 2 3 4 5

20. Information security policy can reduce security breaches?

1 2 3 4 5

21. Security awareness plays important factor in implementing security policy?

1 2 3 4 5

Section Three: Training

22. This training helped me to understand the need of implementing the organisational information security policy?

1 2 3 4 5

23. This training will help me complying with the information security policy in the future?

1 2 3 4 5

24. Because of this training I will comply with the organisational information security policy in the future?

1 2 3 4 5

25. Because of this training I have the knowledge to apply the organisational information security policy in the future?

1 2 3 4 5

26. The most effective part of the training has been?

You can select more than one:

Assessment

Communication

Satisfaction

Motivation

Feedback

Effective awareness

Reinforcement