Information Security Governance Implementation within the Mobile Device Environment

Celeste Phillips – PHLCEL001

A Dissertation presented to the

Department of Information Systems

University of Cape Town

In partial fulfillment of the requirements for the

Masters Degree in Information Systems

INF5005W

2/14/2014

1 DECLARATION

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this dissertation “How do organisations go about implementing information security governance within mobile device environments?” from the work(s) of other people has been attributed, and has been cited and referenced.
3. This dissertation “How do organisations go about implementing information security governance within mobile device environments?” is my own work.
4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

Signature:…….. **Date**: 14/02/2014

Full Name of Student: Celeste Phillips

Student Number: PHLCEL001

2 ACKNOWLEDGEMENTS

A heartfelt ‘Thank you’:

- To my supervisor, Irwin Brown, for his continuous support, guidance and for giving so generously of his time.
- To my research participants for their willingness to participate and contribute to this research.
- To my family and most of all, my husband, Colin Phillips, for allowing me the time to complete this dissertation.

3 ABSTRACT

Organisational information has been acknowledged to be a valuable asset which must be protected no matter where it is accessed from or how it is accessed. Mobile devices such as smartphones and tablets are becoming a popular means of accessing the organisation's information whether it is on a company-owned or personal mobile device. This has led to an increased awareness of potential risks to the organisation within the mobile device environment which requires organisations to be more vigilant with regards to information security governance. The objective of the research was, therefore, to investigate how organisations go about implementing information security governance within the mobile device environment.

The research was conducted at a Retail company where two mobile device implementations took place. The research philosophy was interpretive and the research strategy employed was a grounded case study which allowed theory to be developed using a combination of the grounded theory methodology and the case study method. The use of a mixed approach, deductive and inductive, allowed a conceptual framework to be developed from literature which was used as a sensitising device to start the data collection and analysis process. Qualitative data was collected from multiple sources such as semi-structured interviews and company documents.

The theory developed shows how organisations go about implementing information security governance within the mobile device environment. Mobile information security governance implementations are triggered by risks to company information, the company's mobility strategy and also the strongest concept in the study, the mobility audit. Once the mobile information security governance has been implemented, any changes or new proposals to the mobile environment cannot be implemented without the consideration of the newly implemented mobile information security governance. As a result of this, there are benefits to the organisation from a risk management perspective such as the mitigation of risks to the organisation's information. However, one of the most prominent consequences, as highlighted by this study, of remaining compliant with mobile information security governance is the impact on the satisfaction of the employees. The theory suggests that if organisations ignore the satisfaction of the employees while trying to protect the

organisation’s information, it may result in implications such as an interference with employee’s job roles, productivity and compliance with policy.

The theory also indicates that a close relationship exists between governance, risk management and compliance, all working together to ensure that a secure environment is provided for the organisation.

This research contributes to the understanding of how organisations may go about implementing information security governance within the mobile device environment and has highlighted issues that organisations may struggle with such as change management and mobile device fragmentation.

TABLE OF CONTENTS

1 DECLARATION i
2 ACKNOWLEDGEMENTS ii
3 ABSTRACT iii
4 INTRODUCTION 1
4.1 Background and context 1
4.2 Purpose 2
4.3 Gaps in literature 2
5 LITERATURE REVIEW 3
5.1 Corporate governance to IT governance to information security governance 3
5.2 History of information security 5
5.3 What is information security governance? 6
5.3.1 Information security governance themes 9
5.4 Why is information security governance important? 21
5.4.1 Information as a strategic business asset 21
5.4.2 Adherence to legal requirements 22
5.4.3 Risks to company information 22
5.4.4 Audit compliance 25
5.5 Implementing information security governance 26
5.5.1 Information security management programme 26
5.5.2 Using best practice to guide the implementation 28
5.6 Mobile devices in the workplace 29
5.6.1 Evolution of mobile devices 29
5.6.2 Bring your own device (BYOD) 31
5.6.3 Business implications of mobile devices 32
5.7 Summary of literature review 34
6 RESEARCH DESIGN 36
6.1 Research question/objectives 36
6.2 Research Method 36
6.2.1 Background to IS research 37
6.2.2 Purpose of Research 38
6.2.3 Ontology and Philosophy 38
6.2.4 Research Approach 40
6.2.5 Research Strategy 41
6.2.6 Data collection 46

6.2.7 Data analysis 49
6.2.8 Timeframe 52
6.2.9 Sample 52
6.2.10 Ethics 56
7 ANALYSIS AND RESULTS 57
7.1 Implementation one analysis 57
7.1.1 Drivers of mobile information security governance implementation 58
7.1.2 Provide secure environment 62
7.1.3 Mobile information security governance implementation 63
7.1.4 Employee Dissatisfaction 74
7.1.5 Ensure Compliance 78
7.2 Implementation two analysis 81
7.2.1 Drivers of new mobile technology implementation 81
7.2.2 Drivers of information security governance consideration 87
7.2.3 Implementation of new mobile technology 90
7.2.4 Provide secure environment 94
7.2.5 Ensure compliance 95
7.2.6 Employee Dissatisfaction 95
7.3 Combined view of implementations 97
7.3.1 Commonalities between both implementations 98
7.3.2 Storyline 99
7.4 Final grounded theory in relation to existing literature 106
7.4.1 Discussion and implications 108
8 LIMITATIONS AND FUTURE RESEARCH 111
8.1 Limitations 111
8.2 Future research 112
9 CONCLUSION 113
10 REFERENCES 115
11 APPENDICES 123
11.1 Appendix A – First interview guideline 123
11.2 Appendix B – Research permission letter 126
11.3 Appendix C – Cover letter sent to participants of implementation 1 127
11.4 Appendix D – Summary and letter sent to email participants of implementation 2 128
11.5 Appendix E – Descriptive level of detail for implementation one 130

INDEX OF FIGURES

FIGURE 1 - THE GARTNER INFORMATION SECURITY AND RISK GOVERNANCE MODEL (SCHOLTZ, 2011A) 7
FIGURE 2 - ISG CONCEPTS - (DE OLIVEIRA ALVES ET AL., 2006) 8
FIGURE 3 - A TAXONOMY OF INFORMATION SECURITY TECHNOLOGIES (VENTER & ELOFF, 2003) 10
FIGURE 4 - DOCUMENT HIERARCHY (STEVENS, 2007) 11
FIGURE 5 - INFORMATION SECURITY RESPONSIBILITIES MODEL (SCHOLTZ, 2011B) 14
FIGURE 6 - IT AUTHORITY LEVELS (KRITZINGER & SMITH, 2008) 18
FIGURE 7 - RISK MANAGEMENT PROCESS (HUMPHREYS, 2008) 23
FIGURE 8 - EVOLUTION OF MOBILE DEVICES (ERNST & YOUNG, 2012) 30
FIGURE 9 - UNISYS STUDY CONDUCTED BY IDC (BURT, 2011) 31
FIGURE 10 - INFORMATION SECURITY GOVERNANCE THEMES 35
FIGURE 11 - RESEARCH ONION (SAUNDERS, LEWIS, & THORNHILL, 2007) 37
FIGURE 12 - CYCLE OF DATA COLLECTION IN THE GROUNDED THEORY METHOD (URQUHART ET AL., 2010) 46
FIGURE 13 - CASE STUDY RESEARCH: DESIGN AND METHODS (YIN, 1994) 48
FIGURE 14 - THE CODING PROCESS (POZZEBON ET AL., 2011) 51
FIGURE 15 - RELATIONSHIP BETWEEN AUDIT AND RISKS 61
FIGURE 16 - DRIVERS OF MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION 61
FIGURE 17 - PROVIDE SECURE ENVIRONMENT 63
FIGURE 18 - RELATIONSHIP BETWEEN TIME PRESSURE AND TEAM DIVERSITY 65
FIGURE 19 - MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION 67
FIGURE 20 - CHANGE MANAGEMENT 73
FIGURE 21 – EMPLOYEE DISSATISFACTION 77
FIGURE 22 – THEORY DEVELOPED FROM IMPLEMENTATION ONE 81
FIGURE 23 - DRIVERS OF NEW MOBILE TECHNOLOGY INPLEMENTATION 86
FIGURE 24 - DRIVERS OF INFORMATION SECURITY GOVERNANCE CONSIDERATION 89
FIGURE 25 - IMPLEMENTATION OF NEW MOBILE TECHNOLOGY 93
FIGURE 26 – THEORY DEVELOPED FROM IMPLEMENTATION TWO 96
FIGURE 27 - COMBINED VIEW OF IMPLEMENTATIONS 97
FIGURE 28 - GUIDING PRINCIPLES FOR WRITING THE STORYLINE (BIRKS ET AL., 2009) 99
FIGURE 29 - PERSPECTIVE ONE: NO MOBILE INFORMATION SECURITY GOVERNANCE IN PLACE 100
FIGURE 30 - PERSPECTIVE TWO: INFORMATION SECURITY GOVERNANCE IN PLACE, NEW OR CHANGE PROPOSAL TO BE CONSIDERED 104
FIGURE 31 - STRIVING TOWARDS A SECURE ENVIRONMENT 107

INDEX OF TABLES

TABLE 1 - CASE DATABASE 48
TABLE 3 - DRIVERS OF MOBILE SECURITY GOVERNANCE IMPLEMENTATION 58
TABLE 4 - PROTECT COMPANY INFORMATION 62
TABLE 5 - MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION 63
TABLE 6 - CHANGE MANAGEMENT 67
TABLE 7 – EMPLOYEE DISSATISFACTION 74
TABLE 8 – ENSURE COMPLIANCE 78
TABLE 9 – DRIVERS OF NEW MOBILE TECHNOLOGY IMPLEMENTATION 82
TABLE 10 - DRIVERS OF INFORMATION SECURITY GOVERNANCE CONSIDERATION 87
TABLE 11 - IMPLEMENTATION OF NEW MOBILE TECHNOLOGY 90
TABLE 12 - PROVIDE SECURE ENVIRONMENT 94

4 INTRODUCTION

4.1 BACKGROUND AND CONTEXT

Organisational business processes are driven by information which involves employees at all levels of the organisation from the lowest levels to the highest levels. Today, information is used to gain competitive advantage and has grown to become the lifeblood of many organisations (Von Solms & Von Solms, 2006; Von Solms & Von Solms, 2005; Posthumus & Von Solms, 2004). Information, therefore, needs to be protected so that the impact of threats are minimised. Threats such as social engineering which is used to commit fraud seem to be on the increase (de Oliveira Alves, da Costa Carmo, & de Almeida, 2006) and since the use of information systems inherently has risks (Williams & Andersen, 2001), information security governance (ISG) is recommended as being vital to addressing all these risks (Von Solms, 2006). Simultaneously, the benefits and value that can accrue from having secure information systems should be recognised (Williams & Andersen, 2001). Information needs to be protected so that business opportunities are maximised and that the business continues to run smoothly (de Oliveira Alves et al., 2006).

The advancement of technology exposes company information in different ways since the line between the work environment and personal life has merged with communication options such as instant messaging, social media sites and video conferencing (Cisco, 2008) used beyond traditional email for communication (Gordon, 2007). In the past, organisations would normally provide employees with the necessary devices such as laptops and smartphones to do their work. Today, people are more tech-savvy and may find that the equipment that the companies provide as obstructive, officious and even old-fashioned. The chances of employees bringing their own devices to work have become more and more likely. Employees generally feel like they are more productive with their own smartphones, tablets and laptops because they have chosen it themselves, rather than using devices that the organisation obliges them to use (Mansfield-Devine, 2012). This concept referred to as “Bring Your Own Device (BYOD) “is the practice of employees bringing personally owned mobile devices (e.g., smartphones, tablets, and laptops) to their place of

work, and using those devices to access company resources such as email, file servers, and databases" (The Security Executive Council, 2013, p.1). Traditionally, information needed to only be protected on company assets, now organisations need to ensure the protection of company information on the personal mobile devices of employees as well.

4.2 PURPOSE

Until recently, businesses have been relaxed about the information security risks on these mobile devices (Hart, 2013) but in order for BYOD implementations to be successful, the unique issues presented with BYOD must be considered and addressed in light of existing data privacy, confidentiality and acceptable use practices (The Security Executive Council, 2013). Effective governance must be established as failing to do so can have serious implications. Sufficient rigour must be applied to safeguard the organisation which is done by means of implementing information security governance (Moulton & Coles, 2003).

The objective of the research was to determine how organisations go about implementing information security governance within the mobile device environment.

4.3 GAPS IN LITERATURE

A global information security survey conducted by Ernst and Young (2012) shows an increase in the number of external attacks noticed by respondents from 41% in 2009 to 71% in 2011 and to 77% in 2012 as well as an increase in internal vulnerabilities. The survey suggests that only a few organisations are keeping up with an ever-changing risk landscape (Ernst & Young, 2012) due to technological advancements such as mobile computing. Information security governance ensures that the confidentiality, integrity and availability of the company's electronic assets are maintained (Von Solms, 2006).

Literature on how organisations go about implementing information security governance in the context of the mobile environment and the "BYOD" phenomenon is important and highlighted by a 2012 trend survey which reported that "nearly half of companies that permit BYOD reported experiencing a data or security breach as a result of an employee-owned device accessing the corporate network" (Harris, 2012,

p. 4). These organisations have reacted to these security breaches by installing security software, restricting data access rights or completely revoking BYOD privileges (Harris, 2012). According to the McAfee mobile and security report “four in 10 organizations have had mobile devices lost or stolen and half of lost/stolen devices contain business critical data, such as customer data, corporate intellectual property and financial information” (as cited in Li, Clarke, Cowan, Papadaki & Dowland, 2011, p. 1).

Kotulic and Clark (2004) agree that information security may be one of the most critical areas for research since it is necessary for supporting the viability of the organisation. It is especially critical within the BYOD phenomenon since organisations interviewed as part of the 2012 trend survey report widely agreed that the growth of BYOD is inevitable in future and that senior management are ready to invest in making the implementations as smooth as possible even though there is an understanding of the possible risks (Harris, 2012).

The next section discusses the literature review followed by the research design, timeline, analysis and results, limitations and future research and, lastly, the conclusion.

5 LITERATURE REVIEW

The literature review starts by discussing the movement from corporate governance to IT governance to information security governance. This is followed by a brief history of information security, a discussion on what information security governance is, why information security governance is important, implementing information security governance using best practices and lastly, mobile devices in the workplace.

5.1 CORPORATE GOVERNANCE TO IT GOVERNANCE TO INFORMATION SECURITY GOVERNANCE

Corporate governance is relied on by CEOs and senior managers to ensure that the business is able to respond to internal and external pressures (Saetang & Haider, 2011). In the past, few board members understood that information assets reside in various applications in the infrastructure and that many business decisions rely on the information contained in these assets (Short & Gerrard, 2009). Many are not

aware of how much the continuing operations of their organisation rely on IT (Nolan & McFarlan, 2005) since it is difficult to isolate and review because the use of IT is often embedded within other processes as systems cross internal organisational boundaries (Coen & Kelly, 2007).

Many organisations failed financially due to an excessive focus on return on investment (e.g. Worldcom and Enron). Organisations have had major data breaches or theft due to improper storage of data, such as CardSystems Solutions. Organisations have realised their limitations, such as not having a backup system, as a result of their computer system failing (e.g. Tokyo Stock Exchange) (Raghupathi, 2007). This led to a shift in focus to the concept of IT governance in the nineties even though the need for guidance on the use of IT was required since the early days of computing (Simonsson, Lagerstrom, & Johnson, 2008). An important purpose of IT governance is to ensure that information systems are secure by effectively controlling risk. The integration of computers into aspects of everyday life and the increase in the frequency of security breaches or cyber attacks indicate the growing importance of information security governance (Xiaomeng, Bolzoni, & Van Eck, 2007).

The Sarbanes-Oxley Act requires that information contained in annual reports is signed off by the board. Chief executive officers (CEOs) and chief financial officers (CFOs) need to be able to demonstrate that their organisations have proper internal controls (Von Solms, 2006) and attest to the financial reports being accurate as stated in section 302 (Na-yun, Robles, Sung-Eon, Yang-Seon, & Tai-hoon, 2008). The increase in security breaches and the legislative requirements has resulted in security aspects of information such as the security policies, procedures and security controls being audited since it seems like a futile exercise to audit organisations financial accounts without verifying that the information is adequately and appropriately secured (Vroom & Von Solms, 2004). If the systems maintaining the data are not secure, it is hard to signoff the validity of the data (Von Solms, 2006) and, therefore, business managers need to accept the responsibility and accountability of information security.

5.2 HISTORY OF INFORMATION SECURITY

Dlamini, Eloff and Eloff (2009) state that information security during the computer age dates back to the 1940s when the first computers came into existence, followed by the time of mainframe computers. The only security issues that needed to be considered were that only privileged computer operators were permitted to have access and that the computers and storage media were not damaged by outsiders or stolen, but the data was safe. During the early 1970s dumb terminals enabled multiple users to have access to one computer which posed a risk to data because unauthorised people may have been able to access to it. Physical security was no longer enough, so user identification and authentication was introduced. Later networks and multi-user systems were introduced with the mini computer which led to access controls to prevent users from interfering with one another's workspace (Dlamini et al., 2009). This marked the first phase of information security referred to by Da Veiga and Eloff (2007) and Von Solms (2006) which was characterised by the "technical people" only using technical measures such as firewalls, biometrics and passwords to mitigate threats to information and to secure the IT environment. Information security was only seen as a technical issue that the technical experts needed to resolve (Von Solms, 2006).

It soon became apparent that management needed to become involved (Da Veiga & Eloff, 2007) and the importance of policies was recognised (Von Solms, 2006). Information security then became incorporated into organisational structures (Da Veiga & Eloff, 2007). This second phase was marked by management involvement and the technical protection mechanisms mentioned earlier continuing in parallel (Da Veiga & Eloff, 2007). The third phase related to creating a security culture within the organisation (Da Veiga & Eloff, 2007) since people have been recognised as often being the weakest link in security and not the expected answer of some "older" technology that no longer meets the requirements of the security environment (Bresz, 2004). Information security had to become a part of an employee's job so that it becomes a way of life (Da Veiga & Eloff, 2007). Even though it was realised years ago that management's security consciousness and corporate culture needs to be addressed (Williams & Andersen, 2001), past studies in information security consistently report that the awareness of managers and users is lacking and a major obstacle (Rhee, Ryu, & Kim, 2012). A South African information security survey

conducted in 2011 confirmed that the overall lack of commitment from senior management to information security continues to be challenging (Wolfpack, 2011).

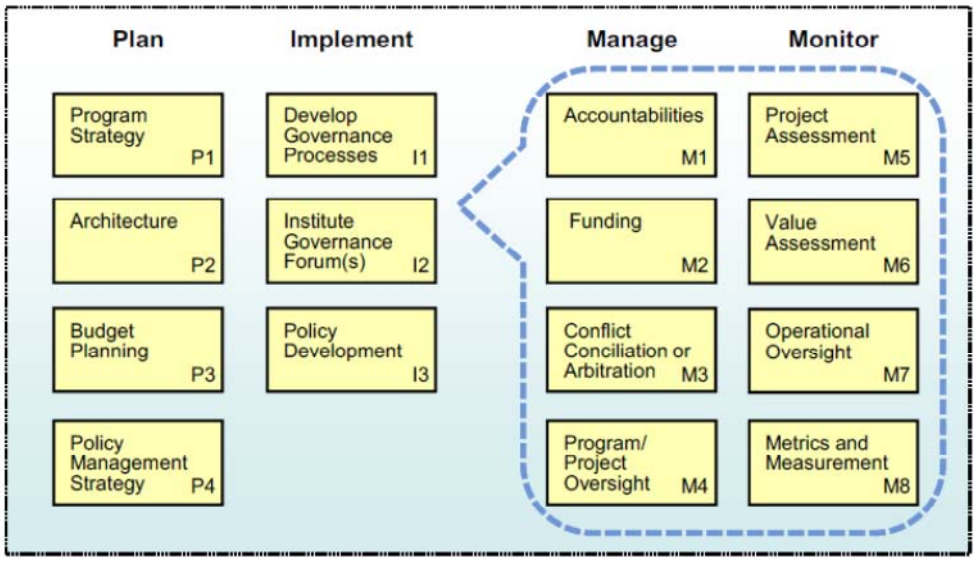
The fourth phase is the realisation of the crucial role that information security governance plays and its development (Von Solms, 2006). Dlamini et al. (2009) warns that attackers have matured and no longer attack machines but target people for financial gains resulting in risks such as social engineering, fraud, identity theft and phishing all of which are the key drivers of this phase of information security governance (Da Veiga & Eloff, 2007).

5.3 WHAT IS INFORMATION SECURITY GOVERNANCE?

Information security has received great attention with the development of IT governance. Many uncertain factors resulting in damages to the organisation are difficult to quantise after their occurrence. An important purpose of IT governance, therefore, is to ensure that information systems are secure by effectively controlling risk (Jian, Wei-hua, & Wen-jing, 2011). Information security is concerned with the integrity (ensuring accuracy of information and processing methods), confidentiality (ensuring authorised access) and availability (ensuring access to information and assets by authorised users only) of the data that are contained in computer systems and the safeguarding thereof (Xiaomeng et al., 2007).

Information security governance is defined as “the processes that ensure the requisite actions are taken to protect the organization’s information resources, in the most appropriate and efficient manner, in pursuit of its business goals” (Scholtz, 2011a, p.2). Figure 1 depicts it is as having the following macro processes:

- Planning
- Implementation
- Management and
- Monitoring (Scholtz, 2011a).



Source: Gartner (March 2011)

FIGURE 1 - THE GARTNER INFORMATION SECURITY AND RISK GOVERNANCE MODEL (SCHOLTZ, 2011A)

The term information security governance (ISG) has also been described as “the process of how information security is addressed at an executive level” (Posthumus & Von Solms, 2004, p.639). Other authors have not only defined it as “the act of directing and controlling an organisation aligned with the strategy and business objectives” but includes the following to the definition, “establishing and retaining a culture of information security, optimising the related processes (based on indicators and learned lessons), and assigning activities to the most competent people to perform the necessary actions” (De Oliveira Alves et al., 2006, p.72). This definition is depicted in Figure 2. The authors have also mentioned that all these actions need to be supported by the board.

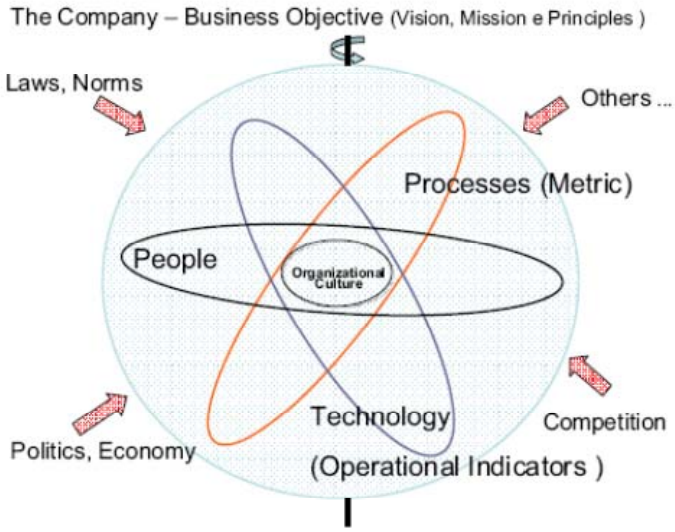


Figure 2. ISG concepts

FIGURE 2 - ISG CONCEPTS - (DE OLIVEIRA ALVES ET AL., 2006)

Moulton and Coles, (2003, p. 581), however, only refer to it as being "the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems" and explicitly excludes

- audit which ensures the proper establishment and functioning of governance processes,
- security operations which are the security administrative activities that are performed on a day to day basis and
- security developments such as meeting security objectives by creating new processes).

Harris (2007, p.74) describes it as follows: "Security governance is all the tools, personnel, and business processes necessary to ensure that the security implemented meets the organisation's needs. It requires organisational structure, roles and responsibilities, performance measurement, defined tasks and oversight mechanisms".

Von Solms (2001), however, suggests that information security governance is but one dimension of information security as a whole which has to do with the way that information is structured and organised in a company. This dimension is completely separate from the policy dimension or awareness dimension or any of the other dimensions mentioned and should all work together to ensure a secure environment.

An integrated view which synthesises aspects from all the definitions by
Von Solms (2006, p. 167) states that information security governance consists of “

- the management commitment and leadership,
- organizational structures,
- user awareness and commitment,
- policies, procedures, processes,
- technologies and
- compliance enforcement mechanisms,

all working together to ensure that the confidentiality, integrity and availability (CIA) of the company’s electronic assets (data, information, software, hardware, people, etc.) are maintained at all times”.

The researcher has adopted this definition and further elaborates on each aspect of the definition in the sub-sections, technologies (5.3.1.1), policies, procedures and processes (5.3.1.2), establishing and retaining a security culture (5.3.1.3), organisational structures (5,3,1,4), roles and responsibilities (5.3.1.5), awareness (5.3.1.6) and lastly, compliance (5.3.1.7).

5.3.1 INFORMATION SECURITY GOVERNANCE THEMES

5.3.1.1 TECHNOLOGIES

Information security technologies are used to secure information at the application, host and network level. These technologies such as the ones depicted in Figure 3 provide countermeasures for security problems such as hackers sending malicious code to servers connected to the internet causing the servers to fail. The taxonomy is based on whether the specific technology is proactive, meaning that measures are taken to secure data before a security breach occurs, or reactive meaning that measures are taken immediately to secure data as soon as there is a detection of a security breach (Venter & Eloff, 2003). Levine (2005), however, states that an important aspect of data security solutions is that it should be transparent to the user. A user wanting to take a memory stick home to complete a work related document should not be stopped but at the same time it should be possible to lock down or to wipe the memory device should the user lose it.

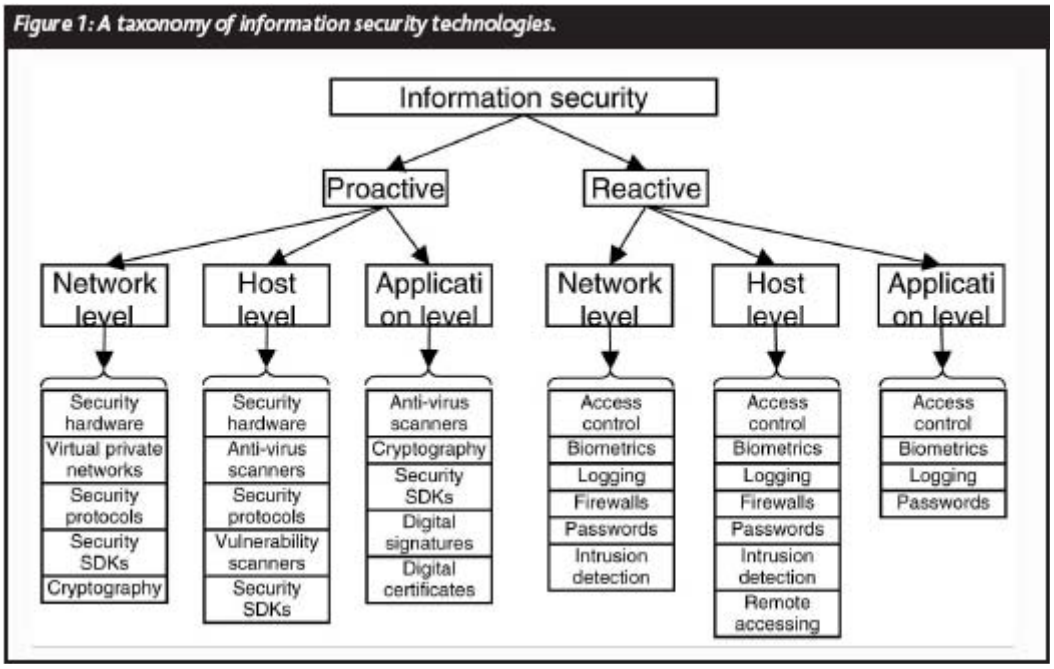


FIGURE 3 - A TAXONOMY OF INFORMATION SECURITY TECHNOLOGIES (VENTER & ELOFF, 2003)

This part of security governance also referred to as information security operational management, includes activities such as firewall management, which sets the rights on firewalls, and identification and authentication management, which is the adding, deleting and changing of usernames from the database, has thus far always been well understood (Von Solms, 2005b). These technical aspects are vital (Dhillon & Backhouse, 2000) but the non-technical aspects such as policies, awareness and compliance enforcement mechanisms have been recognised as pivotal to good information security governance (Von Solms, 2005b). The next sections, therefore, discusses the non-technical aspects of information security governance.

5.3.1.2 POLICIES, PROCESSES AND PROCEDURES

The environment within an organisation influences the beliefs and attitudes of employees. Senior management has the power to actually change the culture of an organisation and, therefore, it is important for management to articulate the vision of the organisation in terms of information security. One way of doing this is via a formally agreed upon corporate information security policy which will demonstrate the dedication of senior management to information security (Thomson, Von Solms, & Louw, 2006).

The development of documentation such as policies, procedures, standards and guidelines are recommended as a key factor for the implementation of information

security (Da Veiga & Eloff, 2007). Stevens (2007) suggests that a document hierarchy is established as displayed in Figure 4 which can be used as a communication tool which explains which documents are applicable to senior executives, business managers, end users and other stakeholders. This structured approach improves awareness and compliance because the stakeholders are able to access documents that are applicable to them and they do not need to read unnecessary lengthy detailed documents (Stevens, 2007).

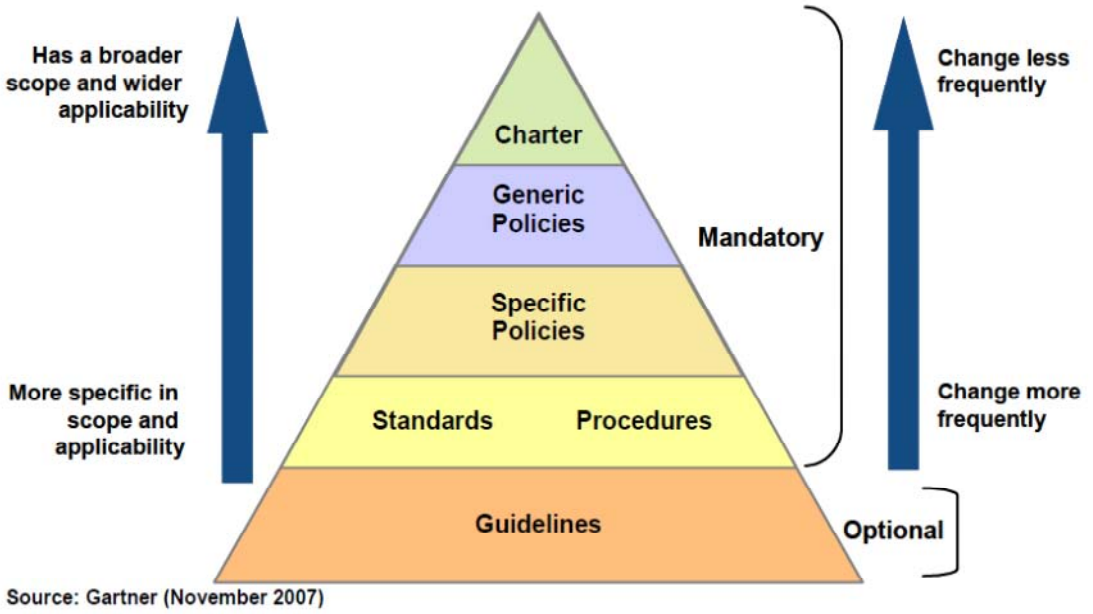


FIGURE 4 - DOCUMENT HIERARCHY (STEVENS, 2007)

Developing proper security policies for risk mitigation is regarded as part of security governance (Mishra & Dhillon, 2006) which define rules on how an organisation wishes to operate and also clear statements on approaches to ensure the protection of information assets (Ward & Smith, 2002). It includes security objectives as well as the methods of achieving those objectives (Karyda, Kiountouzis & Kokolakis, 2005). Walton (2002) also recognises that the mitigation of risks can only be achieved through an information assurance programme that is built on a solid strategic foundation defined by policy and not merely the implementation of malicious code prevention, firewalls, incident response or any other tactical countermeasures. The emphasis should not just be on these technical measures but security should rather be viewed as an ongoing process in which organisations take on the mindset that security policies will evolve over time to cater for evolving security vulnerabilities and attacks (Levine, 2005).

Ward and Smith (2002), however, highlights that the dissemination of the policies are equally important and is the first step towards providing an understanding for the need for security. Despite the common practice of developing and using security policies, when implementing the security policy often the goals are not accomplished even though information security management best practices and guidelines are available (Karyda et al., 2005). Organisations are still at risk because their information security policies are not followed by their employees (Siponen, Mahmood, & Pahnila, 2009). Ordinary employees who don't always understand all the risks are not the only ones guilty. Computer security professionals that attended the RSA 2002 conference participated in an informal survey which showed that 91% of them break their own company policies (Hinde, 2002); this is a serious threat to the organisation (Siponen et al., 2009) and indicates that information security governance programmes fail as a result of not addressing the beliefs, individual values and the means of encouraging the conformity with the organisation's policies (Mishra & Dhillon, 2006).

The following theme, therefore, discusses the establishment of a security culture within the organisation.

5.3.1.3 ESTABLING AND RETAINING A SECURITY CULTURE

People are vital to the success of any organisation (Vroom & Von Solms, 2004) and are extremely important in the role as frontline defence of the organisation (Dhillon, Tejay & Hong, 2007) but they have also been referred to as the weakest link when it comes to information security (Bresz, 2004; Vroom & Von Solms, 2004).

The risk of fraud being committed using social engineering seems to be increasing (Von Solms, 2006); employees often fall prey to hackers and their social engineering ploys (Dhillon et al., 2007). The amount of security incidents by employees inside the organisation exceeds the amount of security breaches with outsiders according to the 2001 information security industry survey; this behaviour is unacceptable (Vroom & Von Solms, 2004). This has resulted in the realisation by senior management that the information security problem cannot solely be solved by technical means. High level strategic decisions need to be made to ensure that all the users of the organisation are aware of the possible risks because the human side of using IT

systems by employees, customers and clients can cause serious risks irrespective of the amount of money that is spent on technical measures (Von Solms, 2006).

Vroom and Von Solms (2004) argue that in order to change the culture of an organisation to a more secure society, not only should the behaviour of the individual be changed but it needs to be changed at the group level, which is made up of individuals and also develops unique characteristics which should be examined, as well as at the formal organisational level. The development of a security culture requires a security consciousness that needs to be created amongst employees through a set of norms, values and beliefs which results in a unique character of the organisation which constitutes its culture (Mishra & Dhillon, 2006).

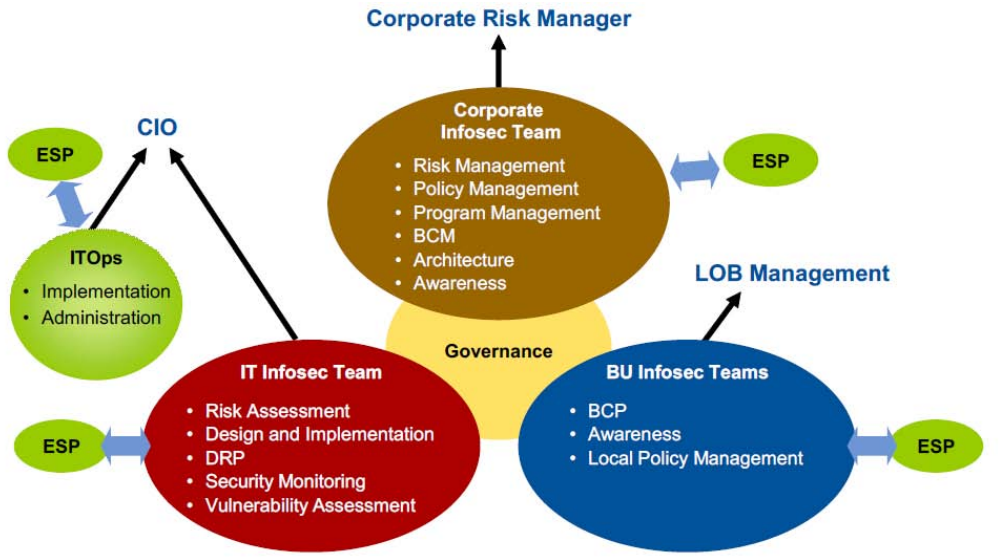
Vroom and Von Solms (2004) describe an utopian information security culture as one where the guidelines of the organisation are followed by the employees voluntarily as part of their second nature. An example provided by the authors describe that employees automatically backup their laptop files on the first Monday of every month because it is part of the organisation's culture. These behavioural aspects of information systems security governance have been neglected since more research is done with regards to the technical aspects yet it is recognised as an integral part of an information systems security governance program (Mishra & Dhillon, 2006).

5.3.1.4 ORGANISATIONAL STRUCTURES

The importance of the structure and organisation of the information security within an organisation is essential for the success of an information security governance plan. Several codes of best practices for information security management stress the importance of having a proper information security organisational structure which includes the creation of an information security forum (Von Solms & Von Solms, 2004). McMillan and Scholtz (2010) suggest that the information security governance forum should consist of representatives from mid-level to senior-level management from lines of business, IT, audit and risk.

Scholtz (2011b) recommends the distribution of the responsibilities for security functions via the organisational functions depicted in Figure 5 as follows:

- The organisation wide strategic processes such as policy management, program management, risk management and business continuity management is the responsibility of the strategic corporate function.
- Security processes such as technical architecture design, vulnerability assessments and disaster recovery together with oversight processes such as incident monitoring and policy compliance are the responsibility of the IT security function.
- Technology implementation, configuration and administration activities are the responsibility of the IT security operations function.
- Local business continuity planning, awareness, training and policy management are the responsibility of business unit security functions.
- Maintaining clear accountability, authority, responsibility and budget for information security is the responsibility of the governance function.



BCM = business continuity management; BCP = business continuity planning; BU = business unit; DRP = disaster recovery planning; ESP = external service provider; Infosec = information security; ITOps = IT operations; LOB = line of business

Source: Gartner (June 2011)

FIGURE 5 - INFORMATION SECURITY RESPONSIBILITIES MODEL (SCHOLTZ, 2011B)

This corporate information security team, depicted in Figure 5, within the organisational structure reinforces the involvement of the business in information security governance and that it is not just an IT function. The fact remains, however, that barriers for the creation of the structure recommended in Figure 5 still exist, which prevents or provides resistance to an information security governance programme's development, such as the fact that it still continues to be seen as an operational component of IT (Johnson & Hale, 2009).

Williams (2007), however, states that one holistic entity should be created which is an integration of all the different functions that have been previously responsible for aspects of security. Whenever any threats to corporate information or assets arise within the organisation, this entity will be capable of recognising, preventing and even reacting to them. An example supplied is the bringing together of more than 530 employees from the IT, corporate and physical security divisions of British Petroleum (BP) in order to protect the organisation globally by devising plans. The plan of linking physical security to IT security will enable the monitoring of employees who have logged onto their workstations against whether the employees have actually physically entered the building (Williams, 2007).

5.3.1.5 ROLES AND RESPONSIBILITIES

Information security is everyone's responsibility from the general members of staff all the way up through all levels of management to the CEO and board of directors (Humphreys, 2008) but if all employees involved do not understand their roles and responsibilities, the organisation will not be able to protect the integrity, confidentiality and availability of its information (Thomson et al., 2006). It is, therefore, important that people understand the protection available to them when faced with threats (Furnell & Clarke, 2012) and also when they are the ones causing the threat to the organisation. Willison and Warkentin (2013) refer to employee violations which may be passive such as employees who are poorly trained, careless, unmotivated or who accidentally enter incorrect data values. Examples of such behaviour are the failure to change passwords regularly, failure to shred sensitive documents, delays in making data backups or failure to select strong passwords (Willison & Warkentin, 2013). Employees may not understand that these actions may result in harm to the organisation without them specifically intending to do so therefore, Williams and Andersen (2001) agree with the International Federation of Accountants that clearly communicating individual roles, responsibility and authority is a major activity. All interested parties should be involved but ultimately the responsibility lies at the board level (Williams & Andersen, 2001). They should have an understanding of why information security needs to be governed and that they also have several responsibilities to ensure that information security governance is in place (Williams & Andersen, 2001).

5.3.1.5.1 STAKEHOLDERS

A stakeholder is any individual or group such as customers, suppliers, employees, stockholders, governments and other groups who may have an affect on or who can be affected when an organisation's objectives are either achieved or not (Clement, 2005). The idea is that organisations will be successful in performance such as stability, profitability and growth if they practice stakeholder management. Anyone who has the ability to affect corporate policies should pay attention to all appropriate stakeholders when developing policies or establishing organisational structures since without their support the organisation would cease to exist. This implies that executive management must encourage the assistance from stakeholders, in this case information security employees, to achieve the desired results of the organisation such as stability (Donaldson & Preston, 1995) or the protection of its information assets. Since the theory applies to all stakeholders who can develop policies, it is assumed that in organisations where IT professionals are responsible for the development of polices, that from IT perspective, executive management needs to be taken into consideration and maybe the encouragement in terms of their involvement as far as security initiatives should then be initiated from the IT department.

5.3.1.5.2 EXECUTIVE MANAGEMENT

The fact that information security has often been dealt with as a technology issue means that the governance and the management of security improvements has been limited to technical and operational managers (Williams & Andersen, 2001). It has often been thought of as easier to buy a solution than to change the culture and has often resulted in poorly integrated solutions that leave gaps in protection because they are difficult to manage (IT Governance Institute, 2008). No longer can it simply be delegated to roles such as the chief information security officer (CISO) since corporate information is recognised as a business asset and, therefore, business management needs to be responsible for the overall governance and assurance of security's effectiveness (Williams, 2007). This means that executive management is responsible for ensuring that a secure information systems environment is provided for both internal and external users (Williams & Andersen, 2001).

5.3.1.5.3 CHIEF INFORMATION SECURITY OFFICER AND OTHER ROLES

The task of 'securing' the organisation is often left to the chief information security officer (CISO) without any specific guidance in terms of what needs to be secured, why it needs to be secured, what the priorities are and how to ensure that people will agree to them (Xiaomeng et al., 2007). According to Heiser and Scholtz (2009) this is changing as the role of the CISO is moving up in the organisational structure and is, therefore, interacting with decision makers higher up in the organisation on a regular basis since they have a higher level of prestige. The authors expect that the "security" and technical aspects of the role will become de-emphasised as the CISOs position receives greater visibility within the organisation.

Everyone in the organisation, however, plays a part in information security governance from the driver who is responsible for delivering the products to the customers, to the data entry clerk on the shop floor, right up to the chairman on the board (Von Solms, 2006) including executive management and business process owners. The implementation requires skilled resources such as security professionals, information security auditors and technology providers (Williams & Andersen, 2001). Moulton and Coles (2003) have also expressed the importance of the involvement of both the primary and secondary risk owners, they need to have the opportunity and ability to ensure that the most appropriate and cost effective controls are implemented via the information security programme and that they continue to function as intended.

Kritzinger and Smith (2008) grouped the primary responsibilities of information security into six IT authority levels as depicted in Figure 6 below which suggests that information security should be implemented following a top-down approach and on the other hand a bottom-up approach should be followed to report information security incidents. In this way, security incidents will be escalated to the board level and any necessary changes to the information security policies will be made if it is required.

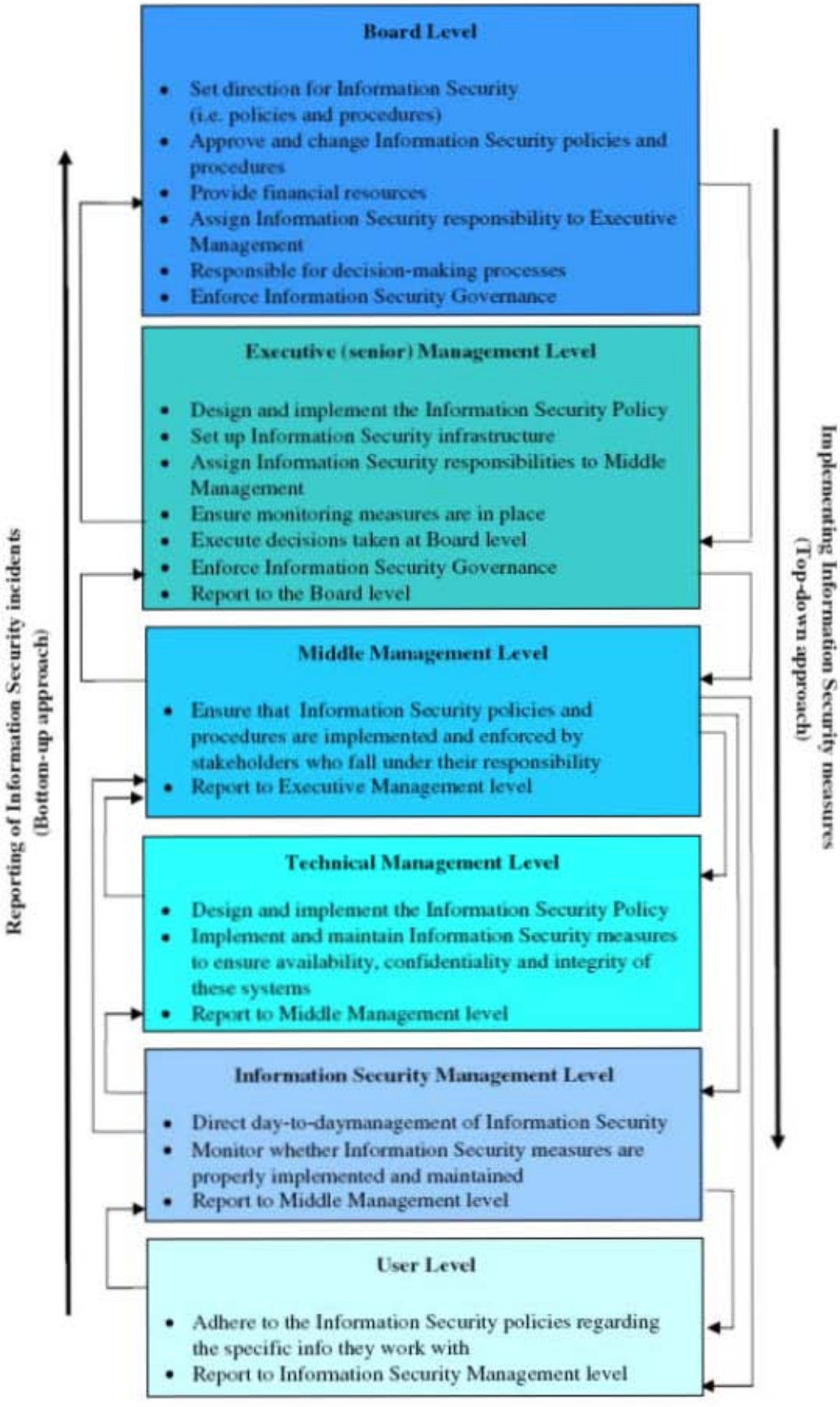


FIGURE 6 - IT AUTHORITY LEVELS (KRITZINGER & SMITH, 2008)

5.3.1.6 AWARENESS

As discussed earlier, organisational information cannot be protected if employees do not understand their roles and responsibilities and this makes training employees to protect information assets a vital aspect (Thomson et al., 2006). Whitman (2003) states that an employee security training and awareness programme should be designed and implemented to educate the employees about the security implementation within the organisation and also relay the importance of security. Since employees deal with vital information on a daily basis, the information security programme seeks to keep security on the minds of the employees (Whitman, 2003) and also proactively prevent security attacks and security breaches due to ignorance (Mishra & Dhillon, 2006) since inadequate knowledge about security mechanisms is at the root of employees "insecure" behaviour (Adams & Sasse, 1999). When devices are lost, users generally do not realise that confidential data has been lost and might fall into the wrong hands, they tend to be more worried about getting a replacement device which indicates a lack of user awareness (Gorge, 2006).

On the other hand, despite the extensive publicity of security breaches, the awareness and commitment of management to information security by previous studies continues to be low (Rhee et al., 2012). The authors Rhee et al. (2012) argue that an understanding of the threats may not be enough for someone to take precautionary or preventive action because people tend to believe that the negative event is unlikely to happen to them and that they are less at risk than others. This is referred to as optimistic bias. The study conducted by Rhee et al. (2012) regarding the perceptions of executives with regards to information security reveals that optimistic bias on security management does exist. Even though the executives have an understanding of the reality of information security risks, they do not associate the reality of the risks with themselves and, therefore, their perception of the information security risks are much lower than others. This comparison is a need that people have to evaluate themselves by using measures and when there are none available, they compare themselves with other people. This is referred as the social comparison theory (Rhee et al., 2012).

5.3.1.7 COMPLIANCE

Increasing an end-user's compliance with information security policies is a fundamental requirement for any information security initiative. Adhering to the core activities as defined by the information security policies is referred to as compliant information security behaviour (Padayachee, 2012). Williams and Andersen (2001) re-iterate that educating users on policies that have been issued and expecting compliance from everyone is something of the past. Other factors such as the user's perception of security play a part in ensuring that users comply with security mechanisms (Adams & Sasse, 1999).

Many suggestions have been made as to why employees would comply with security policies such as:

- Making security policies visible so that it can be taken seriously by the organisation (Adams & Sasse, 1999) and positive social pressure. The promotion of security through education and campaigns in a visible manner significantly affects employee's adherence to policies. The authors argue that even media reports of information security breaches should be made visible and discussed with employees (Siponen et al., 2009).
- Making potential and existing threats to the organisation's systems and information explicit so as to avoid users perceiving security mechanisms as tedious motions that they are forced to go through (Adams & Sasse, 1999). By making it clear, it will change the employee's perception of the existence of security threats also referred to as perceived vulnerability (Siponen et al., 2009).
- Making the systems and information that are sensitive clear since not all information are equally sensitive to avoid users making their own judgements based on their own experience (Adams & Sasse, 1999).
- Making it known that unacceptable behaviour such as employees who circumvent security mechanisms will be challenged otherwise users will tend to assume that it makes no difference if no action is taken when security has been compromised. On the other hand, if the perceived threats to security are low, it may foster careless behaviour because the impression is that the security mechanisms are invincible (Adams & Sasse, 1999).

- A change in the employee's perception of the severity of the threats or degree of potential psychological or physical harm to the organisation referred to as perceived severity (Siponen et al., 2009) which is identified as one of the factors of the protection motivation theory (PMT). PMT is based on perceived severity, which is the degree of harm, perceived vulnerability, which is the probably of the threat actually happening, and fear arousal which refers to the amount of fear that is invoked by the threat. This theory is relevant in the context of information security because a threat that will affect the organisation will most likely affect the employee within the organisation. It also implies that the beliefs of an employee with regards to the importance of information security policies may come from their understanding of how effective the security policies would be in the event of the security threat materialising (Herath & Rao, 2009).

- The belief of employees as to whether they are able to apply or adhere to the security policies referred to as self-efficacy (Siponen et al., 2009).

- The belief of employees that an effective way of preventing security threats is by complying with security policies referred to as response efficacy (Siponen et al., 2009).

5.4 WHY IS INFORMATION SECURITY GOVERNANCE IMPORTANT?

Several reasons have been found in literature as to why information security governance is important such as the fact that information should be seen as a strategic business asset, adherence to legal requirements, risks to company information whether they are old or new and audit compliance. All these are further discussed in the next section.

5.4.1 INFORMATION AS A STRATEGIC BUSINESS ASSET

Information is critical to an organisation's success and is one of its most valuable assets (Von Solms, 2001) and must, therefore, be appropriately protected in the same way as any other important corporate asset (Mishra & Dhillon, 2006). Information is a shared asset amongst all employees of the organisation and employees, therefore, need to be encouraged to take ownership of their share in

order for it to be protected from all possible distortions (Mishra & Dhillon, 2006). However, other stakeholders need to be considered as well such as customers, suppliers and business partners. Convenient ways of accessing information and business services are constantly being demanded by these stakeholders which ultimately mean that organisations are required to share their business information resources more openly. This results in sensitive business information being exposed not only to the technology being used to store, process and transmit it but also to the people accessing the information as well as the business processes applied to manipulate the information as part of the business service or operation that is being provided by the organisation (Posthumus & Von Solms, 2004).

5.4.2 ADHERENCE TO LEGAL REQUIREMENTS

Organisations are expected to adhere to legal requirements such as the South African Electronic Communications and Transactions Act (2002) and the International Basel II Accord or severe prosecution may be faced (Posthumus & Von Solms, 2004). Credit card information storage and transmission is also addressed by the Payment Card Industry standard (PCI) which emphasises that security measures must ensure that data cannot be transmitted, copied or accessed by unauthorised personnel. This applies to mobile devices users as well (Gorge, 2006).

Another example is the Sarbanes-Oxley Act which came about in 2002 as a result of a number of accounting and corporate scandals (Na-yun et al., 2008). The Sarbanes-Oxley Act requires that information contained in annual reports is signed off by the board. CEOs and chief financial officers (CFOs) need to be able to demonstrate that their organisations have proper internal controls (Von Solms, 2006) and attest to the financial reports being accurate as stated in section 302 (Na-yun et al., 2008).

5.4.3 RISKS TO COMPANY INFORMATION

Raghupathi (2007) refers to many examples of organisations that have fallen into financial ruin due to excessive focus on return on investment such as Worldcom and Enron, organisations that have had major data breaches or theft due to improper storage of data, such as CardSystems Solutions, and organisations that have

realised their limitiations, such as not having a backup system, as a result of their computer system failing, such as the Tokyo Stock Exchange. Companies such as Tyco and Parmalat have been mentioned by Short and Gerrard (2009) in addition to the ones already mentioned and referred to as corporate scandals which have heightened the attention of corporate governance. All of these scenarios illustrate the urgency of IT governance (Raghupathi, 2007). In the same way, the integration of computers into aspects of everyday life and the increase in the frequency of security breaches or cyber attacks indicate the growing importance of security governance (Xiaomeng et al., 2007).

A key to the protection of a company's information assets and the governance of the organisation is risk management. Enterprise risk management identifies security risks that could impact the organisation negatively and that adequate controls are in place to prevent potential losses. An organisation will not be able to implement effective protection if the risks are not known (Humphreys, 2008). The risk management process depicted in Figure 7 is suggested by Humphreys (2008).

FIGURE 7 - RISK MANAGEMENT PROCESS (HUMPHREYS, 2008)

An information security governance process should be in place to ensure that due diligence is undertaken when dealing with the protection of company assets against risks. This means that information security risks must be identified and assessed and effective controls must be implemented and regularly reviewed and monitored so that the organisation's information assets are protected (Humphreys, 2008).

Information security governance seeks to protect the organisation's electronic assets against threats, some of which are old and have been around for a long time and others which are new. Some of these threats are discussed in the next section.

5.4.3.1 DATA LEAKAGE AND EMPLOYEE MISTAKES

There are always side effects to the advancements of technology such as the failure of employees to safeguard the organisation's equipment and especially sensitive data (Cisco, 2008). The leakage of sensitive data was recognised as one of the most pressing security issues five years ago (Sophos, 2008) and is still regarded as one of the top ranked issues today that is foreseen as a huge concern in the future (ISACA, 2012).

Data leakage also known as information leakage is described as "the unauthorised transmission of data (or information) from within an organisation to an external destination or recipient" (Gordon, 2007, p. 6). Data may be leaked via a physical method or electronically and does not automatically mean that it was a malicious or intentional action by the employee; it is possible that data leakage was unintentional or inadvertent (Gordon, 2007) meaning by mistake.

Traditionally, activities such as installing anti-virus software, firewall management and configuring security settings on servers and workstations have been regarded as vital to securing the organisation's environment which created the misconception that it is a technical job (Von Solms, 2005b). Later it was realised that non-technical aspects such as policies, awareness and compliance enforcement mechanisms are recognised as pivotal to good information security governance (Von Solms, 2005b).

Even though the development of policies has been recommended as a key factor for the implementation of information security (Da Veiga & Eloff, 2007) all organisations have not developed security policies since a global security survey across 10 countries and 2000 employees on data leakage revealed that many organisations do not have any security policies in place and those organisations that did were ineffective (Cisco, 2008).

The failure to create security policies on the one hand is a major stumbling block (Cisco, 2008) and on the other hand, organisations are still at risk because their information security policies are not followed by their employees (Siponen et al.,

2009). One of the reasons is ineffective education of employees with regards to security and, therefore today, security awareness forms an important part of information security governance because relying on the traditional adhoc approaches to security is not enough (Rhee et al., 2012).

Data leakage is not a new threat but one that persistently plagues organisations and in order to minimise the mistakes of employees, IS management should ensure that they are educated. Technological advances such as BYOD introduces new ways of data being leaked as well as other security implications which are discussed under the heading “Business implications of mobile devices”.

5.4.4 AUDIT COMPLIANCE

Conducting an audit is the prevalent method in practice among the different methods of compliance checking (Ghiran & Bresfelean, 2012). The financial and the technological side of the organisation are no longer the only aspects that are audited, the security aspects of information such as the security policies, procedures and security controls are audited since it seems like a futile exercise to audit an organisations financial accounts without verifying that the information is adequately and appropriately secured (Vroom & Von Solms, 2004). If the systems maintaining the data are not secure, it’s very hard to signoff the validity of the data (Von Solms, 2006). A common understanding of security policies and practices as well as an inconsistency in the application of security controls as a result of audit and compliance reporting requests have been identified by Booker (2006) as the main problems organisations face when managing governance. Most times the response to these audit requests is reactive which means security controls are applied on an adhoc basis (Booker, 2006) in response to a bad audit or incident (Anderson, 2003), therefore, a planned approach is essential (Booker, 2006).

Humphreys (2008) states that a continuous cycle of improvement is required to ensure that information security is effectively established, implemented, monitored, reviewed and maintained, done as part of the internal audit which is seen to be an essential part of the overall process of governance and risk management. Lots of research can be found on each of the topics of governance, risk management and

compliance seperately but these should be viewed in an integrated manner according to Racz, Weippl and Seufert (as cited in Ghiran & Bresfelean, 2012).

5.5 IMPLEMENTING INFORMATION SECURITY GOVERNANCE

5.5.1 INFORMATION SECURITY MANAGEMENT PROGRAMME

In order for security governance to exist, something must exist to be governed such as a security management programme which is a collection of the controls or core components such as risk management, information security policies, procedures, guidelines, standards, security education, security organisation and information classification that an organisation must have in place (Harris, 2007). An information security programme has been suggested as a risk mitigation method that can be used by organisations (Williams & Andersen, 2001), the goal of which is to protect the company's information and assets. Security governance ensures that the strategic needs of the business are adequately met by the security programme (McMillan & Scholtz, 2010).

The start of such a programme requires enterprise management to identify the scope and the risks that the organisation faces (Moulton & Coles, 2003). Harris (2007) describes a top-down approach to an information security programme where top management initiates, supports and gives direction to the information security programme whereas a bottom-up approach is a situation where top management is not involved and the IT department develops the security programme. The bottom-up approach is doomed to fail according to this best practice because the people responsible for protecting the company's assets are not involved and are not driving the information security programme.

Once the risks are identified the idea is to follow a process that enables the management of the risks identified (Moulton & Coles, 2003). The process recommended by Harris (2007) is referred to as being circular which starts with an assessment of the risks to identify the possible damage and potential loss that the organisation could undergo if any of the threats materialised. This enables management to develop the applicable policies and construct a budget in order to protect the organisation by directing the security activities.

This is followed by the systems involved being monitored and evaluated. Williams and Andersen (2001) state that the infrastructure and environment needs to be continuously monitored and tested for vulnerabilities referred to as “test and patch” because of the speed with which risks emerge. Von Solms (2005b) states that traditionally these types of activities have been regarded as information security operational management which created the misconception that it is a technical job. Some of the activities mentioned are:

- Installing and updating anti-virus software
- Firewall management with regards to connecting workstations to the internet
- Configuring and updating security settings of servers and workstations and several others.

This image has, however, changed because the protection of information against threats leading to wrongful disclosure, alteration or loss requires both technical and non-technical safeguards (Von Solms, 2005b). A mixture of evolving policies, improved defences and security fixes are required to respond to these risks (Williams & Andersen, 2001).

This is then followed by an awareness campaign to make everyone understand the issues which results in everyone working towards the same security goals and lastly the defined risks are addressed by implementing policies and controls. The cycle starts again which means that the security environment is constantly evaluated and monitored (Harris, 2007). An aspect which has not been mentioned as part of this process is that of compliance which has been discussed and identified earlier as an important part of information security governance. Von Solms (2005b) confirms that compliance was never considered a part of information security management traditionally but over the last couple years the role of information security management has changed significantly. In light of this, compliance needs to be taken into consideration as part of the information security management programme since it is part of information security governance.

The following section discusses using a framework to guide the implementation of an information security programme.

5.5.2 USING BEST PRACTICE TO GUIDE THE IMPLEMENTATION

An information security governance programme can be successfully implemented by adopting best practices (Williams & Andersen, 2001). Von Solms (2005a) states that companies are realising that rather than trying to establish an information security governance environment on an adhoc basis, it is preferable to follow an internationally recognised reference framework. Several resources exist that can be used as guidance for information security governance such as:

- Control Objectives for Information and related Technology (COBIT) which aids risk mitigation, strategic alignment maturity assessments and IT value delivery (Mataracioglu & Ozkan, 2011; Saetang & Haider, 2011; Raup-Kounovsky, Canestraro, Pardo, & Hrdinova, 2010; Simonsson et al., 2008; Spafford, 2003)
- National Institute of Standards and Technology (NIST) (IT Governance Institute, 2008; Dlamini et al., 2009)
- International Organisation for Standardisation (ISO)/ International Electro technical Commission (IEC) 27000 family of security standards (IT Governance Institute, 2008) such as ISO17799 (Spafford, 2003; Saint-Germain, 2005) and ISO27001 (Mataracioglu & Ozkan, 2011)
- Certified Information Systems Security Professional (CISSP) (Harris, 2007)

Von Solms (2005a) discusses the pros and cons of using both COBIT and ISO17799 and has stated that they are both good choices for information security governance and are complementary and, therefore, when used together can provide benefits to the organisation. COBIT enables the integration of information security into a wider information technology (IT) framework which means that if the company decides to implement the rest of the framework it is available. COBIT, however, focuses on what must be done but does not provide detailed guidelines on how it must be done. ISO17799 on the other hand, provides more detailed guidance on how things must be done but only addresses information security and is not integrated into a wider IT governance framework (Von Solms, 2005a). It is the only framework that allows an

organisation to become certified by undergoing a third party audit (Saint-Germain, 2005).

The IT Governance Institute (2008) recommends that a framework must be established and maintained by management to guide the development and maintenance of an information security programme in order to achieve effective information security governance. Spafford (2003) describes a number of compelling reasons why organisations should rather adopt existing standards such as providing a well defined structure, they have been developed and assessed over many years by many people and organisations, they provide a platform to share knowledge between organisations and they make it easier for organisations to be certified against a base standard from which improvements can be recommended.

The next section discusses mobile devices in the workplace, the evolution of mobile devices, business implications of mobile devices and some of the risks associated with using mobile devices in the workplace.

5.6 MOBILE DEVICES IN THE WORKPLACE

The greatest pressure for change with regards to the use of personal devices such as smartphones and tablets within the workplace is coming from employees across all parts of the business according to managers and senior executives that participated in a recent citrix-commissioned global survey (Millard, 2013). Employees are allowed to work equally effective wherever they are thereby making employees' lives easier. Work is increasingly being recognised as what you do and no longer a place you go to (Millard, 2013).

5.6.1 EVOLUTION OF MOBILE DEVICES

Significant technology advances in mobile devices have been witnessed over the past two decades. These technology advances spans from the late 1990s and early 2000s where the personal data assistants (PDAs) came into existence to the multifunctional and ubiquitous smartphones of today (Ernst & Young, 2012).

In the early 2000s the first Blackberry smartphone was released which provided corporations with benefits such as remote email and calendar access. The idea of

24-hour connectivity was established as corporations began providing a large percentage of their workforce with network access on their smartphone. This led to the release of a number of devices running Android, BlackBerry, Windows Mobile and Windows Phone 7 operating systems. Figure 8 depicts this evolution of mobile devices (Ernst & Young, 2012).

FIGURE 8 - EVOLUTION OF MOBILE DEVICES (ERNST & YOUNG, 2012)

The development of tablet PCs are redefining the concept of smartphones, seen as the next evolution in mobile computing, and are being supported by many companies (Ernst & Young, 2012).

5.6.2 BRING YOUR OWN DEVICE (BYOD)

The concept of BYOD allows employees to dictate the technology they want to use within the company environment and does not follow the process that IT normally follows for vetting, monitoring and auditing equipment (Tokuyoshi, 2013). The technology advances in mobile devices allows constant access to email, allows access and storage of sensitive company information and enables the use of mobile business applications which have blurred the lines between home and the office (Ernst & Young, 2012).

The old way of working where organisations provide employees with devices to do their work is slowly becoming something of the past and can be seen in the growing numbers of employees using their own devices within organisations. Figure 9 illustrates the growth rate of a 10% increase between 2010 and 2011 according to a Unisys study conducted by IDC and according to Cisco systems annual visual networking index forecast there will be almost 15 billion network connected devices such as tablets, notebooks and smartphones by 2015 (Burt, 2011).

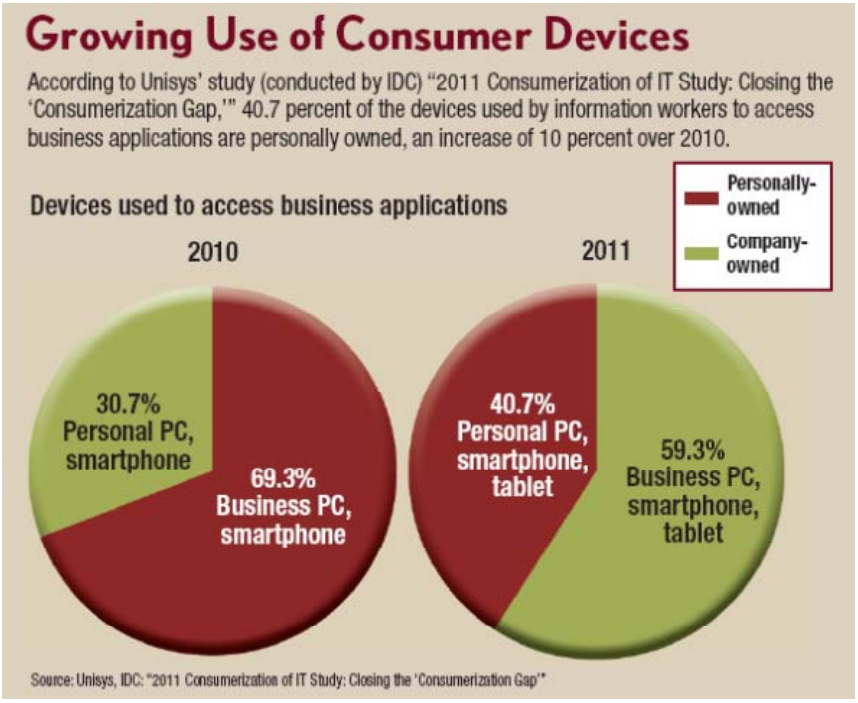


FIGURE 9 - UNISYS STUDY CONDUCTED BY IDC (BURT, 2011)

Users are selecting devices that they find are the most appropriate for their jobs based on the usability of these mobile devices which are enabling users to integrate their personal and business lives together. Users now have the option to choose

between the heavy, boring corporate issued devices or lighter, sleeker personal devices.

There is, however, a conflict between the security of the company's information and the usability of mobile devices (Tokuyoshi, 2013). The next section discusses the business implications of mobile devices.

5.6.3 BUSINESS IMPLICATIONS OF MOBILE DEVICES

The use of mobile devices within the workplace has resulted in a number of implications for businesses. An evaluation of the potential risks and benefits of a mobile platform strategy is required which keeps the audience in mind since some platforms trade-off security in order to achieve usability and simplicity while others have inherent secure controls embedded in the device which presents less risks to an organisation's environment (Ernst & Young, 2012).

5.6.3.1 TANGIBLE BENEFITS

Organisations such as Stadion Money Management has moved to a BYOD policy and plans to eliminate office desktop computers since most of their employees do their work such as editing of documents and checking of emails from their own mobile devices. The organisation claims that it costs far less to support multiple mobile devices than laptops and have reduced their supports costs by 50% for employees who travel extensively (Fernandez, 2012). Other authors such as Ashford (2012), however, disagrees that reducing costs is not a good enough reason to allow employees to use their own devices because it does not outweigh the risk of losing sensitive company data.

Tangible benefits such as staff recruitment, retention and increased productivity have been confirmed by surveys conducted across two-thirds of businesses across all countries (Millard, 2013).

5.6.3.2 IT DEPARTMENT SUPPORT

Traditionally, the devices connected to the network have always been owned by the organisation and most likely it has been approved, configured and installed by the IT people. This can no longer be assumed with the BYOD concept and organisations now need access control based on who is connecting to the network but also what

and where they are connecting from (Mansfield-Devine, 2012). According to Forrester, 33% of users are purchasing personal devices which can specifically be used in the work environment to improve productivity with no consideration as to whether the IT department can support the devices (Tokuyoshi, 2013).

5.6.3.3 SECURITY IMPLICATIONS

Despite the advancement in technology, some businesses are reluctant to move towards a more flexible mobile working environment for their employees due to security concerns such as allowing employees remote access to the corporate network which could potentially lead to corporate data falling into the wrong hands and the risks associated with allowing the downloading of applications and documents (Millard, 2013).

Employees using their own devices for work purposes results in many security implications such as the possibilities of sensitive data being leaked and the infiltration of malware and gaps in the firewall since an employee's personal device is one that is no longer locked down or configured by the company (Mansfield-Devine, 2012). Green (2007) also warned of virus infection of mobile devices, data theft by employees called "podslurping" which is the use of a USB device to copy large amounts of data, vulnerabilities regarding bluetooth technology where bluetooth devices can be used by an attacker to gain access to data as well as wireless technology that introduces another avenue for attackers to access the organisations network.

As devices are becoming popular for both personal and business activity, hackers are turning their attention to them. An increase in mobile malware is being reported by security researchers. The number of malicious android application package files have increased from 139 to 3069 and android malware families have increased from 10 to 37 between quarter 1 of 2011 and quarter 1 of 2012 (Hart, 2013).

The organisation's control over employee devices becomes less which means the visibility of adherence to policies and compliance, ownership and usage virtually becomes non-existent. Important security features can also be disabled by employees since the employee has full control over the device which means the devices are exposed to information security threats (Fernandez, 2012).

The reality of the employees working in unsuitable locations should also be considered since the probability of loss and theft is increased. One way that IS management can ensure the security of the organisations information is by developing a mobility policy which should state that all devices require a password for authentication (Fernandez, 2012) and that the device must have remote-wipe software installed so that the data can be wiped from the device should it be lost. Chigona, Robertson, & Mimbi (2012) argue that the extent of data loss through mobile devices is currently not known and according to the computer crime and security survey, proprietary data loss or theft was reported by only 4% of the respondents.

Burt (2011) recommends that users should be required to sign an acceptable use agreement which means that if the device is part of a legal dispute the device can be seized for an indefinite amount of time.

Organisations moving to a BYOD practice need to realise that governance is critical to its success. For example, Cisco includes stakeholders from business units such as legal and human resources on the BYOD steering committee led by their IT department. Formal governance is required to define how the organisation can strategically move from a managed world to one where IT does not manage every technology asset in use in the organisation and where the security perimeter is no longer defined (Thomson, 2012).

5.7 SUMMARY OF LITERATURE REVIEW

Some of the themes that were found in the definitions of information security governance and in literature have been discussed, and depicted in Figure 10 below. How organisations go about implementing information security governance within an organisation, specifically within the mobile device environment, has not been addressed. There is a lack of literature on information security governance implementations within the mobile environment and Kotulic and Clark (2004) agree that information security may be one of the most critical areas for research.

Figure 10 depicts that literature discusses the importance of the support of executive management of the information security governance implementation. The information security governance implementation consists of both technical and non-

technical aspects which must be considered in order to ensure the confidentiality, integrity and availability of electronic information. By taking all these aspects into consideration threats such as social engineering and identity theft is more likely to be prevented than if they were not considered at all. Figure 10 shows a generic view of all themes found in literature with regards to information security governance. The implementation of information security governance within the context of a mobile device environment is currently an unknown area and, therefore, the research conducted examined how organisations go about implementing information security governance within the mobile device environment.

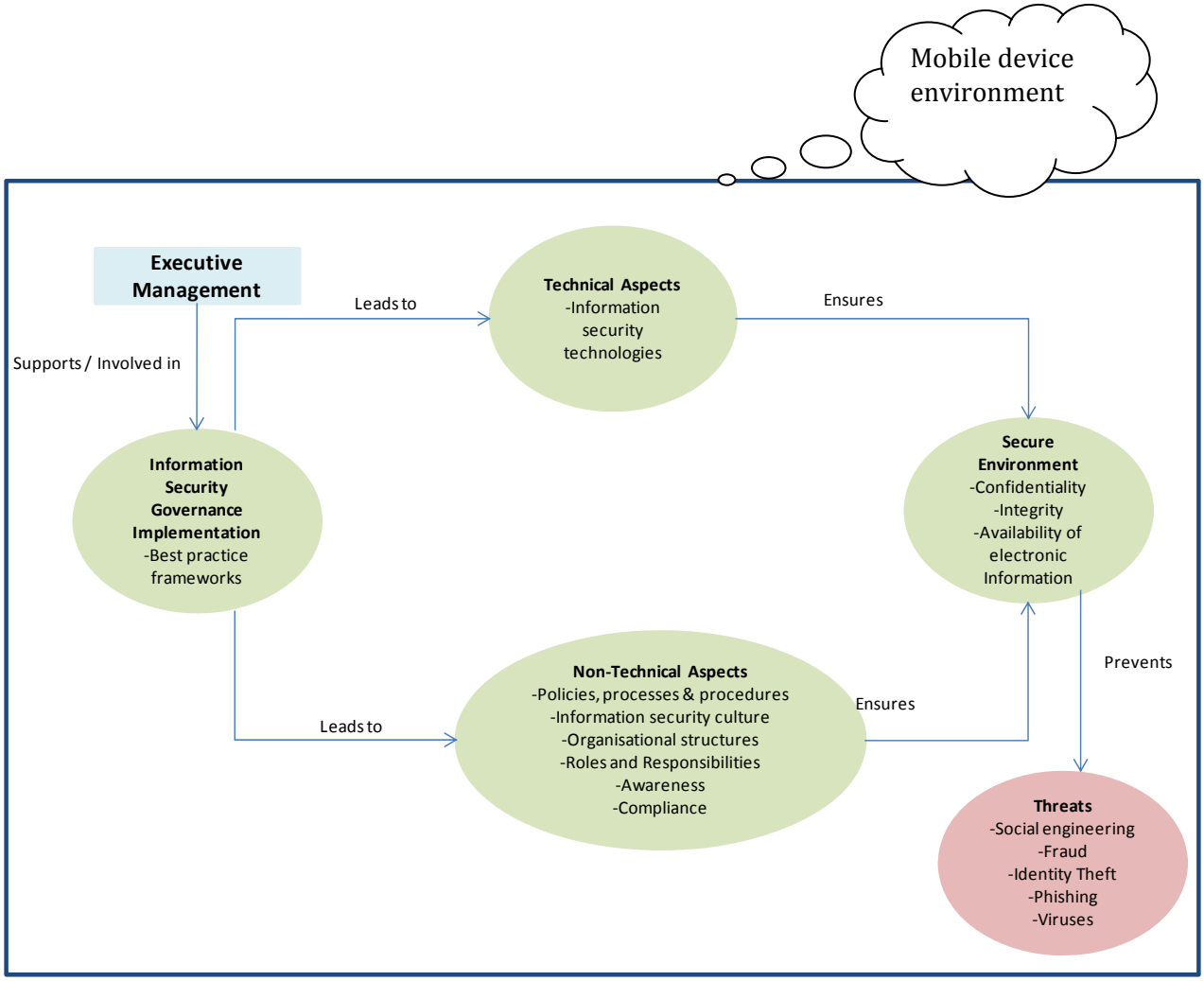


FIGURE 10 - INFORMATION SECURITY GOVERNANCE THEMES

6 RESEARCH DESIGN

The research design starts by discussing the research question then goes on to discuss the research method which explains the background to IS research, the research purpose, philosophy, approach, strategy, data collection, data analysis, timeframe, sample and ethics. .

6.1 RESEARCH QUESTION/OBJECTIVES

The objective of this research was to describe and explore the phenomenon of an 'information security governance implementation' in order to gain an understanding as to how organisations go about implementing information security governance within a mobile device environment. The research question which was answered by the research is:

How do organisations go about implementing information security governance within mobile device environments?

In order to answer the research question, the researcher explored the perceptions of the participants on their views of the activities undertaken prior to implementation, during the implementation and after the implementation of information security governance within the mobile device environment.

6.2 RESEARCH METHOD

The research method starts by discussing a short summary of the background to IS research, the purpose of the research, then goes on to explain the sections as divided by the research onion displayed in Figure 11.

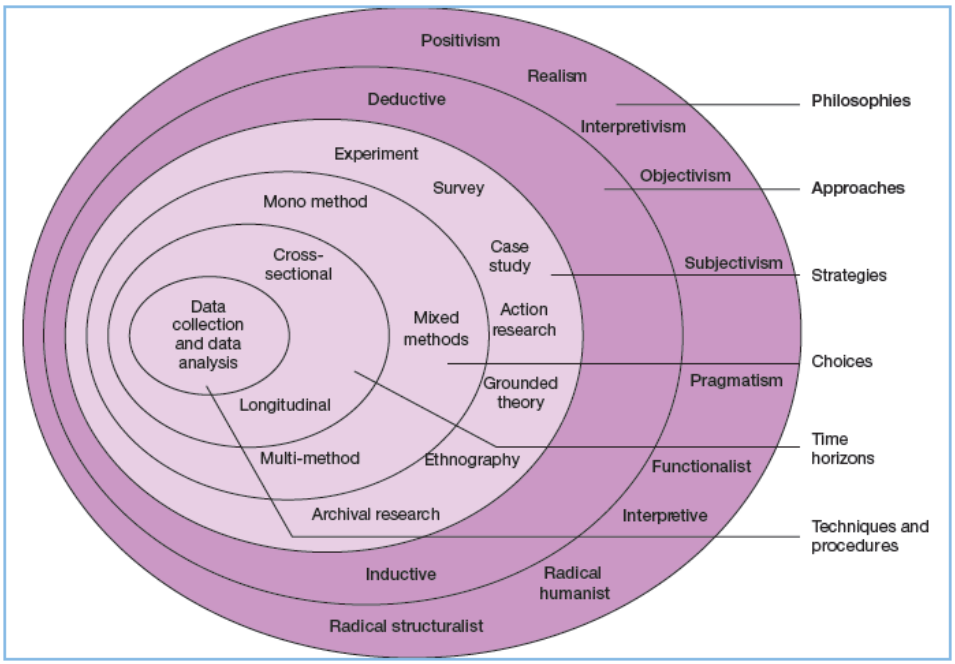


FIGURE 11 - RESEARCH ONION (SAUNDERS, LEWIS, & THORNHILL, 2007)

6.2.1 BACKGROUND TO IS RESEARCH

One hundred and fifty five published articles between 1985 and 1989 were examined by Orlikowski and Baroudi and found that the IS research community was dominated by the positivist paradigm, no critical research work was found and little attention was paid to the interpretive paradigm (Chen & Hirschheim, 2004). This trend continued as discovered by the study conducted by Chen and Hirschheim (2004) who examined 1893 published articles during 1991 and 2001 and found that 81% of the published empirical research was positivist. The information systems field was dominated by the positivist paradigm until interpretivism emerged in the field (Walsham, 1995) and qualitative research became more popular (Chen & Hirschheim, 2004).

In the past according to Baskerville and Myers (as cited in Urquhart, Lehmann, & Myers, 2010) the borrowing of theories from other disciplines was a well-known characteristic of the information systems research domain. These borrowed theories from social science and computer science disciplines (Matavire & Brown, 2013) are often valuable but theories could be generated from within the information systems discipline itself (Urquhart et al., 2010). This research, therefore, aimed to develop theory from within the information security governance domain so that a contribution could be made towards developing theory within the information systems discipline.

6.2.2 PURPOSE OF RESEARCH

The research was firstly descriptive as it aimed to portray the activities required to implement an information security governance initiative (Saunders, Lewis, & Thornhill, 2007).

Secondly, the research was exploratory because it aimed to seek new insights into the phenomenon of information security governance implementation and to shed new light as to how organisations go about implementing information security governance within a mobile device environment. An exploratory study is a valuable means of finding out what the main concerns are of the stakeholders responsible for the information security governance implementation and what impact the outcomes of the implementation has on future implementations (Saunders et al., 2007).

6.2.3 ONTOLOGY AND PHILOSOPHY

Information system researchers may use a number of philosophical perspectives to study information system phenomena (Orlikowski & Baroudi, 1991). According to Chua's classification, three sets of beliefs outline the way the world is seen and researched namely, the researchers beliefs about the phenomenon of study, the beliefs about the notion of knowledge and lastly, the belief about the relationship between the empirical world and knowledge (as cited in Orlikowski & Baroudi, 1991).

Ontological beliefs have to do with assumptions about the empirical world. Either the empirical world is seen to be objective and independent of humans referred to as objectivism. This means that reality exists independently from human experiences, which is the belief of positivists or reality is subjective and is created and recreated through the actions of humans and therefore, organizations, groups and social systems cannot be characterised and measured objectively since they do not exist apart from humans, which is the belief of interpretivists and referred to as subjectivism (Orlikowski & Baroudi, 1991; Saunders et al., 2007).

Positivist, interpretive and critical research philosophies are used to conduct information systems research, each of which constitute different worldviews and research perspectives adopted by the researchers (Orlikowski & Baroudi, 1991).

6.2.3.1 POSITIVIST PHILOSOPHY

Positivist studies attempt to increase the predictive understanding of phenomena by primarily testing theory and assume that a one-to-one relationship between the constructs of the researcher's objects, features or events exists. The researcher does not intervene in the phenomenon but takes a neutral role in the investigation (Orlikowski & Baroudi, 1991). The research is based on the notion that the researcher is independent, the research is objective and the results are valid, reliable and replicable (Pather & Remenyi, 2004).

6.2.3.2 CRITICAL PHILOSOPHY

Critical studies attempt to critically evaluate and transform the social reality being investigated which fosters an understanding and self-consciousness of the existing social conditions. Existing social systems are critiqued and contradictions and conflicts are revealed within their structures (Orlikowski & Baroudi, 1991). Myers and Klein (2011) state that critical research is concerned with social issues with respect to the development, use and impact of information technology such as social control, freedom, values and power. The transformation of alienating and restrictive social conditions is what differentiates the critical research philosophy from positivist and interpretive philosophies which are content with the status quo being predicted and explained (Orlikowski & Baroudi, 1991). Critical researchers declare their interests and biases since they believe that bias is inherent in the human condition and research is conducted by humans (Pather & Remenyi, 2004).

6.2.3.3 INTERPRETIVE PHILOSOPHY

Interpretive studies attempt to understand the phenomenon being studied through the meanings that participants assign to them (Orlikowski & Baroudi, 1991) and acknowledge that their research problems exist in a social context (Pather & Remenyi, 2004). As people interact with the world around them, people create and associate their own subjective and intersubjective meanings (Orlikowski & Baroudi, 1991). The possibility of an "objective" or "factual" account of events and situations are rejected by interpretive studies (Orlikowski & Baroudi, 1991) and, therefore, numbers and statistical tests may not necessarily be the most appropriate way of understanding the actions of social actors (Pather & Remenyi, 2004). Instead a relativistic, shared understanding of the phenomenon being studied is sought. The

intention is to understand the deeper structure of the phenomenon so that other settings may be informed (Orlikowski & Baroudi, 1991). Deep insights into the information systems phenomenon being studied may be produced since an interpretive study aids the researchers understanding of human thought and action in social and organizational contexts (Klein & Myers, 1999).

The philosophy of the research adopted was interpretive as the aim of the researcher was to understand people's perceptions on the phenomenon of information security governance implementation and also how the information security governance that was implemented impacted on other implementations. The researcher needed to understand the viewpoints of the various participants by adopting an empathetic stance (Saunders et al., 2007) which enabled the researcher to produce deep insights into the information security governance implementation phenomena by gaining an understanding of the participants' thoughts and actions (Klein & Myers, 1999).

6.2.4 RESEARCH APPROACH

The researcher used a mixed approach, deductive and inductive; by using a conceptual framework developed from the literature as a sensitising device and then developed theory that addressed the phenomenon of "information security governance implementation".

A deductive approach means that theories or concepts are identified in literature which will be used to test data (Saunders et al., 2007) or to guide data collection. The intent of the researcher was not to test data but to use existing theories or concepts as a sensitising device. This means that the research commenced from a theoretical perspective which had some advantages such as providing an initial analytical framework and links the research into an existing body of knowledge (Saunders et al., 2007). Theoretical sensitivity indicates an awareness of the researcher of the subtleties of the meaning of data; it refers to a personal quality of the researcher. The researcher has insight and is able give meaning to data, is capable of separating pertinent information from that which isn't because of the researcher's capacity to understand. A number of sources can provide the researcher with theoretical sensitivity such as literature, professional experience,

personal experience and the analytic process itself. All these provide a rich background of information that “sensitises” the researcher to what is going on with the phenomenon being studied (Strauss & Corbin, 1990). On the other hand, the researcher is aware that knowledge gained from experience and reading, biases, patterns of thinking and assumptions can block the researcher from seeing what is significant in the data. The researcher made use of techniques such as the use of questioning, making comparisons and analysing phrases or sentences to prevent or rectify these problems (Strauss & Corbin, 1990).

The conceptual framework developed during the literature review as depicted in Figure 10 was used as a sensitising device and used to start the data collection and analysis process.

The research followed an inductive approach which means that the data collected was explored to develop theory and then related back to the existing literature. An inductive approach allowed the researcher to understand the nature of the problem by interrogating the participants using semi-structured interviews and gave the researcher a feel for what was going on (Saunders et al., 2007).

6.2.5 RESEARCH STRATEGY

The research strategy employed needs to be able to answer the research question and objectives and, therefore, is guided by the research question, the researcher’s philosophical stance and the amount of time and resources available (Saunders et al., 2007).

There are several ways of doing social science research such as experiments, history, surveys, analysis of archival documentation, case studies each of which has its advantages and disadvantages (Yin, 1994). Experiments are suitable when the researcher is able to manipulate behavior such as in a laboratory. Surveys are usually associated with a deductive approach and can be used to suggest possible reasons for particular relationships. Histories are the preferred strategy when the relevant individuals are no longer alive to report and the researcher needs to rely on documents and physical artefacts as evidence. Direct observation and interviewing is what distinguishes “history” as a strategy compared to the case study strategy (Yin, 1994).

The qualitative strategies, action research, ethnography, grounded theory and case studies were considered. Neither, action research nor ethnography was appropriate for this research since action research is an iterative process of diagnosing, planning, taking action and evaluating (Saunders et al., 2007). This research was not intended to introduce change and then evaluate it. On the other hand, ethnography involves extended participant observation and the phenomenon is researched within the context in which it occurs. This research strategy requires the researcher to be immersed in the social world completely over an extended period of time (Saunders et al., 2007). The researcher had a time constraint and, therefore, the ethnography strategy was not appropriate. The strategy chosen for this research was a grounded case study. The reasons for the choosing a grounded case study are discussed in the next section which discusses case studies as well as the grounded theory methodology.

6.2.5.1 CASE STUDY RESEARCH

A case study "is an examination of a specific phenomenon such as a program, an event, a person, a process, an institution or a social group" (Merriam, 1988, p. 10). Yin (1994, p. 13) states that the technical definition of a case study is that it "is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between the phenomenon and context are not clearly evident". Eisenhardt (1989) describes a case study research strategy as focusing on single settings and understanding the dynamics present within them and has also stated that building theory from case study research can provide a fresh perspective on a topic that has already been researched.

Flyvbjerg (2006) states that one of the misunderstandings with regards to case study research is that it cannot contribute to scientific development because one cannot generalise from a single case. Merriam (1988) argues that it is possible to enhance the generalisation of a case study's results by providing a detailed description of the case study's context so that readers are able to compare it with their own situation.

A case study is an appropriate strategy when the research question being posed is a "how" or "why" question and the researcher has little control over the events (Yin, 1994). The research undertaken was an information security governance implementation, which is a phenomenon within a real-life context, the researcher had

little control over the events and the research question being posed is a “how” question. Therefore, undertaking a grounded case study as a research strategy was appropriate and was conducted at a Retail organisation where information security governance had already been implemented within the mobile device environment. This research setting chosen was a rich source of information on the research topic.

The boundary determined at the beginning of the research was a single case study which meant that any concepts which may have emerged and required investigation beyond the boundary of the single case may not have been possible. The concepts that emerged were investigated from within the single case setting which provided a detailed description of the case so that readers of other organisations may compare it to their own situation (Merriam, 1998). A grounded case study was, therefore, appropriate and the theory generated was grounded from the case data. This allowed the researcher to observe and analyse an information security governance implementation within the context of its real life using multiple sources to discover evidence (Saunders et al., 2007) and gain an in-depth understanding of the problem (Flyvbjerg, 2006).

The intent of the researcher was not to be able to generalise the findings to a population but to gain a deep understanding of the structure of the information security governance implementation which the researcher believed could be of value by informing other settings (Orlikowski & Baroudi, 1991). The researcher’s aim was to try and generalise the findings to “theory” (Yin, 1994) so that the case of the information security governance implementation could make a contribution to the information systems domain. The applicability of the findings of this case study will in the end be left to the reader’s discretion as to whether the findings are useful, whether it can be learnt from and whether any of the findings can be applied to the reader’s situation (Merriam, 1988).

A grounded case study enabled theory to be built with the use of procedures and techniques of the grounded theory methodology which was popularised by Eisenhardt (as cited in Matavire & Brown, 2013). Matavire and Brown (2013) have encouraged the use of the grounded theory methodology with other research methods in IS research so that a better understanding of the outcomes and the process can be developed. The use of the grounded theory methodology also guided

the researcher to develop a theory in an attempt to explain the phenomenon of an information security governance implementation in a way that it has never been articulated before (Pozzebon, Petrini, Bandeira de Mello, & Garreau, 2011). The next section discusses the grounded theory methodology.

6.2.5.2 GROUNDED THEORY METHODOLOGY (GTM)

Grounded theory (GT) appeared for the first time as a book called “The Discovery of Grounded Theory” published in 1967 by Barney Glaser and Anselm Strauss (Duchscher & Morgan, 2004; Goulding, 1998) and is defined as “theory which has been systematically obtained through “social” research and is grounded in data” (Goulding, 1998, p. 51). A grounded theory represents one that has been discovered and developed inductively from the phenomenon being studied (Strauss & Corbin, 1990).

The main purpose of grounded theory methodology is to generate theory and the interest in the use of grounded theory in information systems research has increased over the past decade (Urquhart et al., 2010). IS researchers are, therefore, able to use GTM as a means to build theory relevant to the discipline being researched (Matavire & Brown, 2013) when little is already known about the phenomenon or secondly to provide a fresh slant on the existing knowledge (Goulding, 1998). Despite this distinct purpose, information systems grounded theory studies as well as other fields have been criticized for having low levels of theory development since many studies have used grounded theory as a coding method only. This use of grounded theory is appropriate, in some cases, but is limited since grounded theory offers a comprehensive method for the generation of theory (Urquhart et al., 2010). This study, therefore, used the grounded theory methodology to generate theory with regards to the ‘information security governance implementation’ phenomenon within the information systems discipline. Grounded theory was selected since it has been used and found to be a suitable method for rigorous theory development in the past (Goulielmos, 2004).

GTM is based on the principle of emergence, constant comparative analysis and theoretical sampling discussed below.

6.2.5.3 PRINCIPLE OF EMERGENCE

One of the principles that grounded theory is based on is the principle of emergence. The use of a conceptual framework before data is collected and analysed is discouraged so that concepts and categories emerge from empirical data that has been analysed (Pozzebon et al., 2011). Authors such as McGhee, Marland, and Atkinson (2007) have, however, argued that there are a number of reasons why a literature review should be conducted before any analysis takes place such as the ability to justify the reason for the study, to assess whether grounded theory is appropriate, to avoid pitfalls conceptually or methodologically and it allows the researcher to have an “open mind” and not an “empty head”. The researcher took this stance and, therefore, engaged with literature prior to data collection.

6.2.5.4 CONSTANT COMPARATIVE ANALYSIS

The general method of comparative analysis is a major strategy which is emphasised for the discovery of grounded theory (Glaser & Strauss, 1967) Firstly, the data is contrasted against itself, secondly, against evolving original data and thirdly, against existing theoretical and conceptual claims. This facilitates the emergence of knowledge (Duchscher & Morgan, 2004).

6.2.5.5 THEORETICAL SAMPLING

Theoretical sampling is the process whereby the researcher jointly collects, codes and analyses the data and then makes a decision as to what data to collect next and where it can be found in order to develop the theory as it emerges from the data (Glaser & Strauss, 1967). The research may begin with a few concepts that the researcher is aware of before the study is conducted which gives the researcher a foothold on the research (Glaser & Strauss, 1967). The researcher conducted a literature review and was aware of concepts or themes with regards to information security governance as discussed within the literature review section which were used by the researcher to start the data collection process.

6.2.6 DATA COLLECTION

Qualitative data was collected since the findings of the research were not arrived at by means of statistical procedures or in other words, quantification. The intricate details of the phenomenon of information security governance implementation may have been difficult to convey with quantitative methods (Strauss & Corbin, 1990) and, therefore, qualitative data was collected.

Urquhart et al. (2010) refer to seed concepts which is the start to the process for generating grounded theory and these seed concepts can come from a range of sources other than data such as 'lived experiences, hunches or other theories as depicted in Figure 12.

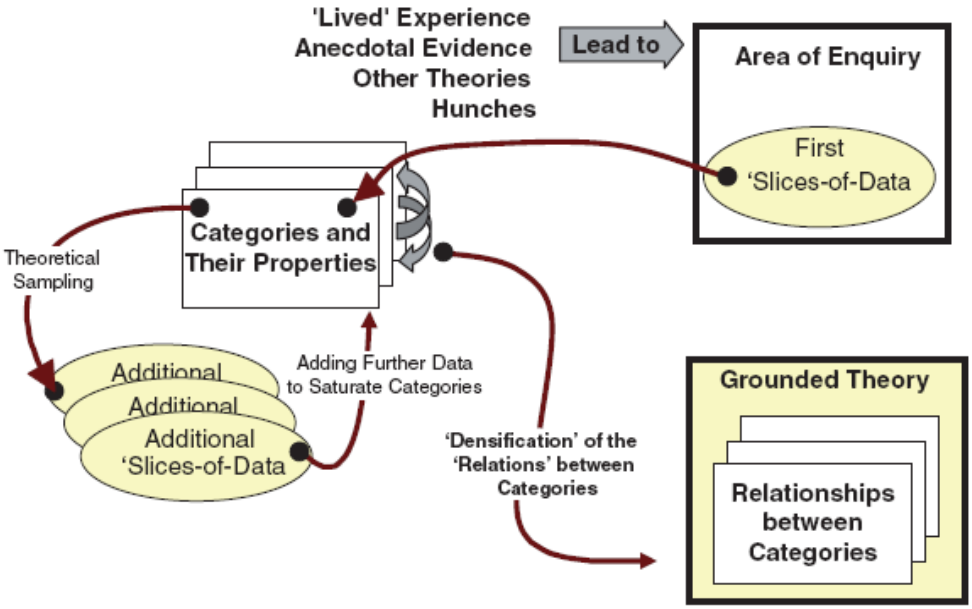


FIGURE 12 - CYCLE OF DATA COLLECTION IN THE GROUNDED THEORY METHOD (URQUHART ET AL., 2010)

The researcher conducted semi-structured interviews to elicit data. The themes found in literature relating to the mobile information security governance implementation were used as seed concepts to structure the questions that were used for the first interview (Appendix A). Although interviews are regarded as one of the most important sources of case study information, some common problems are poor or inaccurate articulation, poor recall and bias and therefore the interview data will be corroborated with other sources (Yin, 1994).

Yin (1994) conveys three principles of data collection namely, the use of multiple sources of evidence, creating a case study database and maintaining a chain of evidence.

6.2.6.1 MULTIPLE SOURCES OF EVIDENCE

A combination of data collection techniques was employed by the researcher such as observation, semi-structured interviews as well as company documentation analysis (Saunders et al., 2007; Yin, 1994) as depicted in Figure 13.

The use of different data collection techniques within one study is called triangulation to ensure the accuracy of the data (Saunders et al., 2007) which helps to counteract the biases of the researcher's collection and analysis of the case data (Darke, Shanks, & Broadbent, 1998) and strengthens the findings of the case study (Yin, 1994). For example, documents can be used to corroborate evidence from other sources, if evidence is contradictory, the researcher has a reason to do further enquiry (Yin, 1994).

An example of a situation that was observed by the researcher can be found in Table 6 (Change Management). The researcher observed that the team that was expected to support the mobile infrastructure environment had a low awareness of the content of the mobile device management policy and as a result almost contravened the mobile device management policy. This was observed after the implementation during conversations with the infrastructure team members.

The researcher observed, recorded the interviews via audio recording as well as took notes to ensure accuracy. The interviewees had the option to turn off the recorder at all times. Some of the interviewees were not comfortable with being audio recorded; these interviews were recorded via typing or taking manual notes during the interviews.

Numerous interdepartmental documentation such as the mobile device management policy, standards, processes, project plan, project scoping questionnaire, user and device information, mobile audit program, mobile computing audit report, IT mobility risks such as the risk of unsecure and unsupported usage of BlackBerry z10 devices and emails were obtained by the various research participants.

An email analysis was conducted for the second implementation between March 2013 and May 2013. The implementation was still in-progress at the time of the data collection stage of the research. The researcher used her discretion as to the best data collection method for the second implementation and since a case study allows for multiple sources of evidence, decided that an email analysis would suffice to triangulate the researcher's observations and conversations with the various implementation participants.

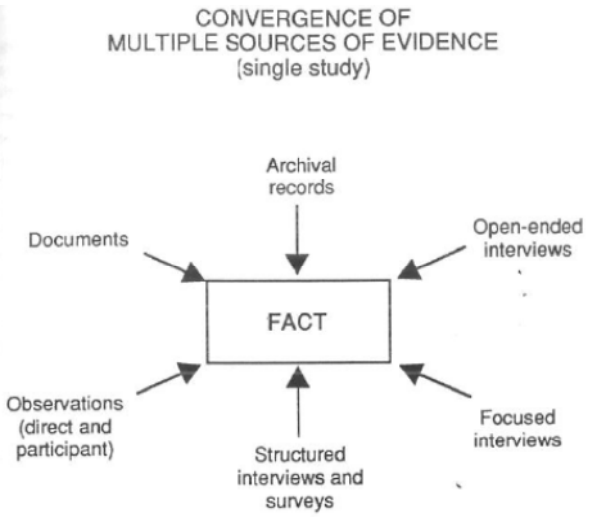


FIGURE 13 - CASE STUDY RESEARCH: DESIGN AND METHODS (YIN, 1994)

6.2.6.2 CREATING A CASE DATABASE

Yin (1994) suggests that a case study database may increase the reliability of the case study conducted since the evidence can be reviewed and is not limited to the written report. The researcher has therefore developed a formal, presentable database in which evidence such as case study documents, the time and place of interviews are all organised, categorised and available for access at a later stage. Table 1 is an extract of the case database.

TABLE 1 - CASE DATABASE

Source	Date	Time	Interviewee	Where	Hyperlink to information
Interview	08/03/2013	11:30 - 12:30	I1TA	Room 4.28	Interview Transcripts
Interview	18/04/2013	11:00 - 12:00	I1ITA	Room 3151	Interview Transcripts

6.2.6.3 MAINTAINING A CHAIN OF EVIDENCE

In an attempt to increase the reliability of the information in a case study, according to Yin (1994) a chain of evidence needs to be maintained. This principle allows the reader of the case study to follow evidence from the initial research question to the case study conclusion. For example, this means that the conclusion of the case study report should reference specific portions of the case study database such as interviews or documents and indicate the circumstances under which the evidence was collected. These circumstances should be consistent with the specific procedures followed which should show that the data collection has indeed followed the specified procedures. The researcher has attempted to maintain a chain of evidence so that clear cross-referencing to methodological procedures and evidence takes place (Yin, 2004).

6.2.7 DATA ANALYSIS

The data was transcribed immediately after each interview so that analysis could take place since data collection and data analysis according to the grounded theory method is carried out concurrently (Pozzebon et al., 2011) which increases the researcher's sensitivity to the concepts, their meanings and relationships (Strauss & Corbin, 1990). Data is analysed as it is collected (Pozzebon et al., 2011). This principle of constantly comparing means that as the data is collected it is constantly compared with concepts and categories being used which means that the theory that emerges is grounded in that data (Saunders et al., 2007).

Strauss and Corbin (as cited in Pozzebon et al., 2011) suggest three types of coding namely open coding which allows for the generation of concepts and categories, axial coding uses relationships to link categories to its subcategories and lastly, selective coding is searching through the categories that have been developed for a central phenomenon to which all categories can be linked to form a theoretical framework.

6.2.7.1 OPEN CODING

Open coding pertains to the naming and categorising of the phenomenon by breaking down the data into discrete parts. These parts are compared for similarities and differences and leads to questions being asked of the phenomenon as reflected in the data which allows the researcher to question her own assumptions about the phenomenon (Strauss & Corbin, 1990). This was the researcher's first step in the analysis of the data. The researcher broke down paragraphs, observations, sentences, ideas and events conceptually. These concepts were then grouped into categories which became the basis for theoretical sampling, meaning that the categories informed the focus in the next interview (Strauss & Corbin, 1990).

6.2.7.2 AXIAL CODING

Once the categories were established, connections between the categories and sub-categories were made to establish main categories. The focus of the category is on the conditions that give rise to the concept (the context), the action which handles it (strategy) and what happens as a result of those actions (consequences). The researcher alternated between open and axial coding during analysis (Strauss & Corbin, 1990). During axial coding sub-categories are linked to categories through the paradigm model displayed as:

"(A) CAUSAL CONDITIONS -> (B) PHENOMENON -> (C) CONTEXT -> (D) INTERVENING CONDITIONS -> (E) ACTION/INTERACTION STRATEGIES -> (F) CONSEQUENCES" (Strauss & Corbin, 1990, p. 99).

According to Strauss and Corbin (1990) the paradigm model will enable the researcher to systematically think about the data and to relate them in complex ways otherwise the researcher's grounded theory will lack precision and density.

During the research undertaken, the researcher attempted to understand the pre-implementation motives and activities (causal conditions), describe the actions and interactions of the information security governance implementation (phenomenon) and what the results of the information security governance implementation were (consequences). The researcher found that initially the easiest way to do this was by means of a diagram showing the relationships at a descriptive level. This was initially done at a descriptive level of detail and illustrated in Appendix E.

6.2.7.3 SELECTIVE CODING

The basis for selective coding has now been developed in axial coding. The integration of materials is not that much different from axial coding, it's just done at a higher level of abstraction. A movement from description to conceptualisation occurs, the core category is related to other categories by means of the paradigm model, the relationships are validated, patterns and connections are uncovered, and categories are grouped according to properties discovered in accordance with the patterns. Lastly, the theory is validated against the data which completes the grounding of the theory in data (Strauss & Corbin, 1990).

Figure 14 illustrates the movement from data in the empirical field to the abstraction field where possible concepts and categories are identified (Pozzebon et al., 2011). These coding methods are specific to the evolved grounded theory approach which can be used in the mixed method approach (grounded case study) according to the distinction made between all grounded theory approaches by Matavire and Brown (2013).

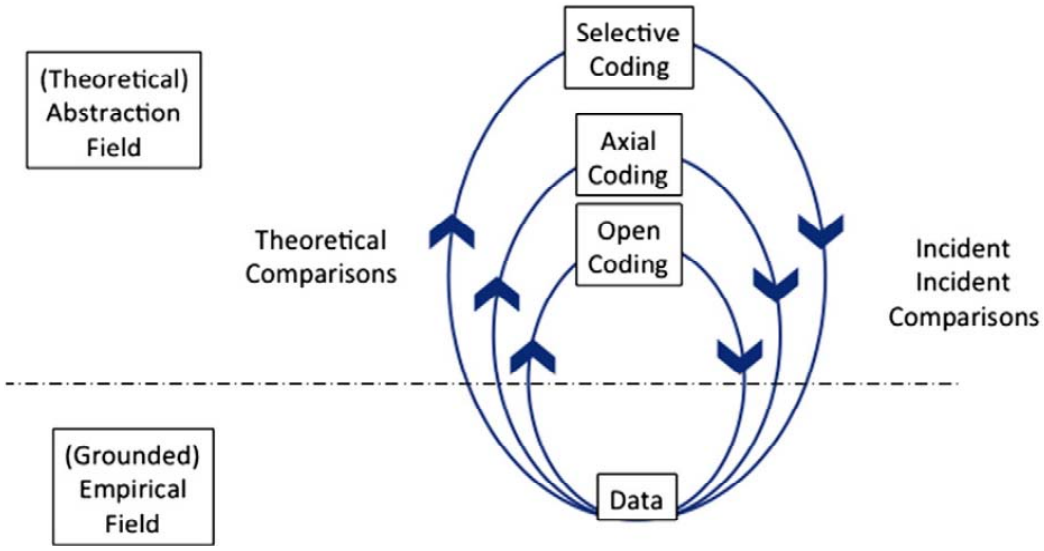


FIGURE 14 - THE CODING PROCESS (POZZEBON ET AL., 2011)

6.2.8 TIMEFRAME

Longitudinal research observes events and people over time and has the capacity to study change and development whereas cross sectional studies a particular phenomenon at a particular time (Saunders et al., 2007).

The research undertaken was cross sectional as the phenomenon of information security governance implementation was studied over a short period of time as a result of the time constraints imposed by the academic course undertaken (Saunders et al., 2007). The first interview took place in March 2013, the final analysis was completed in December 2013 at which point the final write-up of this dissertation continued.

6.2.9 SAMPLE

This section discusses the sample selection and the participants of the research.

6.2.9.1 SAMPLE SELECTION

The sample selection followed the process of theoretical sampling. Data was collected dynamically, guided by the process of theoretical sampling which means that once data has been collected and analysed, the researcher decided based on the analyses which additional data should be collected and analysed (Pozzebon et al., 2011). This process of theoretical sampling continued until the data collected no longer revealed new data relevant to a particular category. The categories at this stage were well developed and understood by the researcher as well as the relationships between categories. Once this happened it meant that theoretical saturation had been reached (Saunders et al., 2007).

The first implementation analysed followed theoretical sampling whereas, an email analysis of the second implementation was conducted. Since the research strategy was a grounded case study, multiple sources of evidence were allowed. Emails were regarded as company documentation.

6.2.9.2 CASE STUDY BACKGROUND AND PARTICIPANTS

There were two units of analysis (two implementations) within the case study which were analysed. This section discusses the case study backgrounds for both implementations and then goes onto discuss the participants of both implementations.

6.2.9.2.1 CASE STUDY BACKGROUND FOR FIRST IMPLEMENTATION

The research was conducted at a Retail organisation in 2013. Information security governance within the mobile device environment was intended to be implemented as part of the organisation's IT strategy but was expedited due to an impending mobility audit which used a best practice audit program to guide the audit. Information security governance was implemented in the mobile device management environment in 2012 and used the SAP Rapid Deployment Solution, which is a pre-configured guide, to conduct the implementation.

Prior to the implementation, employees had access to their company email on their personal mobile devices without any security controls in place (1.1.6). As a result, mobility became an item on the audit plan for the following reasons:

- the advancement in terms of technology within the industry,
- the increasing number of personal devices accessing company information
- the risks associated with mobile devices (1.2.1).

The risks associated with mobile devices are:

- the potential loss and leakage of confidential company information (1.2.3) and
- unauthorised access (1.2.7).

The project launched a tool that enforced the necessary controls to ensure that the company information accessed on mobile devices was protected (1.2.27; 1.1.20). The goals and objectives of the implementation were to:

- set the minimum security levels for mobile devices (1.3.30) such as pin, encryption and remote wipe (1.1.8)
- comply to internal audit
- have a timely adoption of mobile device management software
- have a capability to launch a mobile application deployment platform (1.4.7)

- ensure confidentiality of company information accessed on mobile devices (1.4.8).

6.2.9.2.2 FIRST IMPLEMENTATION PARTICIPANTS

The researcher had an idea as to who the participants were that would be able to make a contribution to this research. Usually with other qualitative methods all interviews are conducted first and then the transcriptions of the interviews are analysed whereas with the grounded theory method, data is analysed as it is collected (Pozzebon et al., 2011). The researcher, therefore, did not conduct all interviews first but made a decision after the data of each interview was analysed.

The participants listed below are those who have been interviewed as part of the first implementation as they were identified as being able to make a contribution to this research. The technical architect was the first interviewee as the researcher was aware that he played the role of the project manager and would be a rich source of information. The second interviewee was the internal IT audit manager at the company since one of the concepts that were identified as part of the first interview was the concept of “mobility audit” and the researcher felt the need to understand the perspective of the auditor with regards to the information governance implementation. The rest of the interviews were initiated in the same manner where the concepts identified led to the area of investigation. The aim of the researcher was to understand the perceptions of the participants listed with regards to the activities required prior, during and after the implementation of information security governance.

- Technical architect
- IT audit manager
- Mobility consultant
- Information security specialist
- Systems engineer

6.2.9.2.3 CASE STUDY BACKGROUND FOR IMPLEMENTATION TWO

Company smartphone devices were not managed within the Information Services department but by the company's Procurement department. The company standard device was determined by the Procurement department a number of years ago and when employees were due for upgrades, the most logical choice of device was the next generation mobile device of the same brand. Unfortunately, due to the fact that this smartphone device worked completely different to the older generation device, this smartphone device was not compatible with the existing technology infrastructure implemented during the first implementation and, therefore, the implementation of this new mobile device was initiated.

6.2.9.2.4 SECOND IMPLEMENTATION PARTICIPANTS

An email analysis was done as part of the second implementation. Documentation analysis was allowed as part of the grounded case study, the researcher regarded email communication as documentation. The participants listed below formed part of the email analysis. The aim of the researcher was to understand how the information security governance that had been implemented as part of the first implementation impacted on the second implementation.

- Senior buyer
- IT manager
- Technical specialists
- Technical architect
- Procurement officers
- Architecture specialist
- Enterprise risk and assurance manager
- Architectures, governance and security manager
- End users
- Group risk manager
- Chief information officer

The analysis of the second implementation aided the researcher's understanding as to what impact the information security governance implemented will have on future

or subsequent implementations. This will provide some guidance for other organisations with their information security governance initiatives.

6.2.10 ETHICS

An introductory letter (Appendix B) using the UCT letterhead requesting permission for the research to be conducted at the organisation was provided. A summary explaining the intention of the research prior to the interview was provided to the stakeholders of implementation one (Appendix C). They were also informed that they are not obligated to participate, it was completely voluntary. Written consent was not obtained as it was implied by the acceptance of the interview.

For the email analysis of implementation two, a summary and cover letter was sent to all email participants (Appendix D). It was agreed with the email participants that the CIO would signoff the completed dissertation before being submitted to UCT to ensure that confidential company information, the company name or participant names were not used.

Walsham (2006) discusses three specific domains of practice namely, confidentiality and anonymity, working with the organsiation and reporting in the literature and offers some practical ways of attempting to resolve ethical issues in these domains. The researcher intends following these suggestions as described in the section below.

6.2.10.1 CONFIDENTIALITY AND ANONYMITY

The participants that have been interviewed are not indentified by name in any written work. Ethical problems may be encountered such as the fact that it may be possible for individuals to make an informed guess as to who the particular views belong to even though no names have been mentioned. Also when reporting in the literature on the views of senior people such as the CEO, it may be possible to guess who is being discussed based on the contexual information provided even though the name of the company is omitted (Walsham, 2006).

6.2.10.2 WORKING WITH THE ORGANISATION

Many IS interpretive researchers may be faced with the decision as to how to convey "bad news" discovered or even whether it should be. The tendancy is to phrase it in opportunities rather than problems. Walsham (2006) suggests that a presentation or workshop would be easier to convey the "bad news" than a written report.

6.2.10.3 REPORTING IN THE LITERATURE

The moral dilemma of truthful reporting against expedient reporting is raised because participants do not want their organisation to be portrated in a negative light in published works. In a case like this, the researcher will make sure that the article is submitted for publication long after the submission of the paper so that any critical comments about the organisation are less problematic for the organisation (Walsham, 2006).

7 ANALYSIS AND RESULTS

The initial information security governance implementation within the mobile device environment was analysed first. Afterwards, an email analysis of a second mobile device implementation was analysed to understand the impacts that the implemented information security governance would have on subsequent implementations.

7.1 IMPLEMENTATION ONE ANALYSIS

Implementation one refers to the implementation of information security governance within the mobile device environment. The goals and objectives of the implementation as specified earlier were to:

- set the minimum security levels for mobile devices (1.3.30) such as pin, encryption and remote wipe (1.1.8)
- comply to internal audit
- have a timely adoption of mobile device management software
- have a capability to launch a mobile application deployment platform (1.4.7)
- ensure confidentiality of company information accessed on mobile devices (1.4.8).

7.1.1 DRIVERS OF MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION

The drivers of the mobile information security governance implementation were the reasons for the implementation taking place. Three sub-categories with 6 concepts were identified as shown in Table 3. Each sub-category and concept is discussed further and shows how the emerging theory is generated.

TABLE 2 - DRIVERS OF MOBILE SECURITY GOVERNANCE IMPLEMENTATION

Sub-category	Concepts	Incidents	Supporting evidence	Source
Mobility strategy	Mobile device management solution	2	part of the strategy was always to have an MDM, umm but as I mentioned earlier, MDM solutions are fairly, at that point were immature.	1.1.19
			So by taking an overall view of mobile device management [Company] could therefore comply to audit and at the same time leverage opportunities.	1.4.6
	Mobile application deployment platform	2	Some other goals and objectives were to have a timely adoption of mobile device management software. Additional goals were to have a capability to launch or to have a mobile application deployment platform for [Company] so we could deploy [Company] developed applications to smartphones.	1.4.7
			Those opportunities included applications development within the mobile space where services could be offered to [Company] users and potentially external user which could include dealers.	1.4.6
Risk to company information	Risk associated with mobile devices	4	It was initiated because of the risk associated with mobile devices and increasing number of users that is using their devices accessing company data.	1.2.1
			From risk within the company, what was happening in industry, newsletters, conferences (1.2.4).	1.2.4
	Company data loss/leakage	6	Because of risk of loss of information and leakage of confidential information it landed on the audit plan.	1.2.3
			To ensure that probably any sensitive information does not get leaked to the wrong hands, to it's competitors you can say	1.5.16
	Unauthorised access	2	The biggest risk was unauthorised access and loss of data.	1.2.7
Mobility audit	Audit compliance	14	MDM was forced upon us by audit	1.1.1
			It was initiated partly because of internal audit pressures, pending audit against our environment. Our audit department from various sources determined that mobility was a risk and they would need to pay attention to this area within [Company].	1.4.5
	Audit responsibility	1	responsible for execution of IT audits basically identifying the potential audits for the year, to physically do audit, report to audit committee on a quarterly basis	1.2.28
	Risk to company information	4	I don't know if it was implemented because of audit. Because of what's happening in industry in terms of technology and then also risk. Because of risk of loss of information and leakage of confidential information it landed on the audit plan.	1.2.3

			From risk within the company, what was happening in industry, newsletters, conferences.	1.2.4
			I would start with policies and procedures and talk to people responsible for the process. Identify risk to process and link to specific controls. Assess risk in terms of impact and likelihood of occurring. The impact assessment part looks at risk with considering control. Likelihood considers controls (1.2.23).	1.2.23

7.1.1.1 MOBILITY STRATEGY

7.1.1.1.1 MOBILE DEVICE MANAGEMENT SOLUTION

The mobile device management solution was part of the company's mobile strategy and was required to apply security controls to all mobile devices accessing company information. This implementation was expedited due to the pending mobility audit regarding the security of mobile devices.

7.1.1.1.2 MOBILE APPLICATION PLATFORM

The implementation of the mobile device management solution was further required to fulfil the mobile strategy of providing the company with a mobile application development platform from which the company would be able to deploy mobile applications to smartphone and tablet devices.

7.1.1.2 RISKS TO COMPANY INFORMATION

7.1.1.2.1 RISKS ASSOCIATED WITH MOBILE DEVICES

A number of sources such as newsletters, conferences and industry information raised awareness with regards to the risk associated with mobile devices. There was an increase in the number of users accessing company information on their mobile devices and there was a need to mitigate these risks. Two types of risks were particularly mentioned and discussed further.

7.1.1.2.2 COMPANY DATA LOSS/LEAKAGE

The increase in the number of users accessing company information on mobile devices that were not protected was a concern due to the possibility of the leakage or loss of confidential company information. Concerns such as company information being stolen and sent to competitors were raised.

“Then again there’s the problem with the contacts, if you have all your organisation’s contacts on your device then people can steal your contacts” (1.3.25).

7.1.1.2.3 UNAUTHORISED ACCESS

Users that were not authorised to have access to confidential company information were raised as a concern. The mobile device management implementation was required to ensure that a certain level of confidentiality and assurance was provided for employees accessing their company information on their mobile device.

7.1.1.3 MOBILITY AUDIT

7.1.1.3.1 AUDIT RESPONSIBILITY

The Enterprise Risk and Assurance department is responsible for identifying annual IT audits, the execution of the audits and the reporting of audit related information. A number sources such as information with regards the advancement of technology within the industry, conferences and newsletters identified that company information stored on mobile devices was a risk and therefore it was selected as an item on the audit plan.

7.1.1.3.2 AUDIT COMPLIANCE

The concept of audit compliance was highlighted by all employees, except the auditor, as one of the main reasons or drivers for the initiation of the mobile information security governance implementation.

Although the mobility audit was a major driver of the implementation, the mobility audit was not dependent on the implementation. The mobility audit would have gone ahead whether or not the implementation was complete.

“Even if IS didn’t implement, audit would have gone ahead. They were proactive in implementing the tool” (1.2.8)

7.1.1.4 RISKS TO COMPANY INFORMATION

From an audit perspective, as mentioned earlier, company information stored on mobile devices was seen as a risk and was, therefore, selected as an audit item on the audit plan. A relationship has therefore been identified and discussed below.

7.1.1.4.1 RELATIONSHIP BETWEEN 'MOBILITY AUDIT' AND 'RISKS TO COMPANY INFORMATION'

A relationship between the sub-categories 'Risks to company information' and 'Mobility audit' was identified. The evidence of the relationship is highlighted in Figure 15 below; showing that from an audit perspective the main concern was to mitigate the risks to company information.

"I don't know if it was implemented because of audit. Because of what's happening in industry in terms of technology and then also risk. Because of risk of loss of information and leakage of confidential information it landed on the audit plan" (1.2.3).

FIGURE 15 - RELATIONSHIP BETWEEN AUDIT AND RISKS

'Risks to company information' initiates the 'Mobility audit'.

7.1.1.5 EMERGING THEORY IN-PROGRESS

The discussion with regards to the drivers of mobile device management implementation including the relationship identified is depicted in Figure 16 below and will be further developed as the various categories and concepts are discussed.

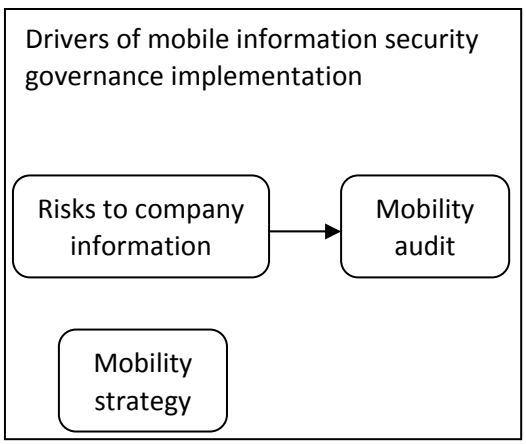


FIGURE 16 - DRIVERS OF MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION

7.1.2 PROVIDE SECURE ENVIRONMENT

In an attempt to provide a secure environment for the company, the Information Services department plans various initiatives relating to their strategies and the Enterprise Risk and Assurance department in a similar fashion identifies areas that may pose as a risk to company information.

Evidence of this can be found in table 4 below.

7.1.2.1 PROTECT COMPANY INFORMATION

TABLE 3 - PROTECT COMPANY INFORMATION

Sub-category	Concepts	Incidents	Supporting evidence	Source
Provide secure environment	Protect company information	6	... the person above them understands the strategic intent of what's happening so that it was to provide a secure environment for the company ...	1.1.20
			the goals and objectives were to set the minimum security levels for devices that umm were interacting with the email because that was the first access to corporate data that mobile devices had	1.3.30
			... there are controls in place. We are trying to secure our information	1.1.20
			There were business reasons around securing data, knowing which devices were connecting, knowing who umm, the capabilities were, we had to have encryption, pin and I forget the 3rd one.	1.1.8
			Pin, encryption, remote wipe, device must be compatible with MDM software	MDM Policy
			The project was basically to launch a tool with the relevant controls to ensure that the data is protected on mobile devices...who can view data	1.2.27

7.1.2.2 PROTECT COMPANY INFORMATION

Ultimately, it doesn't matter whether the drivers of the implementation are viewed from the mobility strategy perspective or the audit perspective because they both have a common goal which is to protect the company's information as depicted in Figure 17.

"audit said that they were going to do a mobility audit, umm, at the same time so who knows which came first. We were told to implement the MDM solution" (1.1.4)

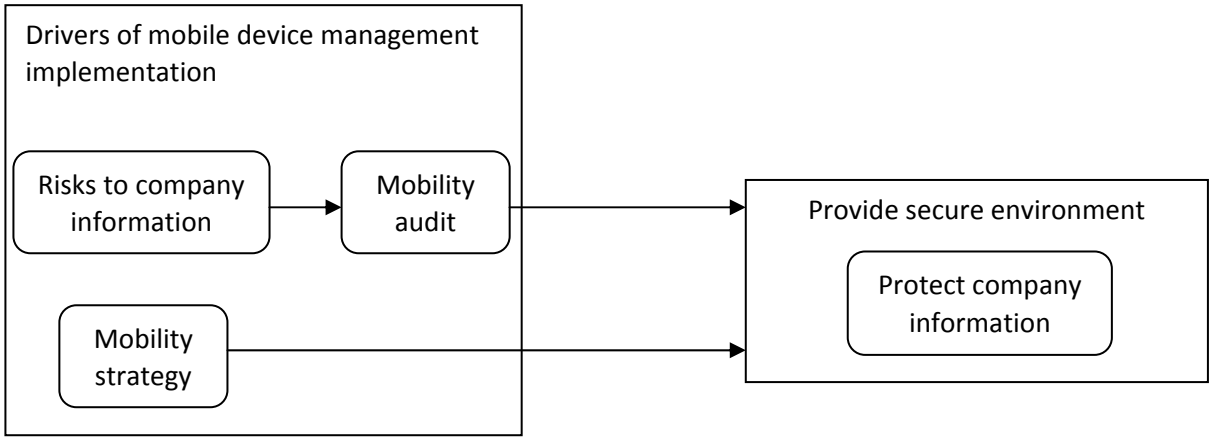


FIGURE 17 - PROVIDE SECURE ENVIRONMENT

7.1.3 MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION

The mobile information security governance implementation consists of 7 sub-categories (time pressure, team diversity, governance artefact development, change management, device education adequacy, communication extent, and stakeholder involvement) as shown in Table 5 and Table 6 below.

TABLE 4 - MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION

Sub-category	Concepts	Incidents	Supporting evidence	Source
Time pressure	Time pressure	9	there was a limited time before the audit happened	1.3.23
			Those things should be decided up front and should be implemented from the onset, not as an after thought, because then you make somebody use to a system and then you just change it. It kind of makes it seem like it was just a rushed implementation	1.5.14
			We were very constrained by the time that we needed to implement.	1.4.24
			The dates of the audit was the big driver because we wanted to comply with the audit.	1.4.9
			The implementation was expedited, we could have communicated to internal IS staff better	1.4.25b
			Having more time could have enabled us to have a more complete communication plan. Also, it could have allowed more indepth analysis of other technologies and vendors.	1.4.25
			we have different types of packages how we implement things so what [Company] chose to do was to do it the quickest way	1.3.31
			The choice of solution had been expedited by management in order to meet the internal audit that was due. They wanted to have a solution in place to meet the audit that was about to take place.	1.4.11
			We had a very short timeframe to get this in	1.1.29

Team diversity	Team diversity	3	as the technology person, well i became the project manager for the implementation and i got a change manager who didn't come to the party. Umm, I had a technical team, I had SAP doing the implementation themselves and we were through their Rapid Acceleration programme, something like that, umm, which they have a methodology to implement umm Afaria umm. I had the policies and governance people to assist on that side	1.1.28
			We knew that umm doing it with the required stakeholders umm would create, would be the fastest way to get it in. I took a lot of heat, umm from a lot of people	1.1.10
			What we find with a lot of projects, the more people you get involved, the slower the project goes. We didn't have the luxury to do that	1.1.10a
Governance artefact development	Governance artefact development	4	Mobile device management policy Mobile device management software Mobile device management processes Mobile device management standards	Outputs of Implementation
	MDM Policy		MDM policy is one of the more stringently managed policies within [Company]. It has a much higher visibility within IS. As far as the approvals are concerned, it needs to be approved by a core set of individuals which is over and above our standard information security policies.	1.4.17
	MDM process		There's been communication about MDM, it's been integrated into the service desk, users are aware of the process that they should follow to access [Company's] information.	1.4.28

7.1.3.1 TIME PRESSURE

The implementation had a limited amount of time within which to complete since one of the drivers of the implementation was to comply with the upcoming mobility audit. One of the ways to alleviate the time pressure was to have a dedicated team as discussed below.

7.1.3.2 TEAM DIVERSITY

As a result of the time pressure being experienced, it was felt that the quickest way to complete the implementation before the mobility audit was to have a small dedicated team since it was believed that this would speed up the implementation process. This led to the exclusion of important stakeholders such as those who would ultimately be responsible for supporting the infrastructure. A bigger team of people would probably not have made a difference but a more diverse group of people, which included the infrastructure support people, would most likely have

contributed to a more successful implementation. Figure 20 highlights that a lack of 'Team diversity' had a negative impact on 'Stakeholder involvement'.

The relationship between these two concepts is shown in Figure 18 with the supporting evidence in the next section.

7.1.3.3 RELATIONSHIP BETWEEN 'TIME PRESSURE' AND 'TEAM DIVERSITY'

The relationship between the sub-categories 'Time pressure' and 'Team diversity' has been identified with the quotes below and depicted in Figure 18.

"We knew that umm doing it with the required stakeholders umm would create, would be the fastest way to get it in." (1.1.10)

"What we find with a lot of projects, the more people you get involved, the slower the project goes. We didn't have the luxury to do that" (1.1.10a)

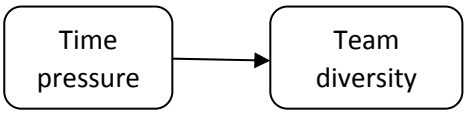


FIGURE 18 - RELATIONSHIP BETWEEN TIME PRESSURE AND TEAM DIVERSITY

'Time pressure' has a negative impact on 'Team diversity'.

7.1.3.4 RELATIONSHIP BETWEEN 'TIME PRESSURE' AND 'MOBILITY AUDIT'

The completion date of the implementation was driven by the date that the mobility audit was taking place. The relationship between the sub-categories 'Time pressure' and 'Mobility audit' has been identified with the quotes below and depicted in Figure 19.

"there was a limited time before the audit happened." (1.3.23)

"The dates of the audit was the big driver because we wanted to comply with the audit." (1.4.9)

"The choice of solution had been expedited by management in order to meet the internal audit that was due. They wanted to have a solution in place to meet the audit that was about to take place." (1.4.11)

'Mobility audit' caused 'Time pressure'.

7.1.3.5 GOVERNANCE ARTEFACT DEVELOPMENT

As part of the mobile information security governance implementation, a number of artefacts were developed or can be seen as outputs of the implementation such as the:

- Mobile device management policy
- Mobile device management software
- Mobile device management standards
- Mobile device management processes

7.1.3.6 RELATIONSHIP BETWEEN 'GOVERNANCE ARTEFACT DEVELOPMENT' AND 'MOBILITY AUDIT'

The starting point of the mobility audit was the governance artefacts used to govern the mobile device environment. The governance artefacts, therefore, needed to be in place before the audit took place. The policies, procedures and processes were reviewed as part of the mobility audit so that any risks within the mobile device management area would be identified and assessed. Evidence of this can be seen in the below quote and depicted in Figure 19:

"I would start with policies and procedures and talk to people responsible for the process. Identify risk to process and link to specific controls. Assess risk in terms of impact and likelihood of occurring. The impact assessment part looks at risk with considering control. Likelihood considers controls" (1.2.23).

'Mobility audit' initiates 'Governance artefact development'.

7.1.3.7 UPDATED EMERGING THEORY IN-PROGRESS

The theory is further elaborated as shown in Figure 19 below with the categories, concepts and relationships discussed.

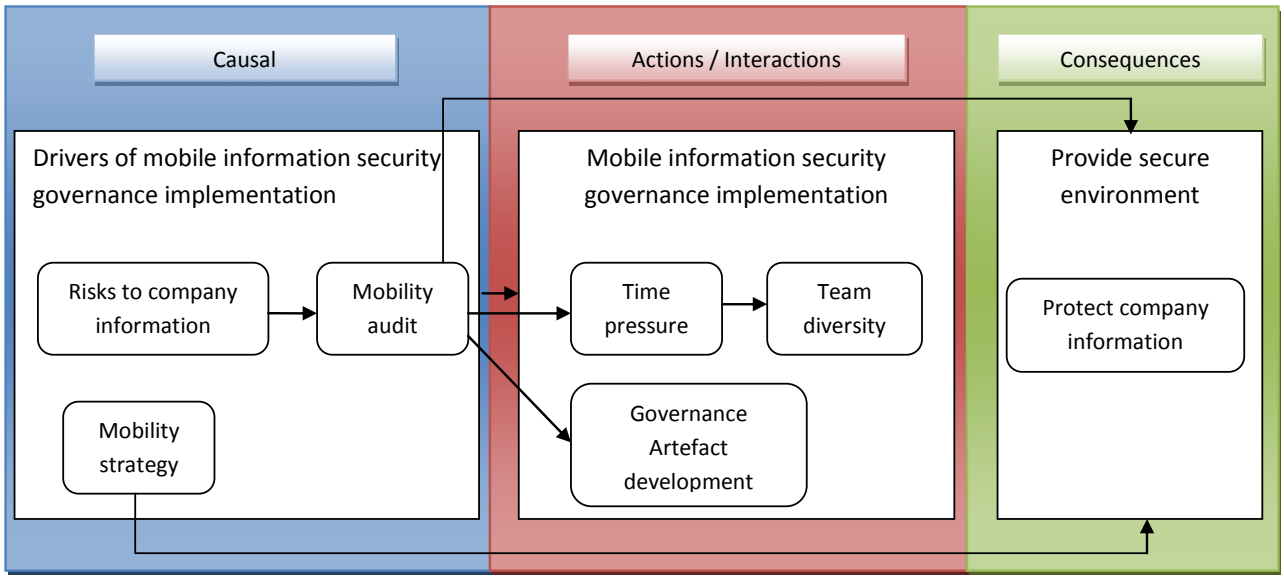


FIGURE 19 - MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION

7.1.3.8 CHANGE MANAGEMENT

The data incidents of concepts within the category of change management indicate that not a lot of thought went into the aspect of change management, device education and communication during the implementation. The evidence of these concepts are shown below in Table 6 and each concept is further described in the below section.

TABLE 5 - CHANGE MANAGEMENT

Sub-category	Concepts	Incidents	Supporting evidence	Source
Change management	Change management	3	The issues came around the change management and I don't know what we can change for it to get better because it was so heated.	1.1.16
			as the technology person, well i became the project manager for the implementation and i got a change manager who didn't come to the party.	1.1.28
			the change management process that has to go in with the solution like this which wasn't actually done but anyway.	1.3.2
Device education	Device education	3	so why didn't you consult us first and that's a big education	1.3.13

adequacy			like for me personally, even like this whole threat of malware it doesn't have impact on me, I don't understand why I need to have a umm anti-virus on my mobile device right so, if there was more education around it then maybe I would understand. The same thing with MDM, it has a bigger impact because of the data involved and because it's private data but there's not a lot of communication.	1.3.26
			I think it's an education part, I mean, it is IS's responsibility to educate the users about information security, so they tell them these are the devices if you want to access your corporate email on devices, these are the devices we will allow you to do and then IS is the organisation that holds this so therefore they should push this information out to the general public so that they know oh if I go and buy a windows phone, I'm not gonna get my email, do I still want it?	1.3.14
	User behaviour	5	a big part of mobile information security is also the end user behaviour right whether they leave their device unattended at the airport while they browsing all those sort of things and that should be part of the change management or the education that is rolled out to the users when we dealing with MDM and for me that wasn't done so I do think that's a big part that's missing	1.3.17
			when I think about governance also I think a lot comes down to the individual himself and to ensure that he is responsible for who he shares his information with if he deals with any sensitive information	1.5.18
			the human behaviour the users behaviour still has a very big impact in that, I think that's also part of the process and part of the knowledge that must be delivered to the end users	1.3.29
			We included it in our induction process but I don't think it's sufficient. People give their laptops to the kids with all the information on it. We don't have a mature culture. We have fancy tools but business is not on board yet.	1.2.25
			It comes down to [Company] behaviours and users need to comply to the policy although there might not be a technology control to enforce it. Not possible to enforce everything in policy so we rely on user's behaviour.	1.4.16
Communication extent	Communication to end users	10	So, you don't think that people actually understand why we did. No, not at all	1.3.18
			i think that just the knowledge to the end users, the end users were never really taken into account	1.3.28
			They also did not understand what we could access that wasn't clearly communicated to them as to where the boundaries were	1.5.10
			I think more consultation with the business would have been better, would have made the acceptance of the application smooth instead of people feel that they were forced to do this.	1.5.11
			I think just the communication to the users.	1.5.13

			More and better communication with the business, informing them about the reason and importance of information security and why it is being rolled out .	1.2.19
			It was affecting the majority of users that were accessing [Company]'s information, there was a lot of resistance. Having more time could have enabled us to have a more complete communication plan.	1.4.25
			there was no communication to the end user	1.3.16
			if there was more education around it then maybe I would understand. The same thing with MDM, it has a bigger impact because of the data involved and because it's private data but there's not a lot of communication. In all companies I've seen that's installed it there's not a lot of information around why this thing has to be installed and must have a password. It's just seen as another process that business want	1.3.26
			because none of this information was given to the user, they didn't actually know so it was complaints, and lots of umm, scary rumours running around. If you install Afaria it will wipe your phone, once it installs it, it first wipes and then you secure	1.3.5
	Communication to technical employees	2	SAP Basis team were not aware of policy statements regarding the collection of data. Low awareness of policy within the IS team.	Observation
			The implementation was expedited, we could have communicated to internal IS staff better	1.4.25b
Stakeholder involvement		6	One thing that bothered me with the entire implementation was that there was no discussion. I was just told that this was the product that we are going to be using and that I was going to be looking after it. I'd be the last point of call from [Company] if anything should go wrong, whether it was server, policy.	1.5.2
			I would have loved to be involved from the start so I could see what a competitor or a different product has to offer. I would like to know why we chose Afaria. What made Afaria the choice. When from what I could see, that the system was not the best system out there or it wasn't the easiest implementation, let's put it like that.	1.5.15
			maybe it must be brought together a bit more because when we initially did the installation we never involved Basis, they were never a part of it.	1.3.22a
			Then we needed to install a dev server and that's when Basis actually got involved discussions around who owns what. That never happened in the initial implementation. Again it was the whole siloed approach, we just dealt with one stakeholder	1.3.22
			it seemed like the implementation was a bit siloed that it was implemented, this is what we doing and we don't care about the rest of the organisation, we doing it this way and you guys must just do it.	1.3.15

			Initially no, umm when there were changes I was explained the policies. When I initially spoke to the third party contractor I asked him if [Company] ever need to create, would I need to create more policies and I was told no. So, the policies that were setup were given to me with the system. Then I wanted to know, would we ever need to develop our own policies, would I need to learn how to create policies and I was told, no, not at that point.	1.5.8

7.1.3.8.1 CHANGE MANAGEMENT

The mobile device management implementation consisted of a small dedicated team of people which included a change manager. The data indicates that the lack of change management could be attributed to the change manager who was assigned to the implementation. Since the characteristics of a good change manager was not the focus of this research, the relationship between the lack of 'Change management' and the 'change manager' was not further investigated. The category of 'Change management' was further analysed according to the various sub-categories identified.

7.1.3.8.2 DEVICE EDUCATION ADEQUACY

The sub-category 'Device education adequacy' consists of two concepts namely, 'Device education' and 'User behaviour'.

7.1.3.8.2.1 DEVICE EDUCATION

The mobile device management software implemented supported specific mobile device types based on the operating system installed on the device. From a technology perspective one of the biggest challenges faced, was device fragmentation which refers to the different types of mobile devices that were available to users on the market. This will remain an ongoing problem for organisations due to technology advancement.

"..fragmentation, the biggest thing is fragmentation." (1.3.32)

The mobile device management software did not support all mobile device types. It was, therefore, important that the employees at the company who required access to their company information using their mobile device were educated on which devices or operating systems would be supported.

"I think it's an education part, I mean, it is IS's responsibility to educate the users about information security, so they tell them these are the devices if you want to access your corporate email on devices, these are the devices we will allow you to do and then IS is the organisation that holds this so therefore they should push this information out to the general public so that they know oh if I go and buy a windows phone, I'm not gonna get my email, do I still want it?"? (1.3.14)

The education regarding the supported mobile devices or operating systems was not done as part of the implementation which resulted in consequences for the employees which are discussed later. If it had been done, the user's expectation would have been managed better.

"the user's expectation is that it should work with everything" (1.3.12)

7.1.3.8.2.2 USER BEHAVIOUR

The second concept identified as part of the sub-category 'Device education adequacy' was 'User behaviour'. The company has no control over the behaviour of the employees. The company entrusts its employees with company assets, whether it is hardware such as devices or soft copies of information that resides on those devices, whether they are company-owned or personal. Employees may not be aware of the dangers of leaving their devices unattended while at the airport or simply sharing sensitive company information with individuals that should not have access to the information provided. One way of familiarising employees with the dangers relating to their behaviour and the information security of company assets is through education. Education with regards to user behaviour was not done as part of the implementation and is an important factor to consider since it is not possible to enforce everything in policy. The behaviour of employees is relied on.

"...should be part of the change management or the education that is rolled out to the users when we dealing with MDM and for me that wasn't done so I do think that's a big part that's missing" (1.3.17)

7.1.3.8.3 COMMUNICATION EXTENT

'Communication extent' had the most number of data incidents compared to the other sub-categories within 'Mobile information security governance implementation'. The number of incidents for 'Communication to the end user' outweighed the number of incidents for 'Communication to technical employees'.

7.1.3.8.3.1 COMMUNICATION TO END USER

A more robust communication plan would have made the transition for users easier. Due to the lack of communication, employees had a low understanding of what the implementation was trying to achieve. The reasons and importance of information security must be communicated to the end user. If this was done, there most probably would have been less resistance and a smoother acceptance of the software.

7.1.3.8.3.2 COMMUNICATION TO TECHNICAL EMPLOYEES

Some of the technical employees were not aware of the contents of the mobile device management policy or even that the mobile device management policy existed.

7.1.3.9 RELATIONSHIP BETWEEN 'TIME PRESSURE' AND 'COMMUNICATION EXTENT'

A relationship was identified between the concept, 'Time pressure' and the concept, 'Communication extent', related to 'Change management'.

"It was affecting the majority of users that were accessing [Company]'s information, there was a lot of resistance. Having more time could have enabled us to have a more complete communication plan."(1.4.25)

"Time pressure' negatively impacts on 'Communication extent'.

7.1.3.10 STAKEHOLDER INVOLVEMENT

Due to the time pressure which led to a small dedicated team of people, there was a lack of stakeholder involvement in the implementation. Important stakeholders required to support the infrastructure and application were either not involved at all, or were only involved at the end of the implementation and explained that they would be supporting the application.

7.1.3.11 RELATIONSHIP BETWEEN 'STAKEHOLDER INVOLVEMENT AND 'TEAM DIVERSITY'

The relationship between the concept 'Stakeholder involvement' and 'Team diversity' has been identified as follows:

"Then we needed to install a dev server and that's when Basis actually got involved discussions around who owns what. That never happened in the initial implementation. Again it was the whole siloed approach, we just dealt with one stakeholder" (1.3.22)

Lack of 'Team diversity' negatively impacts on 'Stakeholder involvement'.

Figure 20 shows an updated version of the emerging theory illustrating the inclusion of the 'Change management' category and sub-categories together with their relationships.

7.1.3.12 UPDATED EMERGING THEORY IN-PROGRESS

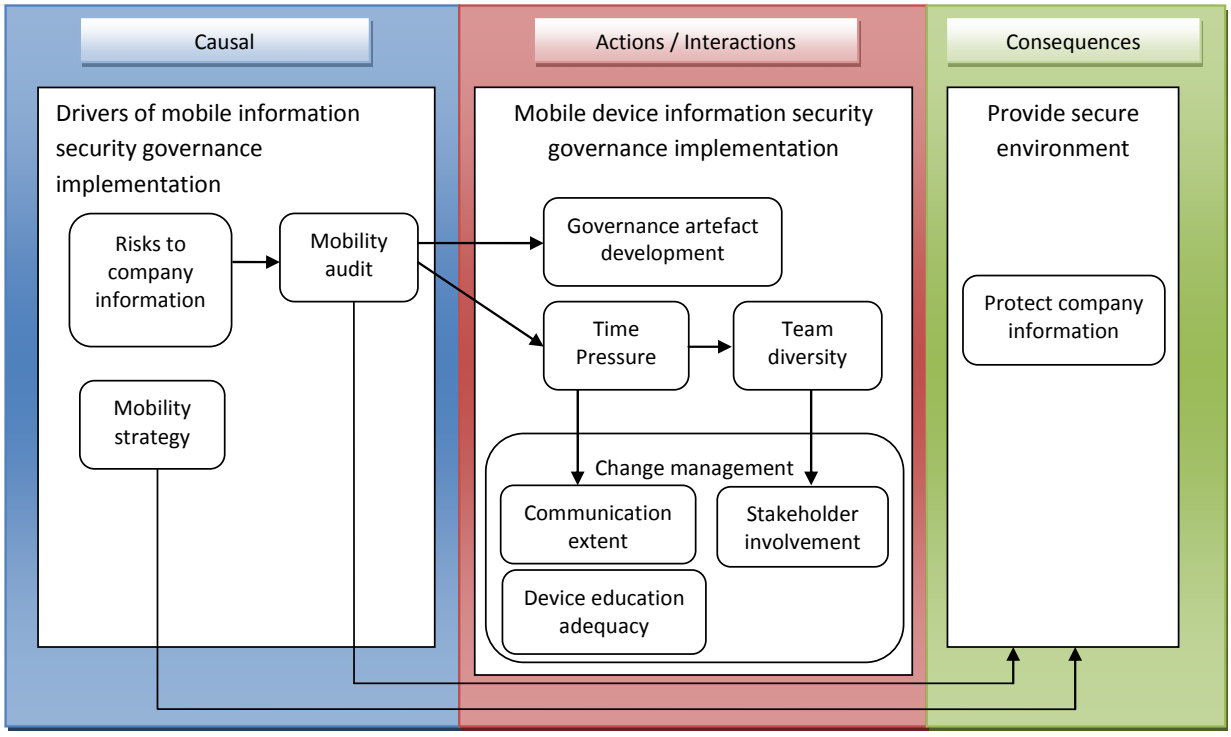


FIGURE 20 - CHANGE MANAGEMENT

7.1.4 EMPLOYEE DISSATISFACTION

The sub-category 'Employee dissatisfaction' consists of five concepts as shown in Table 7 below.

TABLE 6 – EMPLOYEE DISSATISFACTION

Sub-category	Concepts	Incidents	Supporting evidence	Source
Employee dissatisfaction	User resistance	7	No, even the CEO didn't want it on his ipad.	1.2.5
			It was affecting the majority of users that were accessing [Company]'s information, there was a lot of resistance.	1.4.25c
			Initially there were a number of individuals that were not receptive to the software	1.4.13b
			People. they were not very receptive.	1.5.7a
			there were some concerns about [Company] accidently wiping their phones	1.4.13c
			The issues came around the change management and I don't know what we can change for it to get better because it was so heated err what we found that umm there was a lot of noise initially umm but after 2 weeks it disappeared,	1.1.16
			They don't understand, they don't see it as a positive step to securing information, it's a hassle, more work, not positively received by audience.	1.2.15
	Personal Device affected	9	The access of users of Nokia devices that were not compatible with existing MDM software had to be disabled due to an audit finding. Users unhappy because it meant that they would have to upgrade their devices even though they did have a PIN on their device. Devices do not support encryption.	D1
			Nokia user was unhappy about his access being taken away and also with the fact that he had to have an alphanumeric pin - (not the proper standard applied); Once access was removed, IT had to help with removing the PIN from the phone.	C1
			people were complaining about battery power, that their devices were umm, getting run down	1.3.3
			it drained up their battery	1.1.24b
			it used up their data	1.1.24c
			For one, they didn't like the extra password	1.5.7c
			we inadvertently collected possibly personal information, not on purpose, which we said we would not (1.4.13e)	1.4.13e
			and we have denied people access / stopped people from having access to the information that they previously had because their device was not supported by our choice of software	1.4.13
			we have accidently locked a user out of his data where they were not able to recover – there was a loss of personal data	1.4.13d
	Personal data leakage	2	Not necessarily because we had a lot of business push back. It meant a lot more work on their part. They had to change their Pin and was scared that personal data would leak.	1.2.2

			People are scared that the administrator might make changes to the Afaria application and the personal data would be exposed.	1.2.18
	Privacy	4	the complaints that the customers/ users didn't understand what Afaria was doing. They believed that Afaria was running all the time, looking at what they were doing, looking at their phone calls, reading sms's, looking at what what webpages they were looking at	1.3.4
			Privacy, umm reduced capability of their phones so I think that's the right way to put it, it drained up their battery, it used up their data.	1.1.24
			Some of the concerns were that [Company] would be collecting personal information	1.4.13a
			if the person above them understands the strategic intent of what's happening so that it was to provide a secure environment for the company and all these people sort of complained about their personal umm, their privacy, once, at the GM level, they were able to say well, it doesn't affect your privacy, there are controls in place. We are trying to secure our information	1.1.20
	Control of personal device	4	There political challenges, lets put it that way, err where we expected it was going to be err rough thing, a rough situation due to the fact that we were telling users that if they wanted to connect to our environment, we had to have control over their devices.	1.1.9
			people were unhappy that we had the ability to manage and remote wipe their phones.	1.5.9
			because none of this information was given to the user, they didn't actually know so it was complaints, and lots of umm, scary rumours running around. If you install Afaria it will wipe your phone, once it installs it, it first wipes and then you secure	1.3.5
			they didn't like the idea of somebody else being able to control what's on their personal phones	1.5.7b

7.1.4.1 EMPLOYEE DISSATISFACTION

The change management aspect of an implementation provides an easier transition for end users and when it is not done in an effective way or not at all, it leads to a number of consequences which need to be dealt with. As a result of the lack of change management during the implementation, there were five concepts that were highlighted. These are described further.

7.1.4.1.1 USER RESISTANCE

Users resisted installing the mobile device management software on their device because they were unsure of what the consequences would be. The users did not view it as a way of securing the company information; instead they were afraid that their data would be accidently wiped from their device. Users did not have an

understanding of what the implementation was about or what was trying to be achieved.

7.1.4.1.2 PERSONAL DEVICE AFFECTED

Once the mobile device management IT system policies were applied to user's devices, there were a number of complaints related to the affects it had on the devices. Users were unhappy about being forced to have a password on their device and they complained about the fact that their battery life had been affected. Some mobile device users that previously had access to their company information on their mobile devices were no longer able to access the same information because their devices were not compatible with the mobile device management software or the devices did not support encryption, which was one of the security controls enforced.

7.1.4.1.3 PERSONAL DATA LEAKAGE

Users were afraid that the administrators would have access to their personal data on their mobile device or that a small change could be made and, therefore, expose personal data stored on the device. To alleviate these concerns the data collected by the mobile device management software was documented so that users were aware of what data was being collected.

The mobile device management policy specifically states that any changes to the data collected would need to be approved and all employees would be informed and would have the opportunity to rather opt-out of having access to company information on their mobile device.

7.1.4.1.4 PRIVACY

Users did not have an understanding of what the mobile device management software was doing to their device and felt that it was an invasion of their privacy. Users were under the impression that all their activities whether it was a phone call, sms or browsing were being saved and somehow accessible by the administrators.

7.1.4.1.5 CONTROL OF PERSONAL DEVICE

Users were unhappy about the technical employees controlling their personal device. As a result of the lack of communication, users were under the wrong impression as to what would happen once the mobile device management software was installed.

7.1.4.2 RELATIONSHIP BETWEEN 'EMPLOYEE DISSATISFACTION' AND 'CHANGE MANAGEMENT

The relationship between 'Employee dissatisfaction' and 'Change management has been identified as follows:

"..because none of this information was given to the user, they didn't actually know so it was complaints, and lots of umm, scary rumours running around. If you install [software] it will wipe your phone, once it installs it, it first wipes and then you secure" (1.3.5)

"The issues came around the change management" (1.1.16)

Inadequate 'Change management' aggravates 'Employee dissatisfaction'.

Figure 21 illustrates the inclusion of "Employee dissatisfaction" together with the relationship.

7.1.4.3 UPDATED EMERGING THEORY IN-PROGRESS

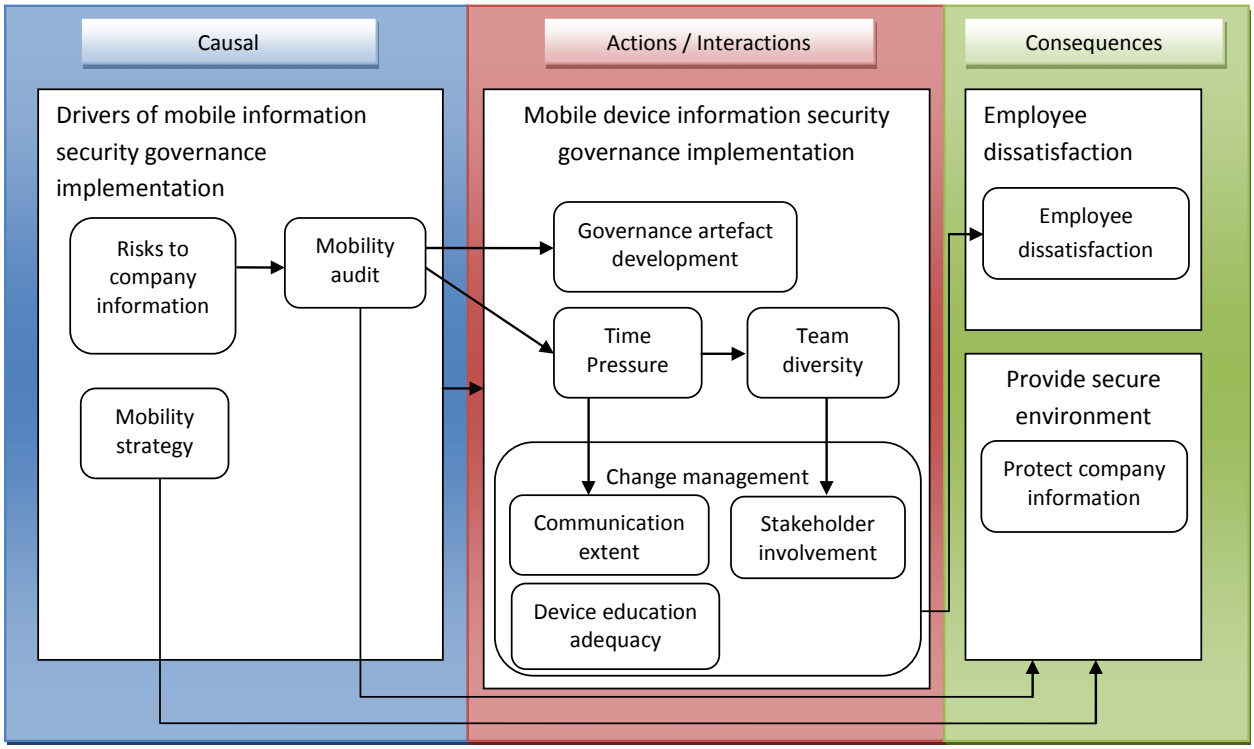


FIGURE 21 – EMPLOYEE DISSATISFACTION

7.1.5 ENSURE COMPLIANCE

As a result of the mobile information security governance implementation, a number of governance artefacts were developed which must be adhered to. Compliance to these artefacts was ensured via a number of ways and the following three sub-categories were identified: 'Technology compliance', 'Governance artefact compliance' and 'Audit compliance' as shown in Table 8. These are discussed in further detail below:

TABLE 7 – ENSURE COMPLIANCE

Sub-category	Concepts	Incidents	Supporting evidence	Source
Technology compliance	Compliance through technology	6	They are forced to comply. Afaria perspective – they can't switch off the policy. Not sure from a BlackBerry perspective.	1.2.17
			They don't have a choice, but the user still needs to inform the Helpdesk if the device gets stolen so it can be wiped.	1.2.14
			we are ensuring compliance through technology, We have an MDM software that ensure compliance.	1.4.19
			I think so because users are forced to abide by the controls of the policy .	1.2.26
			I suppose we enforce compliance because they can't have access to the information unless they have Afaria	1.1.32
			I think people learned to accept that they have to have it. Obviously if they had a choice they wouldn't want it on but they had to have it on, so that had to learn to accept it.	1.5.7
			people accepted that if they wanted something, if they wanted that access they had to do it and they did it	1.1.16a
Governance artefact compliance	Governance intervention	1	We also have a manual intervention from the governance team.	1.4.20
Audit compliance	Audit compliance	6	We have internal audit that reviews our compliance to policy.	1.4.21
			Poor or unsatisfactory, a repeat audit will be done next year. It means there were a number of high risk issues that need to be resolved within 0-3 months.	1.2.10
			For the most part it was a successful implementation. The implementation allowed us to meet the audit requirement and increased the security around mobile devices and therefore this protects [Company] information.	1.4.23
			just the fact that there no audit findings around any of the policies was a feather in your hat	1.1.31
			with the goals that we set out in the beginning with the risk matrix, err yes	1.1.33

7.1.5.1 TECHNOLOGY COMPLIANCE

Employees that required access to their company information on their mobile device were required to have the mobile device management standards applied to their devices. Employees did not have a choice as the standards were applied via a system policy. Standards such as a password and encryption were applied to the mobile device. Employees that did not agree with these standards, as a result of the dissatisfaction concepts discussed, were no longer allowed to have access to their company information on their mobile devices. Most users have, however, accepted that if they wanted access to their company information on their mobile devices then they had to comply.

7.1.5.2 GOVERNANCE ARTEFACT COMPLIANCE

Manual interventions by the Architectures and Governance team were sometimes required since not everything can be enforced with technology.

"...there might not be a technology control to enforce it" (1.4.16)

If necessary, corrective measures were taken to ensure that the governance artefacts were complied with. All statements within the mobile device management policy cannot be enforced with technology. A manual intervention was required by the Architectures and Governance team when infrastructure team members were not aware of policy statements regarding the collection of data. Any technical changes that resulted in a change to the types of data collected from mobile devices would have contravened the mobile device management policy because these changes had to be signed off by the CIO. This observation is highlighted in Table 6.

7.1.5.3 AUDIT COMPLIANCE

Internal audit reviews the Information Services department's compliance to the governance artefacts such as the mobile device management policy. This is done periodically determined by the Enterprise Risk and Assurance function. An audit result of "poor" or "unsatisfactory" means that a repeat audit will be done in the near future and all high risk issues identified must be resolved within zero to three months.

7.1.5.4 RELATIONSHIPS BETWEEN 'MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION', 'ENSURE COMPLIANCE' AND 'PROVIDE SECURE ENVIRONMENT'

The relationships between 'Mobile information security governance implementation', 'Ensure compliance' and 'Provide secure environment' have been identified as follows:

"For the most part it was a successful implementation. The implementation allowed us to meet the audit requirement and increased the security around mobile devices and therefore this protects [Company] information" (1.4.23)

'Mobile information security governance implementation' satisfies 'Ensure compliance'.

'Mobile information security governance implementation' works towards 'Provide secure environment'.

'Ensure compliance' ensures 'Provides secure environment'.

Figure 22 illustrates the theory developed from implementation one with all the categories, sub-categories and concepts discussed above.

7.1.5.5 UPDATED EMERGING THEORY IN-PROGRESS

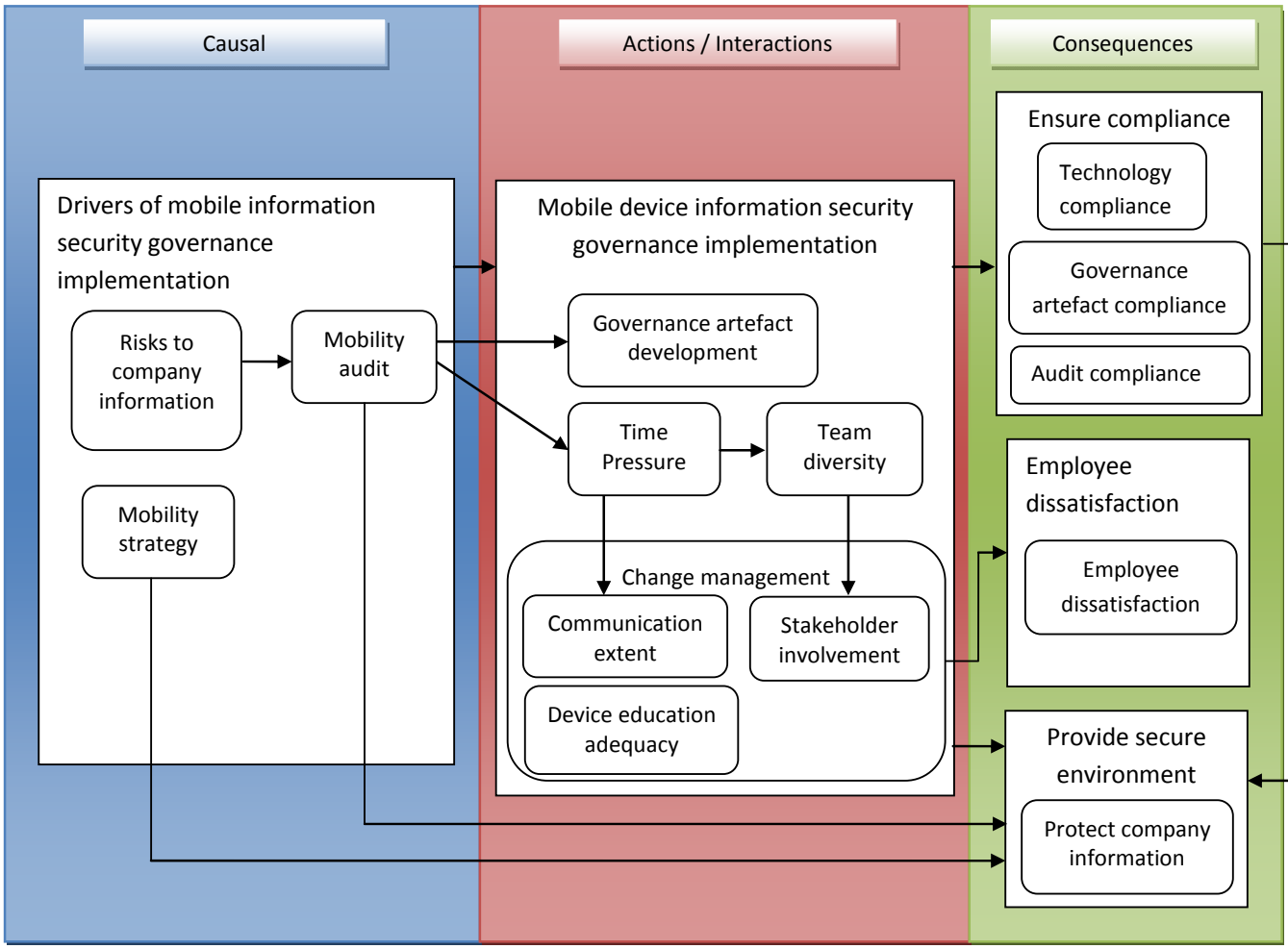


FIGURE 22 – THEORY DEVELOPED FROM IMPLEMENTATION ONE

7.2 IMPLEMENTATION TWO ANALYSIS

The second implementation refers to the implementation tasked to include the newly chosen company-owned mobile device as a supported mobile device within the company's technology infrastructure. The mobile device management software did not support all mobile device types and the newly chosen company-owned mobile device was a device that was not compatible with the technology infrastructure implemented during the first implementation.

7.2.1 DRIVERS OF NEW MOBILE TECHNOLOGY IMPLEMENTATION

The category of "Drivers of new mobile technology implementation" consists three sub-categories "Management of company mobile devices", "Demand for new mobile

technology" and "Mobile device provision pressure" which are all discussed in further detail and supporting evidence shown in Table 9.

TABLE 8 – DRIVERS OF NEW MOBILE TECHNOLOGY IMPLEMENTATION

Sub-category	Concepts	Incidents	Supporting evidence	Source
Management of company mobile devices	Manage mobile devices	2	Please could you check with [Service Provider] as [GM3's] sim card is not activated. It's giving an error message on the phone. We are unable to activate email and calendar on the device before the sim card is sorted.	I2E59/AS
			Procurement have the responsibility to manage [Company]-owned devices and should be the first point of call for users in this category.	I2E16/AM
Demand for new mobile technology	Mobile technology decisions	11	Did you guys log this work order or who was it from. We had PO1 in that Blackberry session and the vendor, not us, explained to her In great detail what infrastructure we require as well as licenses. Now I'm afraid we need to pull out all the stops to get this into our environment.	I2E1/ITM
			we had a meeting with [FIM] this morning to have the BB 10 server setup in our current environment. I'm gathering all the necessary information from [V] to proceed with this requirement.	I2E1/SB
			Please could you provide the link for the CCP policy. Can you provide the reasoning why procurement has not revisited the Blackberry decision (with IS input). Blackberry has made significant changes to their operating model, and current trend is for enterprises is to move off blackberry devices.	I2E5/TA
			Currently 95% of Fortune 500 companies run on a BlackBerry® Solution. I will be arranging a session for IS with [B], the Enterprise Sales Manager from Blackberry at his earliest convenience, I think he is down next week.	I2E5/PO1
			"Currently 95% of Fortune 500 companies run on a BlackBerry® Solution." This statement is straight out of Blackberry marketing material and could be said about any cellphone vendor. The trend that we are seeing is that enterprises are moving away from blackberry. Below is an example of blackberry losing market share.	I2E5/TA
			On my side, I will need the expertise of Mobile at Work, to be educated on what the capabilities on the Z10/BDS is in order to maximise value add. For example, SAP is a business partner of Blackberry and the possibilities are endless but we would need some guidance.	I2E5/PO1

			”In hindsight, the continuation of the BlackBerry device as a company standard device should have been reviewed taking all factors into consideration before being purchased.” As per our previous discussion, Procurement did consult with IS, [FIM], in a meeting that we initiated to get approval and discuss the possibility of upgrading to the Z10. The Z10 was the logical upgrade in the Blackberry range ito “upgrading on contract”. No Z10 contractual upgrades were authorised by myself, up until approval was received from IS to go ahead with a date of possible go-live. If necessary we could track the IS work orders, systems enhancements and communications, in order to proof the date of change on the system was way before the actually contractual signatures on my side.	I2E18/PO1
			Kindly could we schedule a meeting to discuss the Company Cell Phone standard device, Blackberry, which was signed off and implement a while back on Policy. IT have been advising our Company Cell Phone Users that we may procure from a variety of brands i.e iPhone, Samsung etc. Recalling the logic behind the stance we took on implementing a Company standard device; was to eliminate the pressure of supporting various devices from an IT support as well as Supplier Customer Care & Repair Support.	I2E17/PO1
			IS is best positioned to assess and recommend technology choices as we consider not only the cost and supportability of devices but also the risks associated with secure usage of [Company] information in order to preserve its confidentiality, integrity and availability.	I2E16/AM
			We are not promoting any specific device. All we are saying is that there are other devices that are currently compatible within the existing [Company] infrastructure, iPhone and Samsung devices were used as examples of devices that are currently compatible devices.	I2E21/AS
Mobile device provision pressure	Mobile devices required	3	Some of us are due for upgrades promptly	I2E16/EU1
			Following up on the Blackberry Z10 progress to be able to use the phone. (have it now for 6 mnts and paying the contract) . My current blackberry is not in good shape (some of the keys are not working). I am happy even if I can just use as a normal phone (but must have my contacts) for now until they are able to address the emails issue.	I2E52/EU5
			Can I please have a progress update on my application.	I2E53/EU4
	Power - using GM's to get work expedited	6	Please find attached the PO for the BDS server installation. Please expedite the work as the General Managers are awaiting connectivity to receive work related emails on their mobiles.	I2E2/SB
			[GM1] has asked me to run this pass you as IS has proclaimed an ERA finding. Executives awaiting activation : · 8 Company Cell Phone users · CEO · [GM2] · [GM3] · [GM4] · [GM1]	I2E11/PO1

			I've spoken to the Architectures, Governance and Security team and we cannot give anyone access to the BlackBerry Z10 until the necessary security assessments and related work has been completed. I have found out about the device in question and currently phone calls can be made. The only problem is that new emails are not downloading. I have been informed that the user has an ipad which could be used for this purpose in the meantime as the ipad is configured for international roaming. [Desktop support engineer] is avaible tomorrow to check the ipad if it is required. Please let me know. A note will be going out to the whole company soon with regards to the BlackBerry Z10 so that everyone is aware of the current status.	I2E9/AS
			I am fully aware of the pressure from PO1's office for distributing these devices. I am pretty sure the VIP's are pressing hard for it. But we have to be on top of our game before facing those requests. I am sure that if communicated successfully and carefully that the VIP's will understand.	I2E4/TS
			Further our conversation in your office this afternoon, unfortunately, I have received the below comms from IT. A request to use your IPAD instead to retrieve mail has been instructed.	I2E11/PO1
	Power - using ERA to get work expedited	2	Can you please advise as to when security assessments will be completed for BB Z10, the users urgently require access to their emails.	I2E11/EM
			I cannot understand as to why IS is promoting Samsung devices as it is an Android device that is not protected from malware loaded onto these devices. This was discussed at yesterday's AMC meeting. Yu can refer to open audit issue on Malware.	I2E21/EM
	Power - using Business users to get work expedited	1	[AS] has come back to me to say that there are other devices that can be procured such as iPhone or Samsung...the Z10 is not supported right now! Please advise whether I can get other fone urgently	I2E17/EU2

7.2.1.1 MANAGEMENT OF COMPANY MOBILE DEVICES

Company mobile devices are managed by the Procurement department who liaises with business users who require a company-owned mobile device as part of their job. The Information Services department provides these business users with access to their company information, specifically email and calendar, on their mobile devices.

7.2.1.1.1 DEMAND FOR NEW MOBILE TECHNOLOGY

As a result of company mobile devices being managed within the Procurement department, the company standard device choice was made by this department. Unfortunately, the new generation mobile device which was seen to be the most logical choice, given the fact that the company had used this brand of device for a

number of years, was not compatible with the existing mobile infrastructure as a result of it being a new mobile technology.

"Blackberry for a long time has been integrated within our environment" (I2E22/SB)

The decision in terms of the choice of the company mobile device resided with the Procurement department and the Information Services department was unable to convince the business to choose a mobile device which already worked within the environment.

"IS is best positioned to assess and recommend technology choices as we consider not only the cost and supportability of devices but also the risks associated with secure usage of [Company] information in order to preserve its confidentiality, integrity and availability." (I2E16/AM)

A disconnect existed between the Procurement department, where the responsibility of managing company mobile devices resided, and the Information Services department, where the technical experts who had the knowledge as to whether the device would work in the company's mobile environment.

7.2.1.2 MOBILE DEVICE PROVISION PRESSURE

The Procurement department was under pressure to provide business users with mobile devices. Some of these users were due for upgrades and others had faulty devices and required urgent replacement devices.

"Some of us are due for upgrades promptly" (I2E16/EU1)

Some of the business users such as the general managers had already been allocated these new mobile devices which then in turn added pressure to the Information Services department to deliver a solution for these new devices. The fact that these users had already been allocated devices was used as a means of expediting the work required to introduce the new technology into the existing environment.

"Please expedite the work as the General Managers are awaiting connectivity to receive work related emails on their mobiles" (I2E2/SB)

7.2.1.3 RELATIONSHIP BETWEEN 'MANAGEMENT OF COMPANY MOBILE DEVICES' AND 'DEMAND FOR NEW MOBILE TECHNOLOGY'

Evidence of the relationships between 'Management of company mobile devices' and 'Demand for new mobile technology' is as follows:

"The Z10 was the logical upgrade in the Blackberry range ito "upgrading on contract" (I2E18/PO1)

'Management of company mobile devices' generates 'Demand for new mobile technology'.

7.2.1.4 RELATIONSHIP BETWEEN 'MANAGEMENT OF COMPANY MOBILE DEVICES' AND 'MOBILE DEVICE PROVISION PRESSURE'

Evidence of the relationship between 'Management of company mobile devices' and 'Mobile device provision pressure' is as follows:

"Can I please have a progress update on my application" (I2E53/EU4)

'Management of company mobile devices' results in 'Mobile device provision pressure'.

7.2.1.5 RELATIONSHIP BETWEEN 'DEMAND FOR NEW MOBILE TECHNOLOGY' 'AND 'MOBILE DEVICE PROVISION PRESSURE'

Evidence of the relationship between 'Demand for new mobile technology' and 'Mobile device provision pressure' is as follows:

"have it now for 6 mnts and paying the contract"(I2E52/EU5)

'Demand for new mobile technology' intensifies 'Mobile device provision pressure'.

Figure 23 depicts the relationships discussed between all sub-categories of 'Drivers of new mobile technology implementation'.

7.2.1.6 EMERGING THEORY IN-PROGRESS

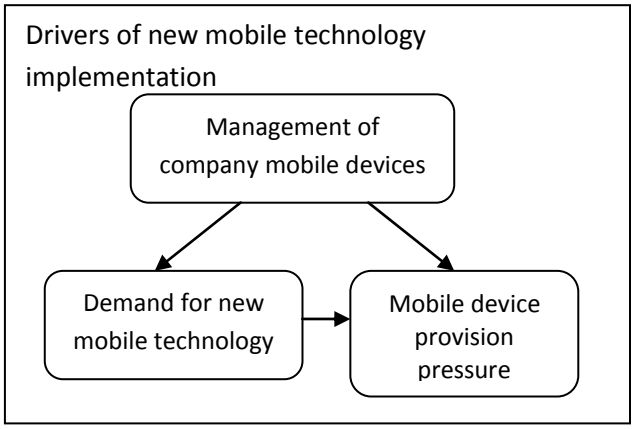


FIGURE 23 - DRIVERS OF NEW MOBILE TECHNOLOGY INPLEMENTATION

7.2.2 DRIVERS OF INFORMATION SECURITY GOVERNANCE CONSIDERATION

The category of 'Drivers of information security governance consideration' consists two sub-categories 'Risks to company information' and 'Governance artefact compliance' which are discussed in further detail and supporting evidence shown in Table 10.

TABLE 9 - DRIVERS OF INFORMATION SECURITY GOVERNANCE CONSIDERATION

Sub-category	Concepts	Incidents	Supporting evidence	Source
Risks to company information	Risks to company information	3	There is an open work order with IS to perform a security and risk assessment of this device. A security assessment is not a trivial exercise and is done to mitigate risks to company information... given the CEO's strategic focus on risk management, I am sure that these users will fully understand the importance of ensuring [Company] information risks are being properly managed.	I2E11/AM
			a)Usage of these devices is a risk to the confidentiality, integrity and availability of [Company's] information as they are not secured through our mobile device management infrastructure.	I2D1
			Please could we meet to discuss the risk identified with the BlackBerry Z10 and obtain your signatures as acceptance of this risk?	I2E61/AS
	Company data leakage	2	As this solution poses a risk in terms of data leakage to [Company's] information, we are in the process of documenting the risk that needs to be signed off before access can be given.	I2E60/AS
			... to accept the risk and responsibility associated with potential information and data leakage.	I2D1
	Unsecure devices	4	IS is best positioned to assess and recommend technology choices as we consider not only the cost and supportability of devices but also the risks associated with secure usage of [Company] information in order to preserve its confidentiality, integrity and availability.	I2E16/AM
			.. a decision has been made that the risk of unsecure devices is too high and we, therefore, cannot give anyone access to [Company's] information until the necessary work has been completed.	I2E15/AS
			.. documented the risk of unsecure and unsupported usage of BlackBerry Z10 devices.	I2E13/AS
			We've discussed the risk identified... and a decision has been made that the risk of unsecure devices is too high and we, therefore, cannot give anyone access to [Company's] information.	I2E60/AS
Governance artefact compliance	Governance artefact compliance	5	...as stated in our published mobile device management policy under roles and responsibilities as follows: IS Security Specialist Review security considerations and impacts of policy Review security impacts of requested exceptions and waivers to policy Review security considerations of change proposals	I2E11/AM

			..ensure that any changes / decisions are in line with the Mobile Device Management policy or make the necessary updates to the policy · ensure that all the configuration standards are in line with the current Mobile Device Management standards · configure the BlackBerry Server and create the relevant IT policies	I2E7/AS
			...assurance that any changes / decisions are in line with the Mobile Device Management policy · assurance that all the configuration standards are in line with the current Mobile Device Management standards	I2E8/AS
			c)The [Company] mobile device management policy requires that any new device that is not supported by our current mobile device management infrastructure must be fully assessed by our Information Security Specialists and their recommendations must be implemented in order to ensure the security of [Company's] information.	I2D1
			According to our published "Mobile Device Management" policy any device that stores [Company] information must be compatible with our mobile device management infrastructure.	I2E16/AM

7.2.2.1 RISKS TO COMPANY INFORMATION

Risk management was one of the key strategic focus areas within the company. The security of the company's information had to be taken into consideration to ensure that any risks to company information were identified and mitigated.

Some of the users that had already been allocated the new mobile devices, required access to their company information on the device immediately and were not able to wait until the necessary work was completed. The risk of giving these users access to company information on their mobile devices was documented and after consideration it was decided that the risk was too high based on the concepts highlighted of 'Unsecure usage' and 'Company data leakage'. Employees were, therefore, not allowed to access company information on these mobile devices until the necessary information security work was completed.

"Usage of these devices is a risk to the confidentiality, integrity and availability of [Company's] information as they are not secured through our mobile device management infrastructure" (I2D1)

7.2.2.2 GOVERNANCE ARTEFACT COMPLIANCE

As the newly chosen mobile device was not compatible with the existing mobile infrastructure, this meant that a change needed to be made in order for the device to work. The role of the security specialist was to review any changes with regards to

devices or sources of information that were not securely supported by the existing infrastructure. In order to remain compliant with the existing mobile device management policy, one of the governance artefacts developed during the first implementation, the information security requirements had to be met or any exceptions to the policy had to be signed off by the CIO.

Another governance artefact mentioned that was developed during the first implementation was the mobile device management standards document. All configuration standards of the new device needed to be aligned with the existing mobile device management standards.

"...ensure that any changes / decisions are in line with the Mobile Device Management policy or make the necessary updates to the policy
ensure that all the configuration standards are in line with the current Mobile Device Management standards" (I2E8/AS)

The sub-categories of "Drivers of information security governance consideration' are depicted in Figure 24.

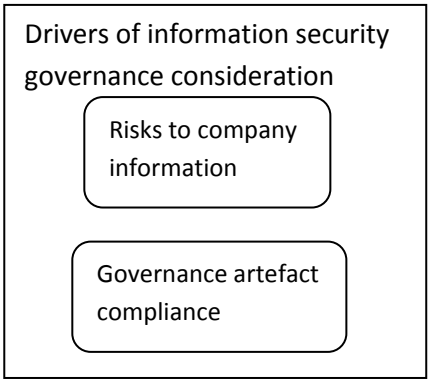


FIGURE 24 - DRIVERS OF INFORMATION SECURITY GOVERNANCE CONSIDERATION

7.2.3 IMPLEMENTATION OF NEW MOBILE TECHNOLOGY

The category of "Implementation of new mobile technology" consists of two sub-categories namely: 'Investigate new mobile technology' and 'Information security consideration' as shown in Table 11 and are described further below.

TABLE 10 - IMPLEMENTATION OF NEW MOBILE TECHNOLOGY

Sub-category	Concepts	Incidents	Supporting evidence	Source
Investigate new mobile technology	Investigate new mobile technology	8	As you know – with the new environment and devices, the handheld generates two profiles as soon as you add it to the network. A personal profile and a work profile. Be default everything is accessed from both profiles and we HAVE to look at setting IT policies to block this.	I2E4/TS
			Then there is the fact that we ourselves don't know how the devices work. I don't feel it is a good idea to add VIP users right now. I am worried that should they contact us for assistance or support that we are not geared for professionally assisting them. I don't want us to sound unprofessional when approached by a VIP (or any business person for that may).	I2E4/TS
			Technically, the device cannot work with the existing infrastructure and, therefore, new development and production servers are being installed especially for this one new mobile device.	I2E18/AS
			... but we are doing our best at a rapid rate on technology that is very new. We have been running BES5 for many years and we know the product inside out. Please don't think that we are just sitting back. We are pushing to get to know this product (amongst other deliveries). BES 10 is the latest and except for some settings – it is a completely new product.	I2E4/TS
			We have no installed the Blackberry 10 server backend. We have 2 devices configured successfully after ironing out minor issues. My question is ……. What now? How do we take this forward?	I2E5/TS
			... we need to just stop and think about some concerns. The new device has 2 profiles – personal and work and both of these are treated differently on the phone and from the backend. What do we lock down on the device? What do we allow? Do we control polices between the profiles? Blackberry 10 is based on Active Sync. User LAN password change will affect the device and how do we handle that load? My point is we have all these questions. Technical support will configure the environment to apply the rules that is decided on, BUT who decides that?	I2E5/TS
			..research in terms of how the device works, we currently do not have any technical documentation for the device and cannot make the necessary decisions	I2E7/AS

			On my side, I will need the expertise of [Third party vendor], to be educated on what the capabilities on the Z10/BDS is in order to maximise value add.	I2E5/PO1
Information security consideration	Information security	5	The reason for this is the fact that this device may not be used to store and access [Company] information until it has been configured, tested and suitable infrastructure has been set up to meet [Company] information security requirements.	I2E16/AM
			c)The [Company] mobile device management policy requires that any new device that is not supported by our current mobile device management infrastructure must be fully assessed by our Information Security Specialists and their recommendations must be implemented in order to ensure the security of [Company's] information.	I2D1
			...an information security assessment of the device to ensure that [Company]'s information is protected	I2E7/AS
			an information security assessment of the BlackBerry Z10 device	I2E8/AS
			Based on current workload, IS has committed to have completed all related work including information security assessment, infrastructure configuration, testing in our environment and updating of policy and standards by the end of July 2013.	I2E11/AM

7.2.3.1 INVESTIGATE NEW MOBILE TECHNOLOGY

The new mobile device chosen as the company standard device worked differently to the existing mobile devices and was a completely new product. The technical specialist needed to understand how the device worked so that once the device was allocated to business users; they would be able to provide the required support for the device.

The new generation mobile device consisted of two profiles, a work and a personal profile. Once the server was installed and configured, questions arose regarding the two profiles and who the decision makers were as far as the IT policy settings for this mobile device. The architectures, governance and security team was approached in order to make the relevant decisions.

"Technical support will configure the environment to apply the rules that is decided on, BUT who decides that?" (I2E5/TS)

7.2.3.2 INFORMATION SECURITY CONSIDERATION

The sub-category of 'Information security consideration' consists of the activities required to review the security considerations of any change proposals which had be done according to the governance artefacts developed during the first implementation. As a result of the new mobile device chosen, there were a number of activities that needed to be completed so as to integrate the device into the existing infrastructure. One of the activities was to complete a security assessment of the configuration settings of the device and also to gain an understanding of how this new device could be integrated into the existing architecture so that the best decision could be made taking the overall mobility architecture into consideration.

7.2.3.3 RELATIONSHIP BETWEEN 'DEMAND FOR NEW MOBILE TECHNOLOGY' AND 'INVESTIGATE NEW MOBILE TECHNOLOGY'

Evidence of the relationship between 'Demand for new mobile technology' and 'Investigate new mobile technology' is as follows:

"research in terms of how the device works, we currently do not have any technical documentation for the device and cannot make the necessary decisions" (I2E7/AS)

'Demand for new mobile technology' prompts 'Investigate new mobile technology'.

7.2.3.4 RELATIONSHIP BETWEEN 'INVESTIGATE NEW MOBILE TECHNOLOGY' 'AND 'INFORMATION SECURITY CONSIDERATION

Evidence of the relationship between 'Investigate new mobile technology' and 'Information security consideration' is as follows:

"The reason for this is the fact that this device may not be used to store and access [Company] information until it has been configured, tested and suitable infrastructure has been set up to meet [Company] information security requirements" (I2E16/AM)

'Investigate new mobile technology' initiates 'Information security consideration'.

7.2.3.5 RELATIONSHIP BETWEEN 'RISKS TO COMPANY INFORMATION' AND 'INFORMATION SECURITY CONSIDERATIONS'

Evidence of the relationship between 'Risks to company information' and 'Information security considerations' is as follows:

"A security assessment is not a trivial exercise and is done to mitigate risks to company information" (I2E11/AM)

‘Risks to company information’ drives ‘Information security consideration’.

7.2.3.6 RELATIONSHIP BETWEEN ‘GOVERNANCE ARTEFACT COMPLIANCE’ AND ‘INFORMATION SECURITY CONSIDERATION’

Evidence of the relationship between ‘Information security consideration’ and ‘governance artefact compliance’ is as follows:

“...as stated in our published mobile device management policy under roles and responsibilities as follows:

- *Review security considerations of change proposals” (I2E11/AM)*

‘Governance artifact compliance’ mandates ‘Information security consideration’.

Figure 25 depicts the inclusion of the category ‘Implementation of new mobile technology’ together with the relationships between categories and concepts.

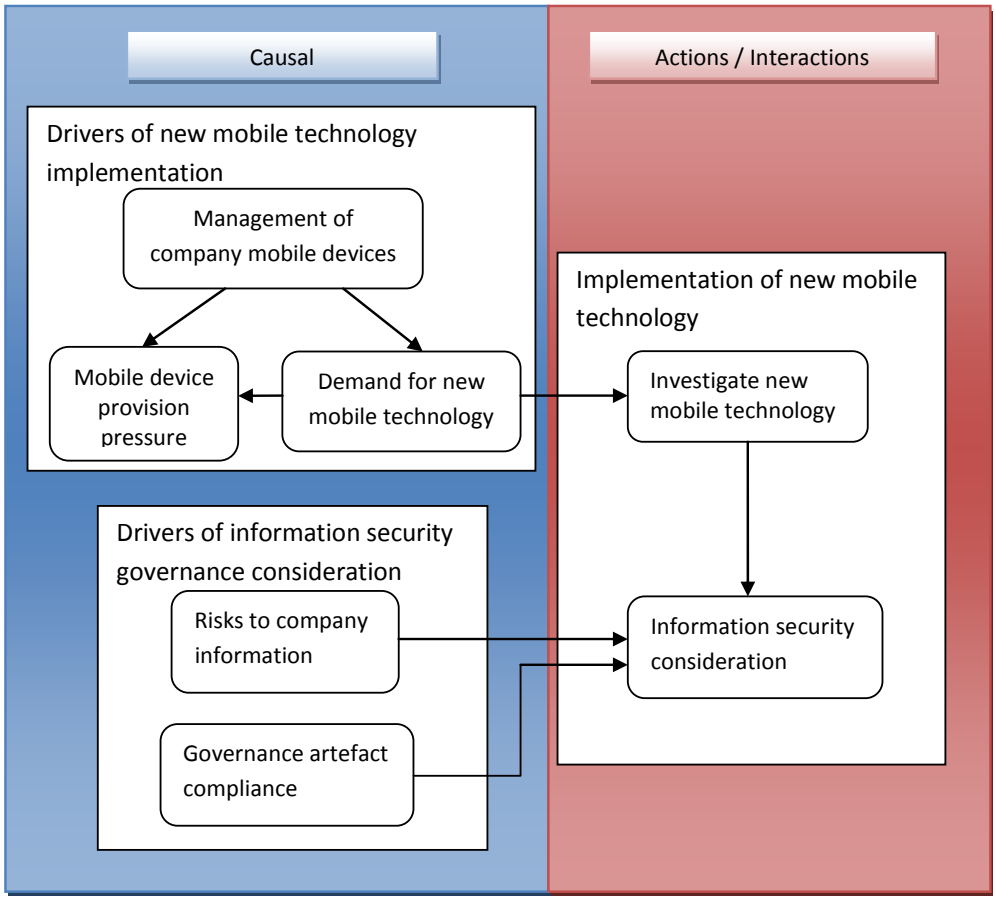


FIGURE 25 - IMPLEMENTATION OF NEW MOBILE TECHNOLOGY

7.2.4 PROVIDE SECURE ENVIRONMENT

The category of "Provide secure environment" consists of the concept "Protect company information as shown in Table 12 and further discussed below.

TABLE 11 - PROVIDE SECURE ENVIRONMENT

Sub-category	Concepts	Incidents	Supporting evidence	Source
Protect company information	Protect company information	4	... this device may not be used to store and access [Company] information until it has been configured, tested and suitable infrastructure has been set up to meet [Company] information security requirements.	I2E16/AM
			... must be fully assessed by our Information Security Specialists and their recommendations must be implemented in order to ensure the security of [Company's] information.	I2D1
			We have had an initial meeting and have found that some investigative work needs to take place to ensure that [Company's] information is protected with the new BlackBerry 10. · an information security assessment of the device to ensure that [Company]'s information is protected	I2E7/AS
			The following work is being conducted with regards to the BlackBerry Z10 device in order to ensure that [Company]'s information is protected:	I2E8/AS

7.2.4.1 PROTECT COMPANY INFORMATION

Ultimately, the company information must be protected. This was done by adhering to the mobile device management policy and standards, completing the necessary security related work and identifying any risks to the company information which had to be mitigated.

7.2.4.2 RELATIONSHIP BETWEEN 'INFORMATION SECURITY CONSIDERATION' AND 'PROTECT COMPANY INFORMATION'

Evidence of the relationship between 'Information security consideration' and 'Protect company information' is as follows:

> *"... must be fully assessed by our Information Security Specialists and their recommendations must be implemented in order to ensure the security of [Company's] information." (I2D1)*

'Information security consideration' ensures 'Protect company information'.

7.2.5 ENSURE COMPLIANCE

The new generation mobile device was not compatible with the existing infrastructure which meant that a security assessment was required to ensure the safeguarding of the company information being accessed on these devices. The act of doing the information security assessment meant that the mobile security governance artefacts including technology were complied with and, therefore, would comply with any future audit in the mobile device environment and ultimately protects the company's information.

The information security consideration was a necessary step not only to ensure the protection of the company's information but also to remain compliant with audit requirements.

"We have internal audit that reviews our compliance to policy" (1.4.21)

7.2.5.1 RELATIONSHIP BETWEEN 'INFORMATION SECURITY CONSIDERATION' AND 'ENSURE COMPLIANCE'

The auditor mentioned in the first implementation that the starting point of the audit is "*policies and procedures and talk to people responsible for the process*" (1.2.23). This was done to elicit information and determine whether the documented policy statements and processes have been followed.

"Ensure compliance' mandates 'Information security consideration'.

7.2.6 EMPLOYEE DISSATISFACTION

The shortage of information security specialists had an impact on the completion date which was based on current workload and priorities. Company information could not be stored on this new mobile device until all activities, including the information security assessment, were completed. This led to a number of unhappy employees because they had urgent upgrade requirements.

7.2.6.1 RELATIONSHIP BETWEEN 'INFORMATION SECURITY CONSIDERATION' AND 'EMPLOYEE DISSATISFACTION'

The evidence of the relationship between 'Information security consideration' and 'Employee dissatisfaction' is as follows:

"My current blackberry is not in good shape (some of the keys are not working). I am happy even if I can just use as a normal phone (but must have my contacts) for now until they are able to address the emails issue" (I2E52/EU5).

'Information security consideration' aggravates 'Employee dissatisfaction'.

Figure 26 illustrates all categories, sub-categories and concepts with all relationships discussed for implementation two.

7.2.6.2 UPDATED EMERGING THEORY IN-PROGRESS

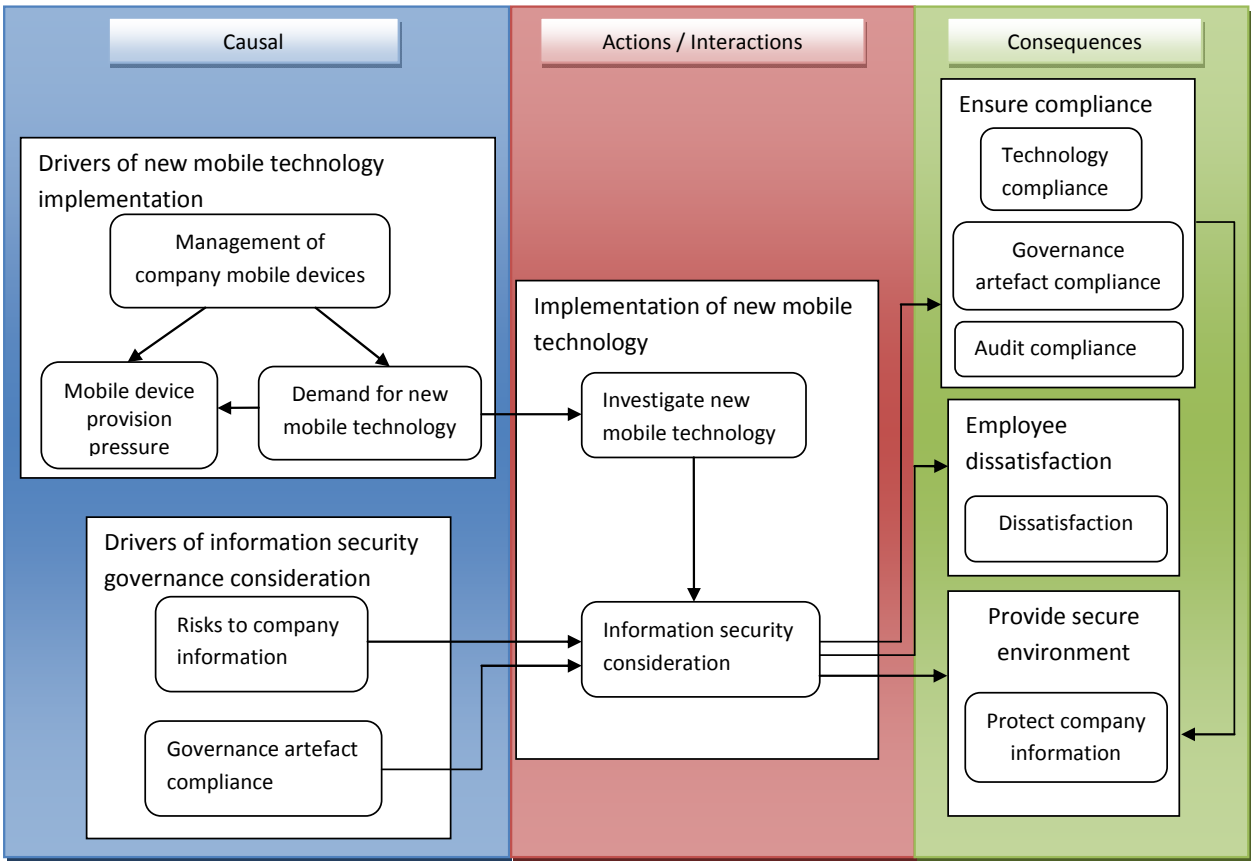


FIGURE 26 – THEORY DEVELOPED FROM IMPLEMENTATION TWO

7.3 COMBINED VIEW OF IMPLEMENTATIONS

Open, axial and selective coding was done for each implementation. All categories that are displayed in the previous diagrams have been deemed important to that particular implementation. Further selective coding was used to link relevant categories from both implementations to the central phenomenon of 'Information security governance implementation' in order to formulate a theoretical framework as suggested by Strauss and Corbin (as cited in Pozzebon et al., 2011).

Figure 27 below depicts the common categories, sub-categories and concepts that emerged across both implementations.

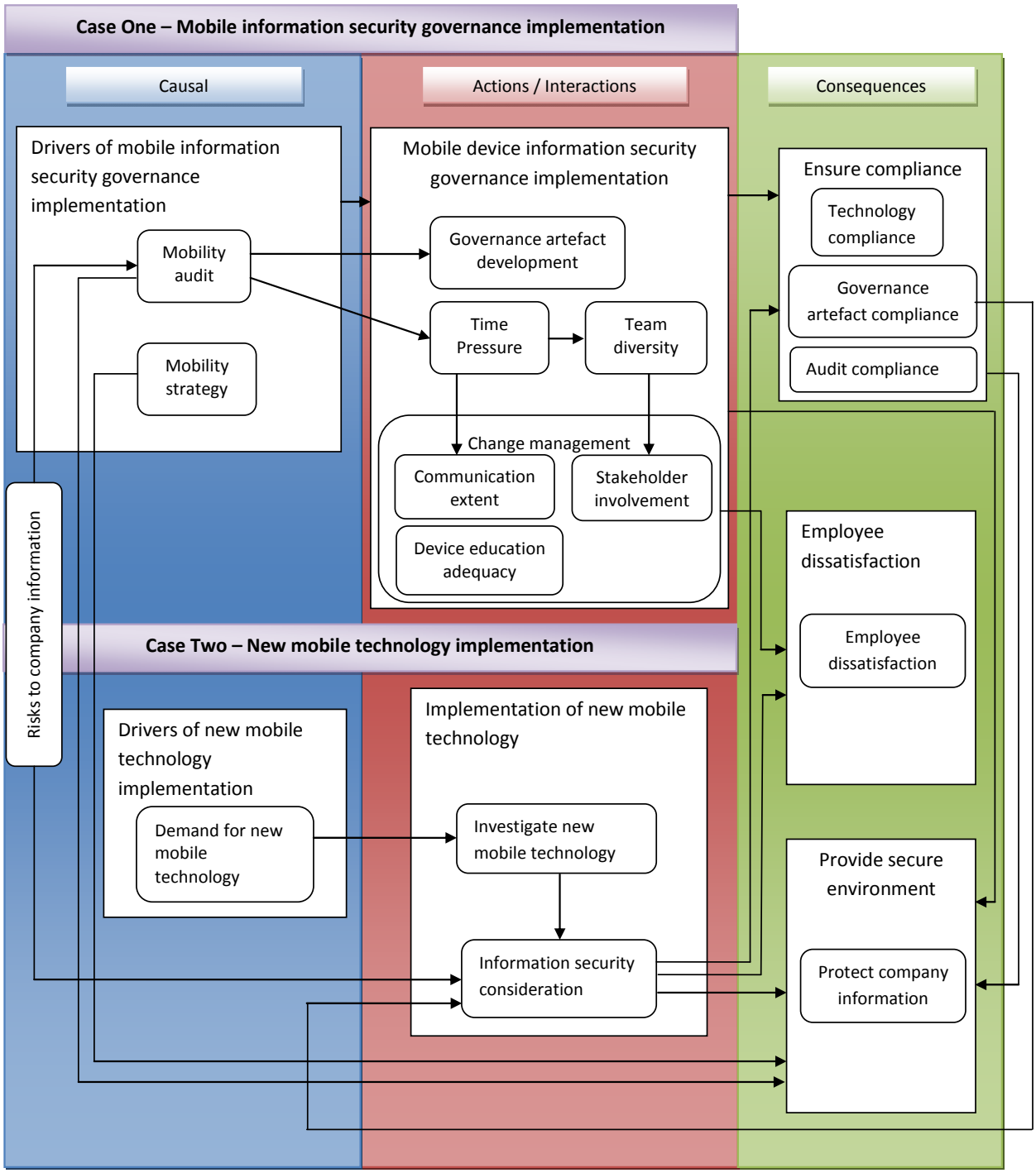


FIGURE 27 - COMBINED VIEW OF IMPLEMENTATIONS

7.3.1 COMMONALITIES BETWEEN BOTH IMPLEMENTATIONS

A number of categories and concepts have emerged as being common to both implementations such as “Risks to company information”, “Ensure compliance”, “Employee dissatisfaction” and “Provide secure environment”. Each of these is discussed below.

The concept of “Risks to company information” was highlighted by both implementations as one of the drivers. It was the reason for implementing mobile information security governance at the organisation and is constantly reflected on when any new mobile technology is being demanded by the Business.

The category of “Employee dissatisfaction” has been highlighted as a consequence of both implementations but there are different reasons for the dissatisfaction. The first implementation has a strong concept of change management, which was lacking, causing employee dissatisfaction. The second implementation led to employee dissatisfaction due to the delay caused by the need to remain compliant with the mobile information security governance, which was essential to ensure that any potential risks related to the introduction of the new mobile technology was mitigated.

“Ensure compliance” was common in both implementations. Compliance was ensured via technology, a manual intervention to ensure governance artefact compliance and lastly via internal audit. The first implementation ensured that mobile information security governance was in place before the audit took place; therefore, the sub-category of “mobility audit” was a prominent driver. The second implementation does not show “mobility audit” as a driver but shows the influence of “governance artefact compliance as being a driver of ‘Consider mobile information security’ which led to ‘Governance artefact compliance’. In this instance, ‘Governance artefact compliance’ is a driver as well as a consequence. By ensuring compliance to the governance artefacts, indirectly there is a compliance with audit.

“Provide secure environment” was a category highlighted by both implementations which means that the goal of implementing or considering mobile information security governance was to protect the company’s information.

In order to provide a theory that is well explained, a storyline will be used.

7.3.2 STORYLINE

Strauss and Corbin define the storyline as the "conceptualization of the story" which is a "descriptive narrative about the central phenomenon of the study" (as cited in Birks, Mills, Francis & Chapman, 2009). The storyline as a technique of analysis is most commonly associated with grounded theory research which aims to explain phenomena in the context within which it exists by producing theory (Birks et al., 2009).

Strauss and Corbin describes the storyline as a tool which aids theoretical development and later describes it also as a means of integrating theory during the process of analysis (as cited Birks et al., 2009). Strauss and Corbin have delayed the use of the storyline until later coding stages, whereas Birks et al. (2009) argue that in grounded theory the storyline can be used throughout the research process so that the final theory is constructed, integrated and finally made visible. The authors claim that a theory that may otherwise have been dry and unpalatable is brought to life by the power of the storyline from a pragmatic perspective.

Birks et al. (2009) have suggested guiding principles for writing the storyline through the mnemonic 'TALES' as shown in Figure 28:

Table I Guiding principles for writing the storyline

Writing the storyline
T – Theory takes precedence
A – Allows for variation
L – Limits gaps
E – Evidence is grounded
S – Style is appropriate

FIGURE 28 - GUIDING PRINCIPLES FOR WRITING THE STORYLINE (BIRKS ET AL., 2009)

The process of open, axial and selective coding has resulted in the grounded theory emerging from the data depicted in Figure 29 below. The storyline will be used to explain the theoretical framework from two perspectives using the two units of analysis within the case study which then results in the final theory emerging as depicted in Figure 31. The two perspectives are:

1. No mobile information security governance in place

2. Mobile information security governance in place, new or change proposal to be considered

A process view has been used to depict and explain the storyline which ends in the development of the final grounded theory.

7.3.2.1 PERSPECTIVE ONE: NO MOBILE INFORMATION SECURITY GOVERNANCE IN PLACE

The theory as depicted in Figure 29 below consists of six process steps which are categorised into areas of high risk, mitigate risk and low risk. The idea behind the framework is that when risks are first identified they could potentially be considered as a high risk until it has been investigated and something is done to mitigate the risk, it then moves into the area of low risk because the chances of the risk occurring has been reduced. Each process step has been further elaborated as part of the storyline.

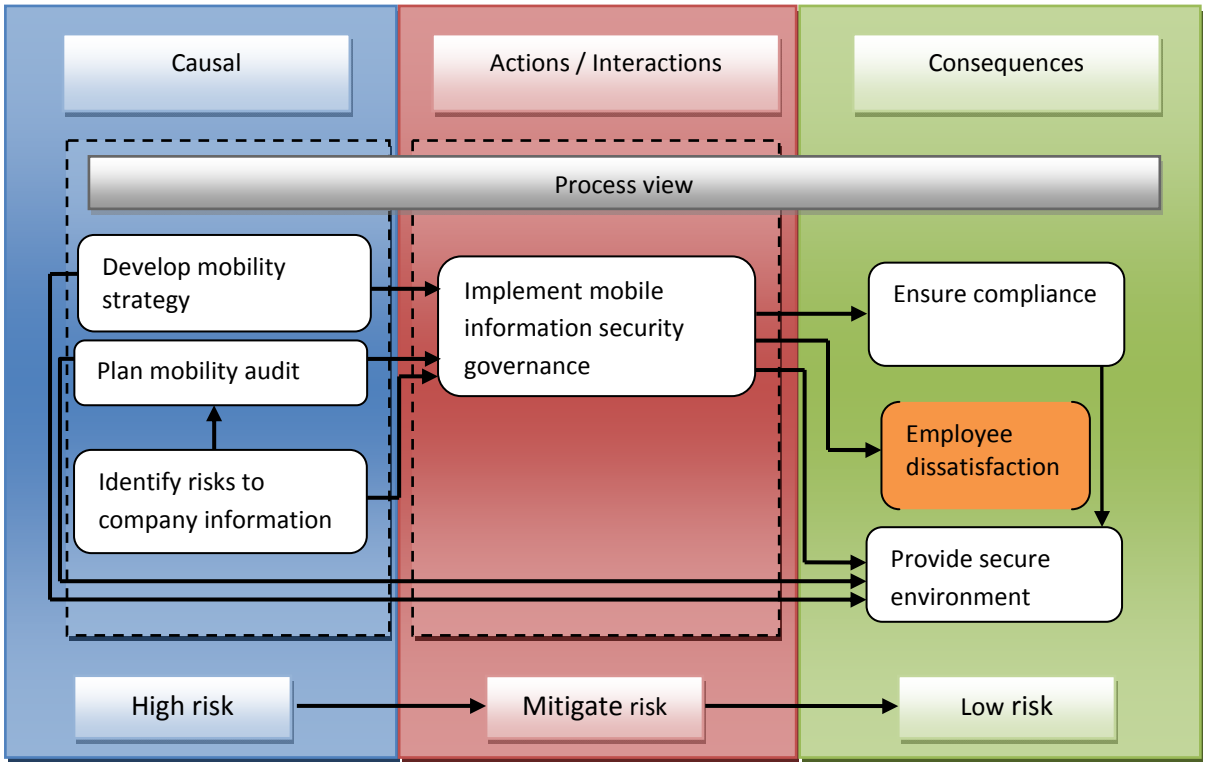


FIGURE 29 - PERSPECTIVE ONE: NO MOBILE INFORMATION SECURITY GOVERNANCE IN PLACE

7.3.2.1.1 IDENTIFY RISKS TO COMPANY INFORMATION

The protection of company information starts with identifying any risks that could potentially impact the company in a negative way. Awareness of these risks to company information is brought about from a number of sources whether it is from an external source such as industry information, disseminated via newsletters and conferences, or an internal source that identifies the risk within the company. In this case, the risks identified were related to the increasing number of users accessing company information on their mobile devices which did not have the necessary controls applied in order to mitigate the risks.

The risks identified with regards to mobile devices were the potential loss or leakage of confidential company information and also access to confidential company information by unauthorised users. These risks could potentially not only have an impact on the company information but also on the bottom line of the company. The example explained was that a cellphone was taken and all meetings were removed from the calendar, this replicated to the server resulting in all meetings for the next six months being cancelled. This scenario could potentially have happened to one of the company's sales personnel which meant that the company's revenue could have been impacted.

7.3.2.1.2 PLAN MOBILITY AUDIT AND DEVELOP MOBILITY STRATEGY

The risk within the mobile device management environment was identified by the Information Services department and was, therefore, part of the Information Services strategy, and the company's Enterprise, Risk and Assurance department and, therefore, landed on the internal audit plan.

Multiple sources of risk identification within companies are necessary because it increases the opportunities of risks to company information to be identified and mitigated.

7.3.2.1.3 IMPLEMENT MOBILE INFORMATION SECURITY GOVERNANCE

As a result of the risks identified, a mobile information security governance implementation was initiated and expedited by management to meet the impending internal audit requirements and to mitigate the risks related to the organisation's information. As a result of the time pressure being experienced due to the mobility audit, it was felt that the quickest way to complete the implementation before the mobility audit was to have a small dedicated team since it was believed that this would speed up the implementation process. The team was established to setup the technical environment and develop the policies, processes and standards. Controls such as a password, encryption, remote wipe and timeout were applied to all mobile devices requiring access to company information. Only those mobile devices that were compatible with the mobile device management software and were able to have the controls applied were allowed access to company information.

Unfortunately, stakeholder involvement, communication, device education, change management were not done well and led to a number of unhappy users. Although "Employee dissatisfaction" is not a process step, it is highlighted within the model since there was such a significant impact on the employees. Some employees could no longer access their company information on their mobile devices because it was not compatible with the mobile device management software or their devices did not support some of the security controls such as encryption and were, therefore, forced to replace their mobile devices. The main focus of the mobile information security governance implementation was to protect the company's information and having the necessary governance in place before the planned mobility audit took place.

7.3.2.1.4 ENSURE COMPLIANCE

Different mechanisms are in place to ensure that the security controls and all governance artefacts such as the mobile device management policy, standards, processes and software are adhered to.

Users of mobile devices that were not compatible with the implemented mobile device management software were no longer allowed to access their company information on their mobile devices which led to dissatisfaction. Users did not have a choice as the security controls were applied via a system policy. Some users chose to no longer access their company information on their mobile device because they

felt that it was an invasion of their privacy, they were not happy that someone else was able to control their personal device and they were scared that their personal information would be compromised. In the end, the users who required access to their company information on their mobile device accepted that they needed to abide by the mobile device management software, policy, processes and standards.

Compliance is not only ensured via the mobile device management software but also through a manual intervention by the architectures and governance team and the internal audit department at the company which reviews compliance to the governance artefacts on a periodic basis.

7.3.2.1.5 PROVIDE SECURE ENVIRONMENT

The information security governance implementation applied security controls in the mobile device environment where none previously existed. The end goal was to provide a secure environment and while it was recognised that it was not possible to have a totally secure environment, the continual identification of risks, the implementation or consideration of information security governance and the mechanisms to ensure compliance aided in moving towards keeping the company information safe.

7.3.2.2 PERSPECTIVE TWO: INFORMATION SECURITY GOVERNANCE IN PLACE, NEW OR CHANGE PROPOSAL TO BE CONSIDERED

The theory as depicted in Figure 30 below consists of five process steps which are further elaborated as part of the storyline.

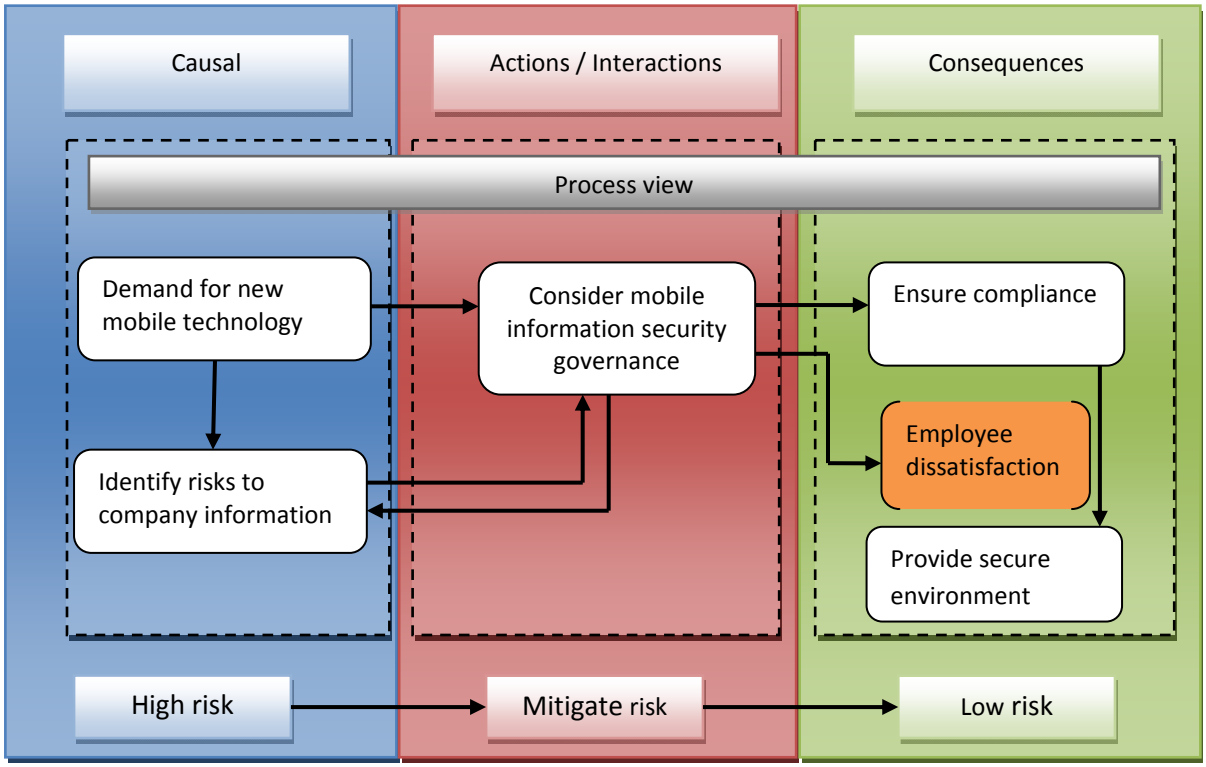


FIGURE 30 - PERSPECTIVE TWO: INFORMATION SECURITY GOVERNANCE IN PLACE, NEW OR CHANGE PROPOSAL TO BE CONSIDERED

7.3.2.2.1 DEMAND FOR NEW MOBILE TECHNOLOGY

The company-owned mobile devices are managed by the Procurement department and as a result the mobile device chosen as the company standard was not compatible with the existing mobile infrastructure. The choice was seen to be the most logical choice given the fact that the company had used this brand of device for a number of years. The new mobile device chosen as the company standard device worked differently to the existing mobile devices and was a completely new product.

7.3.2.2.2 IDENTIFY RISKS TO COMPANY INFORMATION

Unfortunately, these new devices had already been allocated to users and they were not able to access their company information on their device. Some of these users were not happy to wait until the necessary work was completed and wanted to have access to their company information on their mobile device without the necessary mobile security controls being in place. This led to the assessment and

documentation of the risk associated with giving these users access to company information on these new mobile devices which were unsecure and unsupported. After consideration it was decided that the risk was too high based on the concepts of “Unsecure usage” and “Company data leakage”. This highlights the link between ‘Demand for new technology’ and ‘Identify risks to company information’.

If the business users were willing to accept the risk, it needed to be signed off by the CIO according to the mobile device management policy. This was not the case and, therefore, the business users had to wait until all the necessary work was completed. This highlights the link between the process steps ‘Demand new technology’ and ‘Consider mobile information security governance’.

7.3.2.2.3 CONSIDER INFORMATION SECURITY GOVERNANCE

The new generation mobile device consisted of two profiles, a work and a personal profile. Once the server was installed and configured, questions arose regarding the two profiles and who the decision makers were as far as the IT policy settings for this mobile device. The architectures, governance and security team was approached in order to make the relevant decisions.

According to the mobile device management policy developed, the role of the security specialist was to review any changes with regards to devices or sources of information that are not securely supported by the existing infrastructure. A security assessment of the configuration settings of the new mobile device and also an understanding of how this new device could be integrated into the existing architecture so that the best decision could be made taking the overall mobility architecture into consideration was required. Any risks to company information were identified and mitigated as part of the information security assessment. This highlights the iteration between the steps ‘Identify risks to company information’ and ‘Consider information security governance’.

The shortage of information security specialists had an impact on the completion date which was based on the current workload and priorities. Company information could not be stored on this new mobile device until all activities including the information security assessment were completed. This led to dissatisfaction amongst

employees because some of them were due for mobile upgrades and some had faulty devices.

7.3.2.2.4 ENSURE COMPLIANCE

Compliance to the governance artefacts such as the mobile device management policy and standards was achieved by meeting the information security requirements and by not allowing access to company information on the new mobile devices until the necessary work including the security assessment was completed. The security controls defined in the first implementation were applied and tested on the new mobile devices before giving users access to their company information.

In doing these activities, when the mobile device management environment is audited in future, all the necessary work as specified in the mobile device management policy would have been done and should, therefore, not result in any audit findings because compliance was ensured.

7.3.2.2.5 PROVIDE SECURE ENVIRONMENT

The mobile information security governance implemented during the first implementation was used to govern the mobile device management environment for the second implementation. The identification of the risk of ‘Unsecure usage’ and ‘Company leakage’ with the new mobile device can be seen as the starting point. The information security of the new devices was considered and implemented and, therefore, these new devices have safely been integrated into the company’s mobile environment with all the necessary security controls applied. By ensuring compliance to the information security governance artefacts developed during the first implementation, the risks associated with the new mobile device were mitigated thereby keeping the mobile device management area as close as possible to a secure environment.

7.4 FINAL GROUNDED THEORY IN RELATION TO EXISTING LITERATURE

As a result of the iterative nature between the process steps ‘Identify risks to company information’ and ‘Implement/consider information security governance’, the grounded theory developed was updated to reflect the gap that was highlighted during the development of the storyline. According to Birks et al. (2009) this is an

advantage of using the storyline because it highlights gaps, holes and inconsistencies in a grounded theory and makes the limitations obvious in the same way as a story would be incomplete if pages were torn from a novel.

The final grounded theory illustrates that risks to company information must be considered so that any potential risks with new or change proposals are detected as depicted in Figure 31 below. This theory shows that once mobile information security governance is in place, it must always be considered when any new or changes are proposed to the mobile environment to ensure that any potential risks are mitigated.

Employee dissatisfaction has been highlighted in the theory because it emerged as a strong concept during the analysis. As a result of insufficient change management and the process of trying to remain compliant with the mobile information security governance, there were implications on the satisfaction of the organisation's employees. This may be a concept that organisations should take more seriously when implementing mobile information security governance since there are implications of ignoring the satisfaction of employees. The implications and how the concepts in the theory relate back to existing literature is further discussed in the next section.

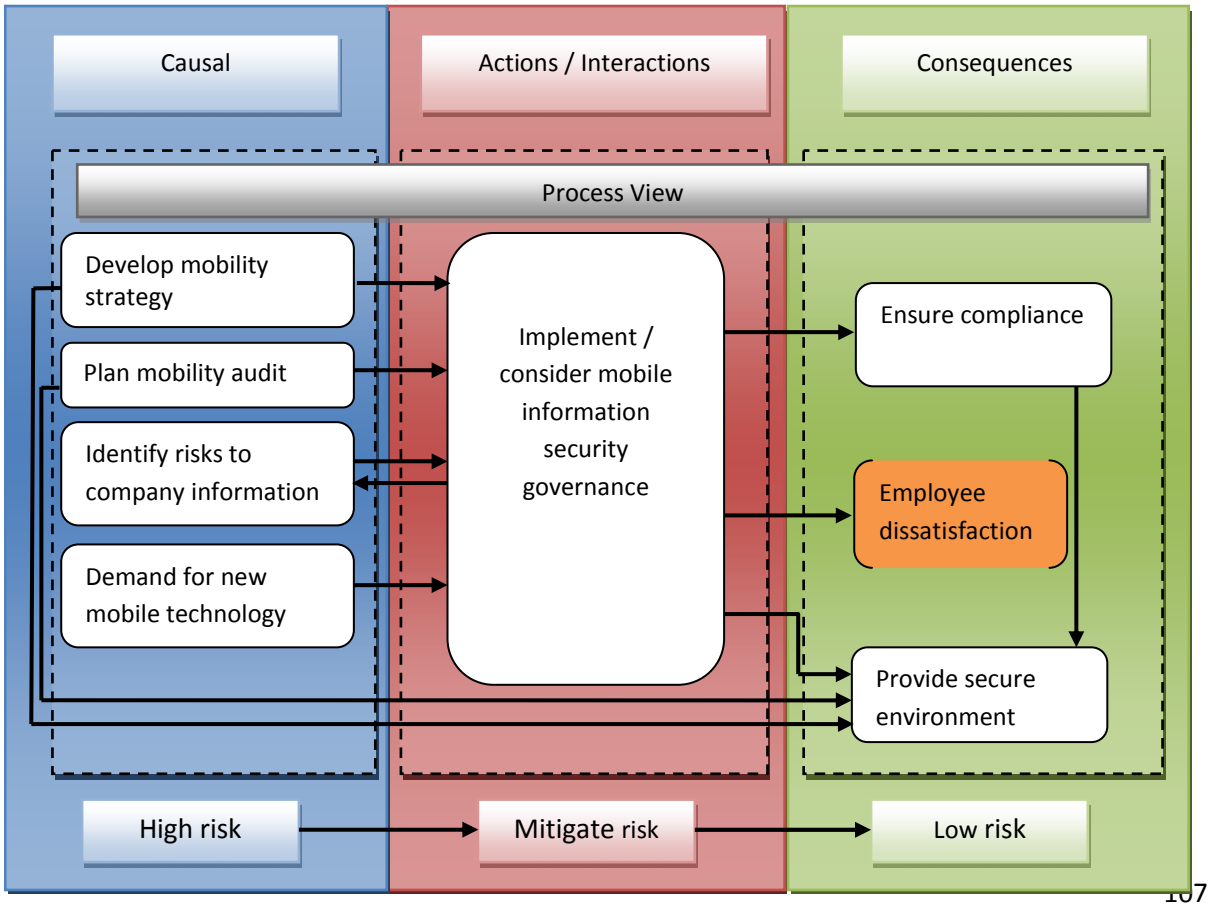


FIGURE 31 - STRIVING TOWARDS A SECURE ENVIRONMENT

7.4.1 DISCUSSION AND IMPLICATIONS

Little literature exists on how organisations go about implementing information security governance within the mobile device environment. This research has made a contribution because many organisations are struggling with the concept of information security governance within the mobile device environment and has shed some light with regards to the issues organisations may face such as device fragmentation and change management.

Each category, sub-category and concept highlighted in the final grounded theory depicted in Figure 31 are discussed further in relation to existing literature.

7.4.1.1 MOBILITY STRATEGY

Best practice frameworks such as COBIT includes strategy as part of one of their main focus areas, plan and organise, for IT governance. IT plans must be developed and aligned with the organisation's business strategies (IT Governance Institute, 2004). 'Mobility strategy' is a relevant sub-category since employees are increasingly moving towards using mobile devices to accesss company information. Ernst and Young (2012a) state that technologies such as mobile computing must be included as part of a new information security strategy and should focus on identifying current risks from a fresh perspective due to technology advancements such as mobile computing.

7.4.1.2 MOBILITY AUDIT

Audit was specifically excluded from the definition of information security governance by Moulton and Coles (2003) because the authors felt that it does not form part of information security governance. 'Mobility audit', however, is still a valid sub-category as a driver and as a consequence of the mobile information security governance implementation since audit ensures that the governance processes are established and functions properly (Moulton & Coles, 2003). Audit aids in ensuring that the organisation's data contained in systems are secure (Von Solms, 2006). In the case of this research, audit was the main driver of the implementation which led to all necessary governance artefacts such as policies, technology, processes and standards to be developed.

7.4.1.3 RISKS TO COMPANY INFORMATION

The identification of current risks and an understanding of what the most important data and applications are and where they reside should be part of the company's information security strategy. A fresh perspective is required when identifying risks, it should not be a process of carrying forward the previous years risks since the risks to company information are different because there are different points of exposure (Ernst & Young, 2012a) such as new mobile technologies. The concept of 'Risks to company information' is valid, it may not be a new concept but due to the advancement of technology and the increasing number of employees using mobile devices for personal and business use, organisations are more vulnerable to new risks associated with mobility.

7.4.1.4 NEW MOBILE TECHNOLOGY

When the year 2016 arrives, approximately 10 billion internet enabled mobile devices will be in existence which equates to every man, woman and child on the planet owning 1.5 of those devices according to a Cisco forecast. Mobile devices are used for both personal and business activities, no longer solely for telephone calls but as a knowledge source and communications tool. The evolving mobile technologies have resulted in organisations urgently implementing mobile policies in order to address the risks to company information (Ernst & Young, 2012a). This confirms the validity of the concept of 'New mobile technology'. Technology advancement together with the benefits to the employee have led to an increase in the adoption of mobile technology (Ernst & Young, 2012a) and due to the vast range of evolving mobile technologies, the implementation of mobile information security governance is important because no longer are mobile devices such as tablets used by executives alone but by the rest of the organisation as well.

7.4.1.5 MOBILE INFORMATION SECURITY GOVERNANCE IMPLEMENTATION/CONSIDERATION

The category relating to the implementation and consideration of information security governance is validated by a global information security survey conducted by Ernst and Young (2012a) showing an increase in the number of external attacks noticed by respondents from 41% in 2009 to 71% in 2011 and to 77% in 2012. According to this survey, organisations have also noticed an increase in internal vulnerabilities of which 37% of the respondents felt that the threat that increased the most over the

past 12 months was that of unaware employees (Ernst and Young, 2012a). This also validates the change management aspect of a mobile information security governance implementation, education should form part of the implementation relaying the importance of security to the employees (Whitman, 2003). It is important that all aspects of information security governance are considered during an implementation.

7.4.1.6 ENSURE COMPLIANCE

'Ensure compliance' is a valid category since a fundamental requirement for any information security initiative is increasing an end-user's compliance with information security policies (Padayachee, 2012). This research shows that various methods accomplish compliance to policies such as the use of systems, manual interventions and regular audit reviews.

7.4.1.7 EMPLOYEE DISSATISFACTION

A study undertaken by Post and Kagan (2007) indicate that generally employees perceive that there is a greater interference with their job responsibilities when more onerous measures or increases in security practices and policies are enforced. 'Employee dissatisfaction' is, therefore, a valid category. When information security controls are designed and implemented more care should be shown towards employees so that there is less interference with employees' job roles and their productivity. In order to accomplish this, Post and Kagan (2007) suggests that the employees must be a part of the security design policy which should result in minimum user disruption and maximum user access. This may alleviate the concerns raised regarding organisations being at risk because their information security policies are not being followed by their employees (Siponen et al., 2009). The mobile information security policy must allow user access without affecting the employees task completion and job performance while protecting the organisation's assets (Post & Kagan, 2007).

7.4.1.8 PROVIDE SECURE ENVIRONMENT

The conceptual framework (Figure 10) developed from literature shows how all the information security governance themes whether they are technical or non-technical all work together to ensure a secure environment for the organisation. 'Provide secure environment' is a valid category because it is ultimately what information security governance works towards, ensuring "that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people, etc.) are maintained at all times" (Von Solms, 2006, p. 167). The conceptual framework developed from the information security governance themes is valid within the mobile device environment. If all aspects of the conceptual framework are considered, the security around the organisation's information accessed on mobile devices will lead to a more secure mobile device environment.

8 LIMITATIONS AND FUTURE RESEARCH

8.1 LIMITATIONS

The research was restricted by the timing and duration of the master's course.

Two implementations were analysed, the initial implementation investigated the implementation of information security governance whereas the second one investigated and analysed the impact the first implementation had on the second one. This was the only implementation that was investigated and analysed to determine the impact that the information security governance had on the implementation due to time constraints. It may have been more beneficial to be able to analyse additional subsequent implementations so that the emergent theory could be further grounded in data by possibly adding additional scenarios to the storyline.

The paradigm model was used to form relationships between categories and sub-categories. The research mostly focused on the causal conditions, the phenomenon, actions/ interactions and consequences. The contextual conditions and intervening conditions have, however, not been specified according to the paradigm model.

8.2 FUTURE RESEARCH

This research is a good starting point for further research. Many avenues were identified as part of the research but were not pursued and could potentially be further investigated as described below:

- A comparison between the role of the IT auditor, risk management and information security governance within organizations.
- How will organisations cope with device fragmentation as technology advancement will intensify the problem.
- Should the management of mobile devices continue to reside in departments outside of the Information Services department when the technical specialists are the ones that hold the knowledge about the complexities of the company's mobility architecture and devices, and know whether it will work within the existing environment?
- The influence of vendors on the Business with regards to technology products and the associated impacts.
- The alignment of Business and IT with regards to information security. The Business's perception of information security is quite different from IT's perspective. The business users generally feel like they can take riskier decisions with company information because they do not see the information as being confidential company information.
- The ownership of business information. The true owners of business information reside in the business but they do not feel accountable for the information because they are too far removed from the deemed accountability. The assumption made is that the CIO is accountable and responsible for company information. How do organisations go about shifting the ownership of business information?
- Lastly, the main aim of information security is to protect the company's information from potential risks, yet there is a risk to personal information as well from an employee's perspective. Employees are also taking a risk by using their personal mobile device in order to be more effective in their jobs and ultimately for the benefit of the company but how is the employee's personal information protected?

9 CONCLUSION

Most employees prefer to use their own personal devices for work purposes which pose many challenges to the organisation from a technology perspective such as device fragmentation and many risks to company information such as company data leakage and unauthorised access. Mobile information security governance is able to address these risks. All risks to company information must be identified whether the implementation is a planned or unplanned one so that the mobile information security governance is considered. Changes within the existing mobile environment (new or change to existing) are considered to be potentially high risks to company information until they have been assessed and accepted or mitigated. Once the mobile information security governance has been implemented, compliance must be ensured which provides assurance that risks to company information are constantly mitigated. When this is done, the organisation may move from a state of having high risks to company information, to mitigating or accepting those risks, to a low risk state because the mobile information security governance has been considered or implemented. This is done to ultimately provide a secure environment for the organisation.

This research has shown how organisations go about implementing information security governance within the mobile device environment which is pertinent due to the increasing number of employees using their personal mobile devices in both a personal and professional context. A grounded case study strategy enabled the research question to be answered and theory to be development with the use of procedures and techniques of the grounded theory methodology.

The research confirms that it is important that all aspects of information security governance are taken into consideration such as user awareness to avoid dissatisfied employees which will ultimately impact on employee productivity, job roles and conformance with policy. The research has also revealed that governance alone is not sufficient to protect the company's information. An integrated view as suggested by Racz, Weippl, and Seufert (2010) of governance, risk management and compliance is necessary.

While the existing research focused on mobile information security governance implementation and while it is recognised that it is not possible to have a completely

secure environment, the research has found that the close relationship between risk management, information security governance and compliance is vital to striving towards providing a secure environment for the organisation.

10 REFERENCES

Adams, A., & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM,* 42(12), 40-46.

Anderson, J. (2003). Why we need a new definition of information security? *Computers & Security,* 22(4), 308-313.

Ashford, W. (2012). Keeping ahead of advancing threats requires an intelligent team effort. *Computer Weekly,* p.4-5. Retrieved August 22, 2012, from Business Source Premier.

Birks, M., Mills, J., Francis, K., & Chapman, Y. (2009). A thousand words paint a picture: The use of storyline in grounded theory research. *Journal of Research in Nursing,* 14(5), 405-417.

Booker, R. (2006). Re-engineering enterprise security. *Computers & Security,* 25(1), 13-17.

Bresz, F. (2004). People – Often the Weakest Link in Security, But One of the Best Places to Start. *Journal of Health Care Compliance,* 6(4), 57-60.

Burt, J. (2011). BYOD trend pressures corporate networks. *eWeek,* 28(14), 30-31.

Chen, W., & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal,* 14(3), 197-235.

Chigona, W., Robertson, B., & Mimbi, L. (2012). Synchronised smart phones: the collision of personal privacy and organisational data security. *South African Journal of Business Management,* 43(2), 31-40.

Cisco. (2008). *Data leakage worldwide: The effectiveness of security policies.* Retrieved August 14, 2012, from http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.html.

Clement, R. (2005). The lessons from stakeholder theory for U.S. business leaders? *Business Horizons,* 48(3), 225-264.

Coen, M., & Kelly, U. (2007). Information management and governance in UK higher education institutions: bringing IT in from the cold. *Perspectives: Policy & Practice in Higher Education,* 11(1), 7-11.

Da Veiga, A., & Eloff, J. (2007). An information security governance framework. *Information Systems Management,* 24(4), 361-372.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. *Information Systems Journal,* 8(4), 273–289.

De Oliveira Alves, G.A., Da Costa Carmo, L.F.R., & De Almeida, A.C.R.D. (2006). *Enterprise security governance: A practical guide to implement and control information security governance (ISG)*, International workshop on Business Driven IT Management, Nanjing,

April 3-7, 2006. Retrieved July 10, 2012, from http://ieeexplore.ieee.org.ezproxy.uct.ac.za/stamp/stamp.jsp?tp=&arnumber=1649213

Dhillon, G., & Backhouse, J. (2000). Technical opinion: information system security management in the new millennium. *Communications of the ACM,* 43(7), 125-128.

Dhillon, G., Tejay, G., & Hong, W. (2007). *Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations*, 40th Annual Hawaii International Conference on System Sciences, Hawaii, January 3-6, 2007. Retrieved July 10, 2012, from http://ieeexplore.ieee.org.ezproxy.uct.ac.za/stamp/stamp.jsp?tp=&arnumber=4076695

Dlamini, M., Eloff, J., & Eloff, M. (2009). Information security: The moving target. *Computers & Security,* 28(3-4), 189-198.

Donaldson, T., & Preston, L. (1995). The stakeholder theory of the corporation: concepts, evidence, and implications. *The Academy of Management Review,* 20(1), 65-91.

Duchscher, J. E., & Morgan, D. (2004). Grounded theory: Reflections on the emergence vs. forcing debate. *Journal of Advanced Nursing,* 48(6), 605-612.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review,* 14(4), 532-530.

Ernst & Young. (2012a). *Fighting to close the gap.* Retrieved 2 9, 2014, from http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf

Ernst & Young. (2012). *Mobile device security: Understanding vulnerabilities and managing risks.* Retrieved December 18, 2013, from http://www.ey.com/Publication/vwLUAssets/Mobile_Device_Security/$FILE/Mobile-securitydevices_AU1070.pdf

Fernandez, T. (2012). BYOD: easing the trepidation. *Money Management Executive,* 20(22), 1-10.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Sage Journals,* 12(2), 219-245.

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

Ghiran, A., & Bresfelean, V. P. (2012). Compliance Requirements for Dealing with Risks and Governance. *Procedia Economics and Finance,* 3, 752-756.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research.* New Brunswick: Aldine transaction.

Gordon, P. (2007). *Data leakage – threats and mitigation.* Retrieved August 14, 2012, from http://www.sans.org/reading_room/whitepapers/awareness/data-leakage-threats-mitigation_1931.

Gorge, M. (2006). Mobility and security: two sides of the same coin. *Computer Fraud & Security,* 2006(11), 15-18.

Goulding, C. (1998). Grounded theory: the missing methodology on the interpretivist agenda. *Qualitative Market Research,* 1(1), 50-57.

Goulielmos, M. (2004). Systems development approach: transcending methodology. *Information Systems Journal,* 14(4), 363-386.

Green, A. (2007). *Management of security policies for mobile devices*, 4th annual conference on information security curriculum development, Georgia, Sept 28-29, 2007. Retrieved August 14, 2012, from http://delivery.acm.org.ezproxy.uct.ac.za/10.1145/1410000/1409933/a22-green.pdf?ip=137.158.158.60&acc=ACTIVE%20SERVICE&CFID=104840894&CFTOKEN=59166920&__acm__=1344977685_6420fcd9dbc7a20cc3d8417afbc49c0b

Harris, C. (2012). *Mobile consumerization trends and perceptions.* Retrieved May 25, 2014, from http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Harris, S. (2007). *CISSP certification all-in-one exam guide fourth edition.* New York: McGraw-Hill Publishing.

Hart, J. (2013). Why the traditional approach to information security is no longer working. *Network Security,* 2013(1), 12-14.

Heiser, J., & Scholtz, T. (2009). Gartner for IT leaders overview: The chief information security officer, 2009-2010. *Gartner*, 1-9.

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

Hinde, S. (2002). Security surveys spring crop. *Computers & Security,* 21(4), 310-321.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report,* 13(4), 247-255.

ISACA. (2012). *ISACA issues COBIT 5 for information security.* Retrieved August 14, 2012, from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Issues-COBIT-5-for-Information-Security.aspx.

IT Governance Institute. (2004). *COBIT Student book.* Retrieved 2 9, 2014, from http://www.isqa.unomaha.edu/dkhazanchi/teaching/ISQA4590-8596/Readings/ISACA-COBIT%20FRAMEWORK/Cobit_Student_Book.pdf.

IT Governance Institute. (2008). *Information Security Governance: Guidance for Information Security Managers.* Retrieved July 10, 2012, from http://www.globalteksecurity.com/SEGURIDAD_EN_LA_NUBE%20%20VIRTUALIZACION/Information%20Security%20Governanc.

Jian, Z., Wei-hua, Y., & Wen-jing, Q. (2011). *Research on security management and control system of information system in IT governance*. Paper presented at the International conference on Computer Science and Service System, Nanjing, June 27-29, 2011.

Retrieved July 24, 2012, from http://ieeexplore.ieee.org.ezproxy.uct.ac.za/stamp/stamp.jsp?tp=&arnumber=5974703

Johnson, A., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM,* 52(1), 126-129.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security,* 24(3), 246-260.

Klein, H., & Myers, M. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly,* 23(1), 67-94.

Kotulic, A., & Clark, J. (2004). Why there aren't more information security research studies. *Information & Management,* 41(5), 597-607.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security,* 27(5-6), 224-231.

Levine, R. (2005). Technology evolution drives need for greater information technology security. *Computers & Security,* 24(5), 359-361.

Li, F., Clarke, N., Cowan, E., Papadaki, M., & Dowland, P. (2011). Misuse detection for mobile devices using behaviour profiling. *International Journal of Cyber Warfare and Terrorism,* 1(1), 1-13.

Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. *Computer Fraud & Security,* 2012(4), 14-17.

Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO27001. *International Journal of Network Security & Its Applications,* 3(4), 111-116.

Matavire, R., & Brown, I. (2013). Profiling grounded theory approaches in information systems research. *European Journal of Information Systems*, 1-11.

McGhee, G., Marland, G., & Atkinson, J. (2007). Grounded theory research: literature review and reflexivity. *Journal of Advanced Nursing,* 60(3), 334-342.

McMillan, R., & Scholtz, T. (2010). Security governance and operations are not the same. *Gartner*, 1-8.

Merriam, S. (1988). *Case study research in education: A qualitative approach.* California: Jossey-Bass Publishers.

Millard, A. (2013). Ensuring mobility is not at the expense of security. *Computer Fraud & Security,* 2013(9), 11-13.

Mishra, S., & Dhillon, G. (2006). *Information systems security governance research: a behavioural perspective*, 1st Annual Symposium on Information Assurance: Intrusion detection and prevention, Albany, June 14-15, 2006. Retrieved July 10, 2012, from http://www.albany.edu/wwwres/conf/iasymposium/proceedings/2006/mishra.pdf

Moulton, R., & Coles, R. (2003). Applying information security governance. *Computers & Security,* 22(7), 580-584.

Myers, M., & Klein, H. (2011). A set of principles for conducting critical research in information systems. *MIS Quarterly,* 35(1), 17-36.

Na-yun, K., Robles, R.J., Sung-Eon, C., Yang-Seon, L., & Tai-hoon, K. (2008). *SOX act and IT security governance*, International Symposium on Ubiquitous Multimedia, Hobart, October 13-15, 2008. Retrieved July 10, 2012, from http://ieeexplore.ieee.org.ezproxy.uct.ac.za/stamp/stamp.jsp?tp=&arnumber=4656548

Nolan, R., & McFarlan, F. (2005). Information technology and the board of directors. *Harvard Business Review,* 83(10), 96-106.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: research approaches and assumptions. *Information Systems Research,* 2(1), 1-28.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security,* 31(5), 673-680.

Pather, S., & Remenyi, D. (2004). *Some of the philosophical issues underpinning research in information systems: from positivism to critical realism*, Proceedings of the 2004 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries, Stellenbosch, October 4-5, 2004. Retrieved October 10, 2012, from http://dl.acm.org.ezproxy.uct.ac.za/citation.cfm?id=1035070

Post, G., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers and Security,* 26(3), 229–237.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers and Security,* 23(8), 638-646.

Pozzebon, M., Petrini, M., & Bandeira de Mello, R. (2011). Unpacking researcher's creativity and imagination in grounded theorizing: an exemplar from IS research. *Information and Organisation,* 21(4), 177-193.

Racz, N., Weippl, E. & Seufert, A. (2010). *A process model for integrated IT governance, risk, and compliance management*. Proceedings of the 2011 conference on Databases and Information Systems VI: Selected Papers from the Ninth International Baltic Conference, DB&IS 2010, Riga, July 5-7, 2010. . Retrieved January 9, 2014, from http://www.grc-resource.com/resources/racz_al_grc_process_model_balticdbis2010.pdf

Raghupathi, W. (2007). Corporate governance of IT: a framework for development. *Communications of the ACM,* 50(8), 94-99.

Raup-Kounovsky, A., Canestraro, D., Pardo, T & Hrdinova, J. (2010). *IT Governance to fit your context: two U.S. case studies*. 4th International conference on Theory and Practice of Electronic Governance, Beijing, October 25-28, 2010. Retrieved July 24, 2012 from http://delivery.acm.org.ezproxy.uct.ac.za/10.1145/1940000/1930365/p211-raup-kounovsky.pdf?ip=137.158.158.60&acc=ACTIVE%20SERVICE&CFID=98312089&CFTOKEN=35745823&__acm__=1343254463_76b17df8e65ac3ef748b0a9e295de518

Rhee, H., Ryu, Y., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security,* 31(2), 221-232.

Saetang, S., & Haider, A. (2011). *Conceptual aspects of IT governance in enterprise environment*. 49th SIGMIS annual conference on Computer personnel research, San Antonio, May 19-21, 2011. Retrieved April 10, 2012, from http://delivery.acm.org.ezproxy.uct.ac.za/10.1145/1990000/1982164/p79-saetang.pdf?ip=137.158.158.60&acc=ACTIVE%20SERVICE&CFID=98312089&CFTOKEN=35745823&__acm__=1343259354_516fb97ffd671f6e7ad1ed51884c0b7b

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC17799. *The Information Management Journal,* 39(4), 60-66.

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research methods for business students.* Essex: Pearson Education Limited.

Scholtz, T. (2011a). Information security and risk governance: functions and processes. *Gartner*, 1-11.

Scholtz, T. (2011b). Information Security Organization Dynamics. *Gartner*, 1-8.

Short, J., & Gerrard, M. (2009). IT governance must be driven by corporate governance. *Gartner*, 1-7.

Simonsson, M., Lagerstrom, R., & Johnson, P. (2008). *A bayesian network for IT governance performance prediction,* 10th International conference on Electronic commerce, Innsbruck, August 18-22, 2008. Retrieved July 24, 2012, from http://delivery.acm.org.ezproxy.uct.ac.za/10.1145/1410000/1409542/a1-simonsson.pdf?ip=137.158.158.60&acc=ACTIVE%20SERVICE&CFID=98312089&CFTOKEN=35745823&__acm__=1343255028_72db9e6f4de08cb81f2327246f167b3f

Siponen, M., Mahmood, A., & Pahnila, S. (2009). Technical opinion Are employees putting your company at risk by not following information security policies. *Communications of the ACM,* 52(12), 145-147.

Sophos. (2008). *Stopping data leakage: exploiting your existing security investment.* Retrieved August 14, 2012, from http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophosdlpwpna.pdf.

Spafford, G. (2003). *The benefits of standard IT governance frameworks.* Retrieved April 4, 2012, from http://www.itmanagementonline.com/Resources/Articles/The_Benefits_of_Standard_IT_Governance_Frameworks.pdf.

Stevens, L. (2007). Toolkit best practices: Creating Security Policy Documents (Security Policy Guidelines, Part 3). *Gartner*, 1-8.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: grounded theory procedures and techniques.* California: Sage publications.

The Security Executive Council. (2013). Bring your Own Device (BYOD) to Work. *Trend Report,* vii.

Thomson, G. (2012). BYOD: enabling the chaos. *Network Security,* 2012(2), 5-8.

Thomson, K., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security,* 2006(10), 7-11.

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security,* 2013(4), 12-13.

Urquhart, C., Lehmann, H., & Myers, M. D. (2010). Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems. *Information Systems Journal,* 20(4), 357-381.

Venter, H., & Eloff, J. (2003). A taxonomy for information security technologies. *Computers & Security,* 22(4), 299-307.

Von Solms, B. (2001). Information security – a multidimensional discipline. *Computers & Security,* 20(6), 504-508.

Von Solms, B. (2006). Information security – the fourth wave. *Computers & Security,* 25(3), 165-168.

Von Solms, B. (2005a). Information security governance: COBIT or ISO 17799 or both? *Computers & Security,* 24(2), 99-104.

Von Solms, B., & Von Solms, R. (2005). From information security to business security. *Computers & Security,* 24(4), 271-273.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security,* 23(5), 371-376.

Von Solms, R., & Von Solms, B. (2006). Information security governance: Due care. *Computers & Security,* 25(7), 494-497.

Von Solms, S. H. (2005b). Compliance management vs operational management. *Computers & Security,* 24(6), 443-447.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security,* 23(3), 191-198.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems,* 15(3), 320–330.

Walsham, G. (1995). The emergence of interpretivism in IS research. *Information Systems Research,* 6(4), 376-394.

Walton, J. (2002). *Developing an enterprise information security policy*, 30th annual ACM SIGUCCS conference on User services, Rhode Island, November 20-23, 2002. Retrieved July 10, 2012, from http://delivery.acm.org.ezproxy.uct.ac.za/10.1145/590000/588678/p153-walton.pdf?ip=137.158.158.60&acc=ACTIVE%20SERVICE&CFID=98312089&CFTOKEN=35745823&__acm__=1343255285_dc455ab8341a7c638f268f84b9c40314

Ward, P., & Smith, C. (2002). The development of access control policies for information technology systems. *Computers & Security,* 21(4), 356-371.

Whitman, M. (2003). Enemy at the gate: threats to information security. *Communications of the ACM,* 46(8), 91-95.

Williams, P. (2007). Executive and board roles in information security. *Network Security,* 2007(8), 11-14.

Williams, P., & Andersen, A. (2001). Information security governance. *Information Security Technical Report,* 6(3), 60-70.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly,* 37(1), 1-20.

Wolfpack. (2011). *South African information security thermometer*. Retrieved August 14, 2012, from http://www.wolfpackrisk.com/the-2011-south-african-information-security-thermometer-survey/

Xiaomeng, S., Bolzoni, D., & Van Eck, P. (2007). *Understanding and specifying information security needs to support the delivery of high quality security services,* International conference on Emerging Security Information, Systems and Technologies, Valencia, October 14-20, 2007. Retrieved July 24, 2012, from http://ieeexplore.ieee.org.ezproxy.uct.ac.za/stamp/stamp.jsp?tp=&arnumber=4385319

Yin, R. (2004). *Case study methods.* Retrieved October 10, 2012, from http://www.scribd.com/doc/37102046/Robert-Yin-Case-Study-Research

Yin, R. (1994). *Case study research: design and methods* (2nd ed.). California: Sage publications.

11 APPENDICES

11.1 APPENDIX A – FIRST INTERVIEW GUIDELINE

Semi-structured interviews were conducted and the questions listed below were used as a guide to conduct the first interview, after analysing the data collected a decision was made as to what data needed to be collected next.

PARTICIPANT OVERVIEW

1. Briefly describe your role in the organisation.
2. How many years experience do you have in this role?
3. What is your understanding of information security?

CONTEXT

4. Describe what the mobility implementation was about and why is it was initiated.
5. Describe the goals and objectives of the mobility implementation.
6. How has the mobility implementation been aligned with the business goals and objectives and how can this be verified?

PRE-IMPLEMENTATION

7. How did the team go about designing the mobility implementation? Who was involved?
8. What was the scope of the implementation plan?
9. What activities were undertaken before the implementation started? Were there any activities that were omitted that should have taken place prior to implementation?
10. Who signed off / gave the go-ahead of the mobility implementation? Was there a formal document that was signed off?
11. Was executive management involved in the decision to go ahead with the implementation? If not, would it have made a difference and how? If yes, do you think that it had an impact on the implementation and how?

12. If best practices are mentioned in the pre-implementation questions, then how effective was the use of best practices?
13. When did the actual implementation take place?

INFORMATION SECURITY TECHNOLOGIES

14. What technologies were used for the implementation? How were they selected? Are the technologies chosen effective and why?
15. Do you think the right decision was made in terms of the technology chosen and why?

POLICIES, PROCESSES AND PROCEDURES

16. Were the relevant information security policies, processes and procedures related to the implementation created or updated? Was this done prior to implementation?
17. How effective are the organisation's information security policies, processes and procedures? If possible, please provide examples.
18. Are the policies effectively implemented and managed and how?

INFORMATION SECURITY CULTURE

19. How would you describe an information security culture at an organisation and would you say that the organisation has an information security culture? Why?
20. Has the mobility implementation contributed to creating an information security culture? If yes, is this within the IS division only or within the broader organisation/ business as well? Why or why not?
21. Do you think that people actually understand why the mobility implementation was necessary? How do you think people feel about it? Was it easily accepted by people? Was there any resistance? Why were people resisting? What were the complaints?

ORGANISATIONAL STRUCTURES

22. How has the implementation changed the existing organisational structure?
23. Do you think the information security structure created is effective?

24. If not, what would make the information security implementation more effective?

ROLES AND RESPONSIBILITIES

25. Were the roles and responsibilities clearly defined between the various teams?

AWARENESS AND THREATS

26. How serious do you think threats to information are from a mobility perspective? Can you provide practical examples?
27. Do you think that people are generally aware of threats to information and how serious it is? Elaborate.

COMPLIANCE

28. How are we ensuring compliance with the mobility policy? Are employees complying with the mobility policy?

TRUST, COMMITMENT, CURRENCIES OF EXCHANGE, ALLIANCES

29. Do you think that the implementation accomplished the goals that it initially intended? So, it was a successful implementation?
30. If yes, what makes it a successful implementation?
31. If not, what could have been done differently to make it more successful?
32. Do you think good relationships have been formed between team members?
33. Have the information security professionals been able to supply you with information security information or assistance when required?
34. Do you feel comfortable enough with the information security professionals to ask questions when you are unsure of something related to the implementation?

SECURE ENVIRONMENT (CONFIDENTIALITY, INTEGRITY, AVAILABILITY)

35. Do you think that the implementation has made the environment more secure? How?
36. What activities could have contributed to a better implementation?
37. Are there any comments, suggestions or recommendations in terms of what has or hasn't worked for the mobility implementation?

11.2 APPENDIX B – RESEARCH PERMISSION LETTER

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag. Rondebosch 7701
Tel: +27 (0) 21 650 4028 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

December, 2012

To whom it may concern.

The Department of Information Systems at the University of Cape Town requires a dissertation for the successful completion of a masters degree in Information Systems. A study entitled "Information security governance implementation and executive management involvement" has been chosen by the researcher, Celeste Phillips.

The objective of the research is to gain an understanding of how organisations implement information security governance programmes and the level of involvement of executive management.

I……certify that I have committed members of my organisation to participate in the study titled 'information security governance implementation and executive management involvement' undertaken by Celeste Phillips. Data may be collected via interviews and documentation related to the study on condition that the organisation and individuals will be masked in the results of the study and that the study is for academic purposes only.

Signature:…… Date:……

11.3 APPENDIX C – COVER LETTER SENT TO PARTICIPANTS OF IMPLEMENTATION 1

Department of Information Systems
Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag, Rondebosch 7701
Tel: +27 (0) 21 650 4028 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

March, 2013

The Department of Information Systems at the University of Cape Town requires a dissertation for the successful completion of a masters degree in Information Systems. A study entitled "Information security governance implementation and executive management support" has been chosen by the researcher, Celeste Phillips.

The objective of the research is to gain an understanding of how organisations implement information security governance.

Your participation in this research will be highly appreciated and is completely voluntary. At any point in time you may choose to be excluded.

All information that is collected is for the sole purpose of the aforementioned dissertation and for academic purposes only. Any findings may be reported in a journal. The researcher guarantees the confidentiality of the interviewee and, therefore, no personal details will be disclosed.

Please consider making a contribution to this research.

Thank you for your assistance.

Sincerely,

Celeste Phillips
Masters Student

Irwin Brown
Research Supervisor

11.4 APPENDIX D – SUMMARY AND LETTER SENT TO EMAIL PARTICIPANTS OF IMPLEMENTATION 2

Dear [Participant],

The Department of Information Systems at the University of Cape Town requires a dissertation for the successful completion of a masters degree in Information Systems. A study entitled “How do organisations go about implementing information security governance for mobile devices” has been chosen.

The objective of the research is to gain an understanding of how organisations implement information security governance and the impact it has on subsequent mobile related implementations.

An analysis of the first Mobile Device Management implementation is being done and since the BlackBerry implementation is the second most recently completed mobile implementation, I would like to include it as part of the research that I am busy conducting. At this stage of the research, interviews will not be required. Secondary data such as email correspondence, etc. will be collected and analysed for the BlackBerry implementation. Interviews may be required at a later stage to confirm the data that has been analysed.

All information that is collected is for the sole purpose of the aforementioned dissertation and for academic purposes only. Any findings may be reported in a journal. No personal details will be disclosed.

The research will be beneficial to [Company] as it will provide a better understanding of the process and recommendations can be made for any future implementations.

If you have any questions or concerns with regards to the research being conducted, please let me know.

Thank you for your assistance and co-operation.

Regards,

Celeste

Department of Information Systems

Leslie Commerce Building
Engineering Mall, Upper Campus
OR
Private Bag, Rondebosch 7701
Tel: +27 (0) 21 650 4028 Fax: +27 (0) 21650 2280
Internet: http://www.commerce.uct.ac.za/informationsystems/

March, 2013

The Department of Information Systems at the University of Cape Town requires a dissertation for the successful completion of a masters degree in Information Systems. A study entitled "How do organisations go about implementing information security governance for mobile devices" has been chosen by the researcher, Celeste Phillips.

The objective of the research is to gain an understanding of how organisations implement information security governance.

Your participation in this research will be highly appreciated and is completely voluntary. At any point in time you may choose to be excluded.

All information that is collected is for the sole purpose of the aforementioned dissertation and for academic purposes only. Any findings may be reported in a journal. The researcher guarantees the confidentiality of the interviewee and, therefore, no personal details will be disclosed.

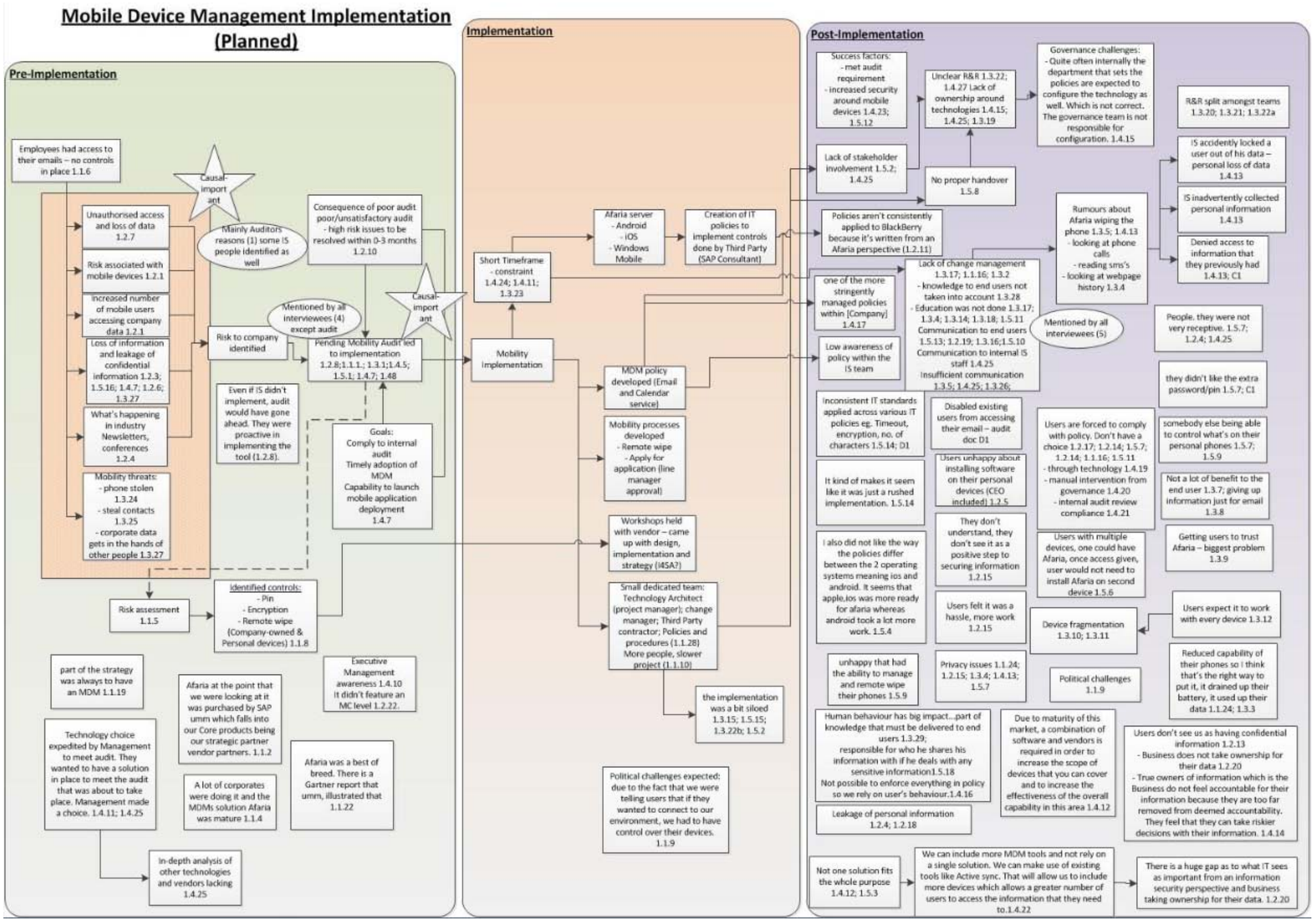
Please consider making a contribution to this research.

Thank you for your assistance.

Sincerely,

Celeste Phillips
Masters Student

Irwin Brown
Research Supervisor


Mobile Device Management Implementation (Planned)
Pre-Implementation
Implementation
Post-Implementation
Employees had access to their emails – no controls in place 1.1.6
Causal-important
Unauthorised access and loss of data 1.2.7
Risk associated with mobile devices 1.2.1
Increased number of mobile users accessing company data 1.2.1
Loss of information and leakage of confidential information 1.2.3; 1.5.16; 1.4.7; 1.2.6; 1.3.27
What's happening in industry Newsletters, conferences 1.2.4
Mobility threats:
- phone stolen 1.3.24
- steal contacts 1.3.25
- corporate data gets in the hands of other people 1.3.27
Mainly Auditors reasons (1) some IS people identified as well
Consequence of poor audit poor/unsatisfactory audit - high risk issues to be resolved within 0-3 months 1.2.10
Mentioned by all interviewees (4) except audit
Causal-important
Risk to company identified
Pending Mobility Audit led to implementation 1.2.8;1.1.1.; 1.3.1;1.4.5; 1.5.1; 1.4.7; 1.48
Even if IS didn't implement, audit would have gone ahead. They were proactive in implementing the tool (1.2.8).
Goals:
Comply to internal audit
Timely adoption of MDM
Capability to launch mobile application deployment
1.4.7
Risk assessment 1.1.5
Identified controls:
- Pin
- Encryption
- Remote wipe (Company-owned & Personal devices) 1.1.8
part of the strategy was always to have an MDM 1.1.19
Technology choice expedited by Management to meet audit. They wanted to have a solution in place to meet the audit that was about to take place. Management made a choice. 1.4.11; 1.4.25
In-depth analysis of other technologies and vendors lacking 1.4.25
Afaria at the point that we were looking at it was purchased by SAP umm which falls into our Core products being our strategic partner vendor partners. 1.1.2
A lot of corporates were doing it and the MDMs solution Afaria was mature 1.1.4
Afaria was a best of breed. There is a Gartner report that umm, illustrated that 1.1.22
Executive Management awareness 1.4.10 It didn't feature an MC level 1.2.22.
Short Timeframe - constraint 1.4.24; 1.4.11; 1.3.23
Afaria server
- Android
- iOS
- Windows Mobile
Creation of IT policies to implement controls done by Third Party (SAP Consultant)
Mobility Implementation
MDM policy developed (Email and Calendar service)
Mobility processes developed
- Remote wipe
- Apply for application (line manager approval)
Workshops held with vendor – came up with design, implementation and strategy (I4SA?)
Small dedicated team: Technology Architect (project manager); change manager; Third Party contractor; Policies and procedures (1.1.28) More people, slower project (1.1.10)
the implementation was a bit siloed 1.3.15; 1.5.15; 1.3.22b; 1.5.2
Political challenges expected: due to the fact that we were telling users that if they wanted to connect to our environment, we had to have control over their devices. 1.1.9
Success factors:
- met audit requirement
- increased security around mobile devices 1.4.23; 1.5.12
Unclear R&R 1.3.22; 1.4.27 Lack of ownership around technologies 1.4.15; 1.4.25; 1.3.19
Governance challenges:
- Quite often internally the department that sets the policies are expected to configure the technology as well. Which is not correct. The governance team is not responsible for configuration. 1.4.15
R&R split amongst teams 1.3.20; 1.3.21; 1.3.22a
Lack of stakeholder involvement 1.5.2; 1.4.25
No proper handover 1.5.8
IS accidently locked a user out of his data – personal loss of data 1.4.13
IS inadvertently collected personal information 1.4.13
Denied access to information that they previously had 1.4.13; C1
Policies aren't consistently applied to BlackBerry because it's written from an Afaria perspective (1.2.11)
Rumours about Afaria wiping the phone 1.3.5; 1.4.13
- looking at phone calls
- reading sms's
- looking at webpage history 1.3.4
one of the more stringently managed policies within [Company] 1.4.17
Lack of change management 1.3.17; 1.1.16; 1.3.2
- knowledge to end users not taken into account 1.3.28
- Education was not done 1.3.17; 1.3.4; 1.3.14; 1.3.18; 1.5.11
Communication to end users 1.5.13; 1.2.19; 1.3.16;1.5.10
Communication to internal IS staff 1.4.25
Insufficient communication 1.3.5; 1.4.25; 1.3.26;
Mentioned by all interviewees (5)
People, they were not very receptive. 1.5.7; 1.2.4; 1.4.25
Low awareness of policy within the IS team
they didn't like the extra password/pin 1.5.7; C1
Inconsistent IT standards applied across various IT policies eg. Timeout, encryption, no. of characters 1.5.14; D1
Disabled existing users from accessing their email – audit doc D1
somebody else being able to control what's on their personal phones 1.5.7; 1.5.9
Users are forced to comply with policy. Don't have a choice 1.2.17; 1.2.14; 1.5.7; 1.2.14; 1.1.16; 1.5.11
- through technology 1.4.19
- manual intervention from governance 1.4.20
- internal audit review compliance 1.4.21
It kind of makes it seem like it was just a rushed implementation. 1.5.14
Users unhappy about installing software on their personal devices (CEO included) 1.2.5
Not a lot of benefit to the end user 1.3.7; giving up information just for email 1.3.8
I also did not like the way the policies differ between the 2 operating systems meaning ios and android. It seems that apple,ios was more ready for afaria whereas android took a lot more work. 1.5.4
They don't understand, they don't see it as a positive step to securing information 1.2.15
Users with multiple devices, one could have Afaria, once access given, user would not need to install Afaria on second device 1.5.6
Getting users to trust Afaria – biggest problem 1.3.9
Users felt it was a hassle, more work 1.2.15
Device fragmentation 1.3.10; 1.3.11
Users expect it to work with every device 1.3.12
unhappy that had the ability to manage and remote wipe their phones 1.5.9
Privacy issues 1.1.24; 1.2.15; 1.3.4; 1.4.13; 1.5.7
Political challenges 1.1.9
Reduced capability of their phones so I think that's the right way to put it, it drained up their battery, it used up their data 1.1.24; 1.3.3
Human behaviour has big impact...part of knowledge that must be delivered to end users 1.3.29;
responsible for who he shares his information with if he deals with any sensitive information1.5.18
Not possible to enforce everything in policy so we rely on user's behaviour.1.4.16
Due to maturity of this market, a combination of software and vendors is required in order to increase the scope of devices that you can cover and to increase the effectiveness of the overall capability in this area 1.4.12
Users don't see us as having confidential information 1.2.13
- Business does not take ownership for their data 1.2.20
- True owners of information which is the Business do not feel accountable for their information because they are too far removed from deemed accountability. They feel that they can take riskier decisions with their information. 1.4.14
Leakage of personal information 1.2.4; 1.2.18
Not one solution fits the whole purpose 1.4.12; 1.5.3
We can include more MDM tools and not rely on a single solution. We can make use of existing tools like Active sync. That will allow us to include more devices which allows a greater number of users to access the information that they need to.1.4.22
There is a huge gap as to what IT sees as important from an information security perspective and business taking ownership for their data. 1.2.20