The Economics of Information Security

by

Moses Thandokuhle Dlamini

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

THE ECONOMICS OF INFORMATION SECURITY

BY

MOSES THANDOKUHLE DLAMINI

Dissertation submitted in fulfilment
of the
Requirement for the degree

MASTER OF SCIENCE (Computer Science)

in the

FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

UNIVERSITY OF PRETORIA

JULY 2010

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

SUPERVISOR: Prof. J.H.P. Eloff

DEPARTMENT: Department of Computer Science

Abstract

In the year 2008, world markets suffered a huge economic crisis. The extent of the economic crisis has been so severe and has had a global impact. As a contingency strategy, governments of wealthy nations have resorted to extensive bailouts and rescue packages to stop organisations from going bankrupt. A skyrocketing amount of money has been spent on rescue packages and bailouts for the tumbling organisations. However, this could not stop some of the world's wealthiest financial institutions e.g. Lehman Brothers, Northern Rock, etc from collapsing.

Most of the surviving organisations froze their expenditure, implemented cost-cutting measures and in the process, numerous employees lost their jobs. Executives were compelled to 'achieve more with less' in order to save their organisations from going bankrupt. It is on this premise that this research proposed the BC3I (Broad Control Category Cost Indicators) model, which is a step towards 'achieving more with less' within information security budgeting. The tumbling world markets and increased requirements for legal and regulatory compliance have made this a timely and relevant research that addressed a current, spot-on and global problem. The BC3I model as the main outcome of this research has indeed come at the right time.

The BC3I model as proposed in this research makes a real contribution towards assisting information security managers as they make informed decisions regarding the optimal and cost-effective allocation of financial resources to information security activities. The proposed model can be argued to be a good start towards the selection of appropriate controls to optimally and cost-effectively protect organisations' information assets and simultaneously achieve compliance with legal and regulatory mandates.

As a proof of concept, the practicality of the BC3I model has been demonstrated in three different scenarios. The model has been illustrated for an organisation chosen from the financial sector; being the hardest hit by the economic crisis. Furthermore, the financial sector is chosen because of its high reliance on information security for the most obvious reasons that of dealing with money and confidential customer information. Finally and for acceptance purposes, the model has been discussed and reviewed by industry experts from the financial sector.

Key Terms: Information security, information security investment, information security budget, information security controls, broad control categories, information security standards, budget constraints, regulatory compliance and cost indicators.

Acknowledgements

Special words of thanks go to my supervisor, Prof. J.H.P. Eloff and Prof. M.M. Eloff for their support, guidance, dedication, commitment, encouragement, belief in my capabilities, cultivating critical-thinking in me, and profound interest in my research.

Special words of thanks also go to my wife, Nosihle Dladla, family and friends for their support, love, patience, understanding and tolerance in the entire duration of this research.

Lastly, I would like to hereby acknowledge the support of SAP Research CEC Pretoria/SAP Meraka UTD and ICSA research group towards this research. Opinions expressed and conclusions arrived at are solely those of the author and cannot necessarily be attributed to ICSA research group and/or SAP Research CEC Pretoria/SAP Meraka UTD.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.0 Background

In today's information-based economy (Bodin, Gordon & Loeb, 2005 and Terzi, 2006), information and its supporting technology form the core of critical business assets. For this reason most organisations depend on information technology (IT) systems to store, process and exchange critical information with their customers, partners and shareholders. This dependency comes along with major risks to the information and its IT systems. As a result information security has gained an unprecedented interest from organisations that rely on information and its IT systems to conduct their business. This is to a greater extent influenced by the huge amounts of money that organisations lose due to information security failures.

Researchers have conducted numerous surveys to capture the total amount of monetary losses that emanates as a result of information security failures. Amongst the widely known surveys in industry is the annual Computer Security Institute (CSI formerly known as the CSI/FBI) computer crime and security survey (Richardson, 2008). This survey has repeatedly reported about organisations losing millions of dollars due to information security failures.

However, the CSI survey only focuses on information security failures in the United States of America (USA) which makes the losses reported therein insignificant when considering the world-wide scenario. As reported in the CSI surveys, organisations maybe losing a lot of money due to information security failures, but how much are they actually spending to protect themselves against these failures? Could they be spending less or more than enough? How much really is enough? How do we justify the spending to properly protect information systems? These questions may look trivial at a first glance, yet the answers are not that trivial. The next section investigates information security spending based on surveys conducted in industry.

1.1 Information Security Spending

Several surveys have been conducted to determine the amount of money that organisations are spending on information security. The following is a list of the most well known surveys focusing on information security spending:

- The CSI computer crime and security survey (Richardson, 2008)
- The Deloitte-Touche global security survey (Owen, 2008)
- The Forrester Research (Speyer et al., 2006)
- The Gartner Research (Pescatore et al., 2008)
- The Global State of Information Security Survey– A Joint Research of the CIO and CSO in partnership with PriceWaterhouseCoopers (Nash, 2008).

These surveys differ in their target population, sectors, countries they focus on and in their choice of respondents among other things. However, most of these surveys argue that organisations spend about 10% of their overall IT budget on information security. Is this enough to secure organisations information assets? Most of the surveys point to an increase in information security spending since 2005, a clear indication that the current 10% of IT budget is not enough (Nash, 2008; LeClare, 2008; Vadera, Potter & Beard, 2008; Richardson, 2007; Melek & MacKinnon, 2005, 2006, Melek, MacKinnon & Kantamneni 2007, Owen 2008; Berinato & Ware, 2005 and Holmes, 2006). What does the future hold for information security spending?

Considering the future of information security spending, MarketResearch.com (2008), LeClare (2008), Research and Market (2008) and Cable (2007) project that the global information security market will continue to increase. Even though, there are different views on the projected figures, all the indicators and projections point to an increase in future information security spending.

The increase reflects the growing commitment of organisations towards information security. When organisations make a commitment to any investment, they surely expect a return. Unfortunately, due to a number of reasons the return on information security investment remains unclear (Liu, Tanaka & Matsuura, 2006; Pfleeger and Pfleeger, 2007; 578). Geer (2002) suggests a cost-effective analysis instead of the usual cost-benefit analysis due to the unclear benefits of information security measures. For instance, it remains unknown if the increase in information security spending as a response to the ever growing number of information security failures really minimises the risk exposure and by how much? It is thus relevant to briefly consider the drivers for information security spending.

Based on the information security surveys discussed previously and the surveys below, this section investigates the major drivers for the increase in information security spending.

- Ernst & Young's Annual Global Information Security survey (van Kessel, 2008), CompTia survey (CompTIA, 2008),
- AMR Research (Swanton & Scott, 2005),
- Celent Research (Jegher et al., 2007) and
- Towergroup Research (Kaya, 2007).

From the year 2005 – 2008 the surveys reflect different views on the real drivers for information security spending (Melek & MacKinnon, 2005; van Kessel, 2006, 2007; Berinato & Ware, 2005; Holmes, 2006; Berinato, 2007). However, most of the surveys show that regulatory compliance is playing a significant role on the increase in information security spending. This can be attributed to the large number of regulations regarding the protection of information most of which came about from the beginning of the 21st century. Moreover, the penalties or consequences of non-compliance to these regulations are very high, forcing organisations to be vigilant in their information security spending.

Even with the increasing information security spending and regulatory compliance pressure, high profile organisations continue to suffer huge losses related to information security problems.

Why? The next section discusses why this is the case and provides the motivation for the dissertation.

1.2 Motivation

Richardson (2008) has reported that most organisations use firewalls and anti-virus software, and a multitude of other technologies. Even though most organisations use these and other technologies, their information and IT systems remain vulnerable to information security threats. Adding layers and layers of the state-of-the-art information security technologies on top of each other does not necessarily make organisations' information assets any safer, but it increases expenses and introduces complexity, an enemy of security (Hill, 2007; Shin & Williams, 2008 and Geer, 2008). A technological focus alone cannot solve the problem.

Gordon et al. (2006) suggest that information security experts must in addition to their technical know-how be well versed with economics, psychology, sociology, financial and risk management aspects of information security. Several researchers (Gordon et al., 2006; Theoharidou et al., 2005; Pfleeger & Rue, 2008 and RAND 2008) have realised that information security should be viewed as a multidisciplinary field. This requires information security experts to bring in academics, scholars and practitioners of different disciplines. A multidisciplinary approach can provide valuable insights on why organisations are still experiencing information security failures even with the reported increase in information security spending. For example, Fratto (2008) argues that the failure to improve the effectiveness of information security programs is a direct result of the misallocation of the monetary resources for information security.

Soo Hoo (2002) claims that organisations must not over-spend or under-spend on information security, but must spend optimally and cost effectively. Information security is not necessarily about spending more money, but it is about making the right decisions and choices with the given budget. This is a call for information security experts to ensure that information security budgets are optimally allocated and directed on a set of selected controls with the potential to reasonably protect an organisation from its identified risks. Anderson (2002) asserts that if spent

smart a very limited information security budget can still be able to adequately protect organisations' information assets and yield maximum returns. For example, a good information security policy that is sufficiently enforced is relatively cost effective with the potential for a high return on information security investment (Liu, Tanaka & Matsuura, 2007). The increase in information security spending does not necessarily increase the protection of organisational information assets. This dissertation focuses on the allocation of resources to information security and stipulates that it must be done in an optimal and cost-effective manner.

There is a surging need for new research efforts that addresses the issue of optimal and cost-effective allocation of resources to information security activities. This is more critical given the current economic meltdown which is forcing information security decision makers to demand vigilance in expenditures. On that foundation, this research is critical, timely and relevant to the current situation of economic crisis.

1.3 Problem Statement

The core problem to be addressed by this research is:

How to effectively allocate an information security budget to an appropriate set of controls?

Given the current status in the allocation of resources to information security activities, this research aims to assist organisations on how to optimally utilise the limited funds (Werlinger, Haley & Beznoson, 2009) when selecting appropriate information security controls.

To achieve the above, this research investigates the following subsidiary questions:

1. What are the trends in information security? In order to address the issue of optimal spending for information security it is important to first understand the current status and future trends of the information security. The main purpose is to highlight critical information security issues that are being overlooked or not being addressed by research efforts currently undertaken.

2. How much should be invested on information security? Before determining the optimal allocation of monetary resources for different types of controls, it is important to start by investigating existing literature on how much to spend on information security overall?

3. On what types of controls and to what proportions should an information security budget be focused on? This question investigates ways of making informed budget decisions that focuses on a selected set of controls with the potential to protect an organisation's information assets holistically. This also should take cognisance of the variability of organisations such as market sector and business strategy.

The next section discusses the approach taken to address the above research questions.

1.4 Research Methodology

The dissertation begins with a background study and literature survey to set the scene. This is followed by an analysis of current decision making processes in information security management to contextualize it and identify the current trends. The next step is the requirements elicitation and definition for the proposed information security budgeting model. This is followed by the design and development of the model. Finally the proposed model is validated using three different scenarios and through expert reviews.

1.5 Dissertation Layout

This dissertation consists of seven chapters presented in two logic parts i.e. Part 1 and Part 2. Part 1 consists of chapter 1 - 3 and Part 2 consists of chapter 4 – 7.

1.5.1 Part 1: Current State-of-the-art Information Security Management

Chapter 1 provides an introduction to the research problem. This chapter sets the scene of by discussing the background, motivation, research questions and the research methodology. It concludes by providing an overview and structure of the dissertation.

Chapter 2 is a descriptive and analytic evaluation of literature on the past and current information security trends. This is an overview of how information security got to where it is today and what direction is it likely to take in future. The main aim of this chapter is to create awareness of the rapid changing information security threat landscape and the special need to address information security threats by taking a strategic and multi-disciplinary approach.

Chapter 3 provides an overview of the current state-of-art information security management which highlights the potential for applying economic theory in enhancing security managers' decision making process. Hence, information security management is discussed in the context of economics of information security with a specific focus on cost-effective and optimal information security investment. This chapter critically examine existing literature on information security investment models to identify the gaps and short-comings.

1.5.2 Part 2: Advancement beyond the current state-of-the-art

Based on the gaps and short-comings of the existing information security investment models as identified in Chapter 3 and in order to advance the current state of affairs in information security investment; Chapter 4 begins by discussing and defining the requirements for the proposed model. This is followed by the design and development of the model in Chapter 5. The proposed model is validated using a case study (three different scenarios) and expert evaluations in Chapter 6.

Chapter 7 concludes the research undertaken and discusses the extent to which the research problem has been solved. This chapter marks the end of Part 2 and provides the conclusion, contribution and pointers to future work for the overall dissertation. Finally, the list of references

and appendices are included to mark the end of this dissertation. The layout is illustrated in figure 1.1 below.

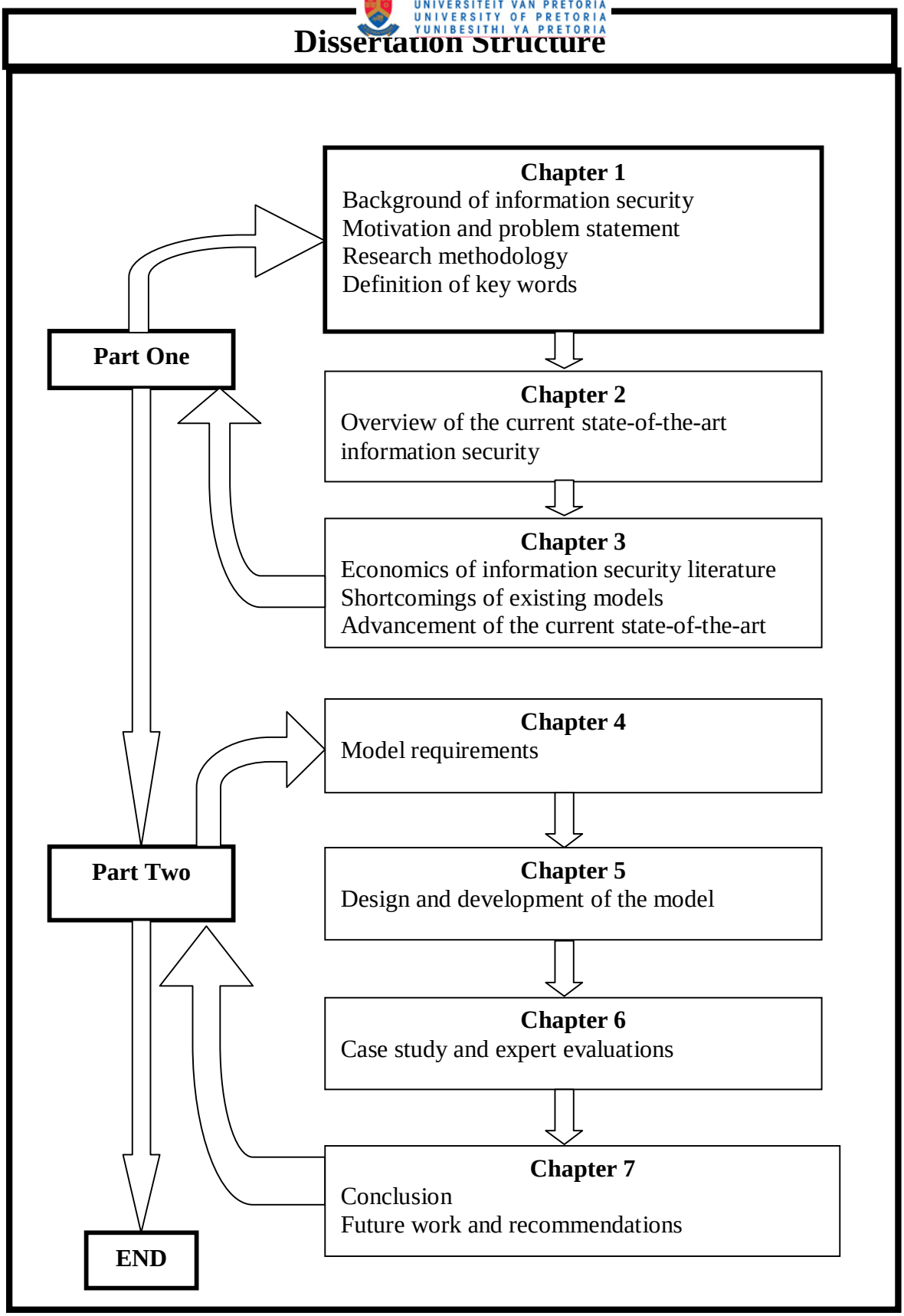


Figure 1.1 Dissertation Structure

1.6 Definition of key words

Information security – is a coordinated and well informed use of physical and logical controls to protect information and information systems in accordance to its sensitivity and impact from the risks of improper use, unauthorized access or transfer, denial of access to authorized users, accidental or deliberate modification, improper disclosure, destruction, disruption, loss, damage and misuse.

Information security management - describes the strategic management of risks to organisational information and information systems in a sensible, optimal and cost effective manner.

Information security control – is an information security measure that reduces, mitigates or eliminates the risk of a threat materialising and becoming an incident.

Broad control category – this is a high level grouping/categorization/classification of information security controls.

Information Security Standard - is a legal document of information security requirements that organisations need to comply with set out by standard bodies or management to assist in protecting information assets.

All the above definitions have been put in the context of the research at hand.

1.7 Conclusion

This chapter has provided an introduction to the overall research. It has discussed the background, motivation (why is this research important?), research questions (what is to be research?) and research methodology (briefly outlined how the envisaged end result is to be achieved). This chapter has also presented a brief overview and the structure of the dissertation. The following chapter (Chapter 2) presents a descriptive and analytic evaluation of literature on the past and current information security trends.

Chapter 2

Overview of the current state-of-the-art information security

2.0 Introduction

As noted in Chapter 1, the overall goal of this research is to investigate how to effectively allocate a budget for information security to an appropriate set of controls. Therefore any attempt in searching for potential solutions would be ineffective without a proper understanding of current state-of-the-art information security in general. The aim of this chapter is to establish the current trends and issues of information security. In order to determine these trends and issues; we investigate the evolution of information security; how it came to be what it is today? The key message is that information security should not be about looking at the past in anger of an attack once faced; neither should it be about looking at the present in fear of being attacked; nor about looking at the future with uncertainty (Dlamini, Eloff & Eloff, 2009).

Organisations and individuals must be alert at all times. They must at all times be aware of past and current trends and issues of information security to be in a better position to predict and prepare for the uncertain future. According to Ormerod (2003), a clear map is useless and almost impossible to navigate if the current position and direction is unclear. Based on Ormerod's assertion, Botha and Gaadingwe (2006) argue that a good understanding of the past and current information security trends and issues can provide valuable indicators of the future of information security.

This chapter is structured as follows: it begins with a brief overview of information security to set the scene. This is followed by a review literature on past security issues. The next section is on the assessment and analysis of information security publications in conjunction with surveys conducted in the information security industry. The next section is a comparison, analysis and discussion of the results carried out to determine the current trends of information security. The following section highlights the critical information security issues that are being overlooked or

not being addressed by research efforts currently undertaken. The last section concludes by recommending new research efforts and highlights the theme of the next chapter.

2.1 Overview

In the early days of computing, information security breaches mainly included viruses and worms that would flash a message or advertisement on the screen without causing any serious damage to the information or IT systems being used. However, rare cases of attacks with the potential to harm information did occur, such as the Friday 13th virus which was set to erase all the information on infected disk drives on a certain Friday 13th late in the 1980s (Denning, 1991).

As times changed, attacks also changed. Since the turn of the century, corporate information assets are at significant risk 24 hours a day, 7 days a week and 52 weeks a year (Lidow and Stahl, 2007). These include risks such as leakage of personal identifiable information, trade secrets, business strategies, the loss of credit and debit card information, the loss of revenue, intellectual capital, intellectual property, brand value, image, reputation and market share (Humphreys et al. 2006).

Unlike in the past, information security has evolved from addressing minor and harmless risks to managing those (stated above) with a major impact on organisations' reputation, profitability, customer confidence and overall economic growth (Romer & White 2006). These risks have the potential to go as far as threatening the existence of organisations and can attract huge penalties from the relevant regulatory or legal bodies. Cybertrust (2005) argue that this problem is two-fold: firstly it is due to the increase in economic and political uncertainty and secondly to the pressure from consumers and regulatory bodies.

As an example, a security breach such as the leakage of credit card information can imply an enormous damage to card payment companies due to the cancellation and re-issuing of compromised cards. This could also cost millions of dollars in penalties to regulatory compliance

bodies. In 2007, the case of a gang of Europeans who cloned 32 000 credit cards worth £17 million was reported in the Computer Fraud & Security News (2007) as the biggest (yet) uncovered credit card fraud. Between 2006 and 2008, three hackers stole over 130 million credit and debit card numbers from five corporate companies in the United State (Marra, 2009). This is just a glimpse of losses related to today's information security threats.

It is therefore very important for companies to notice that their strength in attaining and sustaining competitiveness in the highly volatile, demanding and uncertain markets lies in their ability to securely protect their information assets and IT infrastructure. For this reason information security has become a lingua franca not only to the world of computing, but also to various other industries. Multiple workshops and conferences have surfaced recently with the sole aim of discussing information security issues beyond technologies.

Does this mean information security is a new field or just another "fad"? No, information security is neither new nor a "fad". What is new, is its broader focus and wider appeal. For a long time most organisations would not recognise the importance of securing the infrastructure that holds and transmits their strategic information. Information security has been treated as a by-product, if not as a "necessary evil that hinders productivity" (Conray-Murray, 2003). Organisations would do it merely because everybody else is doing it. However, slowly but surely information security is getting into the forefront of things, and has been promoted from a by-product to an integral part of business operations (Conner & Coviello, 2004). It is therefore important to consider how exactly did information security get to the current situation? Accomplishing the last mentioned is not possible without considering the past of information security.

2.2 The Past of Information Security

Information security came into existence even before the invention of a computer. Rusell and Gangemi (1991) argue that information security is as old as information itself. From the time when information began to be transmitted, stored and processed, it required protection. This

dates back to the time when human beings first learned how to write. Denning (1999) takes us back to the first century when Julius Caesar devised a secret code to protect messages sent to his friends from being intercepted, i.e. protecting the confidentiality of the message.

In the 1840s when the telegraph was invented (Rusell & Gangeni, 1991), an encryption code was developed to safeguard the secrecy of the transmitted telegrams. This was followed by the invention of the telephone and a year later legislation prohibiting wiretapping was put in place. Information security has moved from protecting the secrecy of hand written messages to telegrams, to telephone conversations and later to the world of computing. Information security originated with a main concern of protecting the secrecy or confidentiality of transmitted data and information.

2.2.1 The 1940s to the 1950s

The 1940s up to the 1950s marked the dawn of computing, when the first-generation computers came into existence. This was followed by the era of mainframe computers when only a few operators were permitted to use these computers. Other users would submit their jobs to the operator through protected slots (batch processing). The key information security issue during this era was ensuring that only the privileged computer operator (one user one computer) would have access and that the physical computer was not stolen or damaged by outsiders. The scope of security gradually increased from the protection of the confidentiality of information, to safeguarding the information infrastructure (mainframe computers) that processed the information and storage media. Physical security was the basic principle underlying all security of computer systems.

Mainframe computers were isolated stand-alone units and networks were non-existent back then. Human messengers or physical mail was used to transfer programs and their data between computers. The only threat related to the transmission of information was that storage media could be lost or stolen. Even though it would take days to get information or data to its destination, data was safe.

2.2.2 The 1960s to 1970s

The late 1960s until the early 1970s mark the beginning of dumb terminals. These enabled users (multiple users - one computer) to access and use remote data. This innovation introduced a new risk to remotely held data. Data could be accessed by unauthorized people or outsiders. Elementary physical security could not deal with this new risk. Therefore user identification and authentication came into play in the early 1970s. Physical access to terminals was screened by a security officer before the user could start the identification and authentication process. Since there were few terminals it was easy to keep track of all logged-in users and their activities.

However, since there were no information security policies in place to enforce the use of strong passwords, password cracking was a big threat at this time. Password sharing posed another major problem. Guest and anonymous logins were still acceptable, as outsiders without much identification and authentication could access only limited resources inside the network.

The era of dumb terminals was succeeded by that of mini computers. The introduction of mini computers marked the beginning of networks, time-sharing and multi-user systems which further changed the rules of the game. The number of people with computer know-how increased with the drop in prices of modems and terminals. Access controls were introduced to prevent users from interfering with one another's workspace. The work of Harrison, Ruzzo and Ullman (the HRU model) was the pioneer of access controls. This was followed by the Bell-LaPadula confidentiality model for Multics (Pfleeger & Pfleeger, 2007) and digital signatures from around the late 1970s to early 1980s. The Biba Integrity model was introduced and built on the Bell-LaPadula model (Sural, 2006). Over and above confidentiality, the concern for integrity came on-board.

Also in the early 1970s public key cryptography came into existence. The Data Encryption Standard (DES) (Brown, Good & Prabhakar, 1993) was adopted by the then National Bureau of Standards (NBS) of USA, which is now called the National Institute of Standards and Technology (NIST). This is around the same time that the ARPANET began, aimed at providing a reliable and robust network to ensure the availability of computer systems (Denning, 1999).

This innovation introduced a new dimension for the protection of information, and the goal posts were again moved. In response, the US government passed the Privacy Act of 1974 to safeguard personal information recorded in government systems (Rusell & Gangemi, 1991).

2.2.3 The 1980s to 1990s

The 1980s marked the introduction of personal computers and suddenly every user had their own computer (Rusell & Gangemi, 1991). Again the number of people with computer know-how increased. Companies began to automate their operations and new information security threats emerged as critical corporate data was now stored on easily accessible secondary storage. The scope of information security further widened. Hence, the 414 gang, the intruder (Markus Hess) who broke into computers at Stanford campus in the USA and the West German programmer who broke into the US military computers to steal documents were reported to be among the first intruder break-ins (Denning, 1991; Stoll, 2000).

This decade marked the rise of computer viruses, which spread through the use of diskettes. Denning (1991) reported viruses called “Elk Cloner” and “The Brain” to be among the first viruses ever created. The former was created by Rick Skrenta, targeting Apple II disks, and would display a poem on the screen. The latter flashed an advertisement for a Pakistani company and is believed to have been the work of two Pakistani brothers. Denning (1991) also cited Robert Morris to have created the first worm in 1988, arguing that even though it was harmless, it produced a massive scare. These were just a minor annoyance to the user but did not really do any harm to the information stored or processed, or to the infrastructure. Microsoft Windows and Local Area Networks (LANs) emerged in this decade.

The USA government issued the Computer Fraud and Abuse Act of 1984 to prosecute and establish harsh penalties for offenders (creators and authors of computer viruses). This Act came into practice following the conviction of Robert Morris, author of the first Internet worm (Russell & Gangemi, 1991; Denning, 1991; Denning, 1999). It was followed by the Computer Security Act of 1987, also from the USA, which dealt with the training of security personnel involved in the processing of sensitive information.

The late 1980s also saw the introduction of anti-virus software. Carey (2008) argues that the European Bernt Fix in 1987 created the first ever anti-virus. Carey also asserts that in 1988, Alan Solomon, of Great Brittan released an anti-virus software called Dr. Solomon's Anti-Virus Toolkit.

2.2.4 The 1990s

What was conceived in the late 1960s and born in the early 1970s as the ARPANET grew in the 1990s as LANs and WANs merged in distributed systems. Dlamini et al. (2009) argues that the 1990s was dominated by open systems and mobile computing. More and more personal computers connected to the Internet. This innovation brought new risks, as would be expected since open systems would also be open to abuse (Denning, 1991). The hacking community created freely available hacking tools, and hence virus and worm attacks intensified and script kiddies started showing their faces. Anti-virus products were a prime solution.

Carey (2008) claim that by the end of 1990, there were approximately nineteen anti-virus software environments including Symantec's Norton anti-virus, ViruScan by McAfee; and IBM's anti-virus. However, there are conflicting views as Pearson Education (2007) claim that Norton and ViruScan were among the first anti-virus environments created to combat viruses and worms.

Towards the end of the 1990s attackers changed from using worms and viruses to more sophisticated attacks. The introduction of distributed denial of service and malicious code attached to business emails and web pages shifted the focus to the gateways. This saw the introduction of filtering firewalls. Perimeter security came into existence to provide a wall around networks and keep out the outsiders. But as the use of the Internet intensified, network boundaries disappeared and perimeter security vanished.

2.2.5 The 21st century

As we entered the 21st century, things changed. Attackers started hacking for financial gains and not just to show-cast their skills. IT infrastructure became pervasive in almost all industries (known as the era of pervasive computing). Every second word now began with an E, for example E-commerce, E-voting, E-business, E-government, etc., because everything had gone electronic. As all sorts of devices came on-board (Personal Digital Assistants, Smart phones, Laptops, Notebooks, Tablet PCs, etc.), it became difficult to clearly define a computer. Mobile computing (Bluetooth and Wi-Fi) also emerged to complicate things even further. Online payment systems and the usage of credit cards became highly popular and web-based applications intensified. However, the fact remains that all these new developments in technology were vulnerable and like all other good things came with side effects (risks).

2.3 Information Security – a current perspective

The 21st century innovations and developments came along with a strong dependency on IT infrastructure. This opened new and attractive doors for the hacking community. Attackers have evolved from computer enthusiasts to professional hackers (Gelbstein, 2006). Bruce Schneier, quoted in Anderson (in press), argues that “it is only amateurs who still target machines; career criminals now target people who operate them, not just for fun, but for financial gains”. Attackers have matured from using hacking skills to showing that they can circumvent the authentication process to access each other's files to use them in the theft of confidential information. This has resulted in information security threats like identity theft, social engineering, phishing, etc which can easily compromise authentication and authorization credentials. Nowadays the motive of an attacker is financial gains and in order to evade the “long arm of law”, he or she will do everything to cover his or her tracks. As a solution and in addition to the authorization and authentication credentials, verification of users became necessary for access. Banks introduced chip-and-pin. Non-repudiation has since become a critical issue of the 21st century.

Viruses and worms have evolved from minor annoyances to having catastrophic impacts and can infect thousands of machines in seconds (Zetter, 2003; Petreley, 2004). Creators of these threats have opted for a new twist on an old trick (MacMillan, 2008). Simple attacks have matured to become sophisticated, automatic, subtle and very hard to detect (Schneier, 2003; Carey, 2008; Ioannidis, Markatos and Kruegel, 2009). There is also the evolution of spam and phishing from email to SMS (short message service) and MMS (multimedia message service) technology in mobile phones (Symantec Internet Security Threat Report, 2007). Attackers are on the verge of re-inventing the wheel. They use old tricks in new twisted ways (MacMillan, 2008) and therefore the history of information security is as critical as the uncertain road ahead.

The future of information security remains clouded with numerous uncertainties. However, two things remain certain – IT infrastructures are vulnerable and motivated attackers are always ready to exploit these vulnerabilities. It is therefore critical that securing information and its IT infrastructure should not be considered with the fear of inevitable attacks, but in preparedness for the uncertain future threats. This requires innovative ideas and insightful analysis of information security issues to appropriately respond to the challenges posed by new developments. Another challenge is that as information security moves to respond to new threats in current and future environments, it must also protect against well-known threats. The goal posts are not only moving, but they also widen each time, making it very difficult to protect information and its infrastructure.

2.3.1 Identification of the Current Information Security Trends

Despite several studies aimed at providing much needed statistical information on information security trends and issues, there is still an urgent need to find one that is complete and reliable. CSIA (Cyber Security Industry Alliance) (CSIA, 2007) compiled a list of disparate sources of information and statistics related to information security issues and their trends. This includes an overview of the work of Symantec, Sophos, Deloitte global security survey, Ernst & Young global information security survey, CSI/FBI computer crime and security survey, SANS institute, etc. However, most of these target the US and UK communities and very few have the world community as their target. Information security experts can gain a good understanding of

the current information security trends and issues by using the results of the above surveys. It is unfortunate that there is still (to the author's knowledge) no work that pays attention to the aggregation of the above surveys to get a holistic picture of the global information security landscape.

To further develop a good understanding of the current information security landscape, this chapter outlines the following two phases:

- Phase 1 monitored, assessed and analysed articles covered in the following four journals: Computer & Security, Computer Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security. The main aim is to identify the critical issues currently being addressed by information security professionals to gain a complete picture of today's information security posture. The survey is based on publications for the years 2005 until December 2006. The question can be asked why these four journals? There are many journals and publications available today which focus on information security related issues. However, the authors of this chapter wanted to include journals that represent both an academic (Computers & Security, IEEE Security & Privacy, Information Management & Computer Security) as well as a business (Computer Fraud & Security) view on the matter. Furthermore, because the author wanted to focus on identifying trends it was important to include journals that are well established and have been available for a long enough time e.g. Computers & Security. It was also decided to only include journals that have information security as its primary focus.

Phase 2 made an analysis of the 2006 report issued by the Computer Security Institute/Federal Bureau Investigations (CSI/FBI) (2006) on computer crime and security (Gordon et al 2006) as well as the SANS Institute (2006) report. The reasons for including surveys conducted by these two institutes are as follows: both institutes have delivered for many years a service to the information security community in the large; they both provide a wealth of security related content free to the public; both institutes have extensive research archives. It is important to acknowledge and discuss a priori the limitations of our approach. The next section is an outline for the limitations.

2.3.2 Limitations

Phase 1

All the publications under investigation above seem to be more common in university libraries than in chief security officers' offices. Hence, it is unlikely that this approach will capture the true picture of the current information security landscape. Whilst the publications to a lesser extent reflect current research, they do not really reflect on the breaking information security issues faced by information security practitioners. This is because the publications go through a long peer review process which adds a long time lag to the publication route and hence, they tend to rather deal with long term issues than short-term issues. The publications seem to focus more on full papers than the small section on breaking information security issues. As a result they are not so responsive to the current information security trends and issues. Hence, they tend to be a following rather than a leading indicator of information security trends. However, the publications are published almost monthly and contain articles written and reviewed by experts in the information security field which makes them relevant. They also to a certain extent reflect the latest developments in the information security field. Although these four publications do not at all represent the whole spectrum of information security publications, the authors believe that assessing them can provide valuable insights into the current state and trends of information security.

Phase 2

The SANS Institute and CSI/FBI reports are both based on survey respondents. There are several drawbacks in such surveys which involve survey respondents, more especially information security experts. Firstly, survey respondents tend to be biased when reporting information security breaches in fear of the consequences of legal liability, and of damaging customer confidence and company reputation. Organisations usually do not report or reveal exact security breaches as they occurred (Eppel, 2005). Secondly, criminals hide their successful attacks which makes some information security breaches go undetected and never accounted for in such survey

results. Thirdly and final, vendors exaggerate the risk to market their products (Eppel, 2005). Hence, CSIA (2007) argues that surveys may provide valuable insights but there are doubts about their authenticity, correctness and completeness.

It is therefore very difficult to get a true and comprehensive view of the current state of information security based on the results of such surveys. However, to remove such doubts the results from the survey respondents will be aggregated with those of Phase 1 to help in developing a holistic picture of the current security trends and issues. This includes a survey on information security journals as well as the analysis of The SANS Institute and CSI/FBI security reports in order to determine current information security trends.

2.3.3 Data Collection

This section investigates the computer and information security issues found in the Computers & Security, Computer Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security publications for the year 2005 and 2006.

2.3.3.1 Topics Covered in the Journals (Phase 1)

The data collection process started with a brainstorming session where all sorts of information security related topics were identified. These were then grouped into broad topic categories to accommodate most of the topics identified in the brainstorming sessions. For example, every topic that dealt with surveillance cameras, fences, security guards and the likes were grouped as ***physical security***. Information security budgets, spending, culture, behaviour and anything that pertains to the management of information security were categorized as ***information security management***. The same strategy applies to all the other broad topics. All the topics that appear not to be part of any of the broad topics were categorized as ***other***. This category included topics like: security outsourcing; critical infrastructures; anonymous protocols and end user security to name just a few.

Even with this general option ***other***, there are certain limitations of the study as some topics could sometimes fit into more than one broad category. For example, the case of digital forensics and legal issues often overlap. To correctly categorise such issues, the abstract and keywords of an article would be read to determine its key theme. If still unclear, the conclusion would be consulted. The same technique applies for topics that are unclear or ambiguous. What must be noted though is that the categorisation used in this study does not represent a standard scientific categorisation, but solely the views and opinions of the authors.

2.3.3.2 Results obtained from the journals

This sub-subsection outlines the profile of articles published in all four publications over the period investigated. Some of the publications (i.e. Computers & Security and Computer Fraud & Security) contain a section on brief news or short discussions that would otherwise not qualify to be called full articles. These are also included in the survey results because they provide qualitative information about current security issues. Figure 2.1 summarises the amount of coverage given to each topic by all the journals included for this survey.

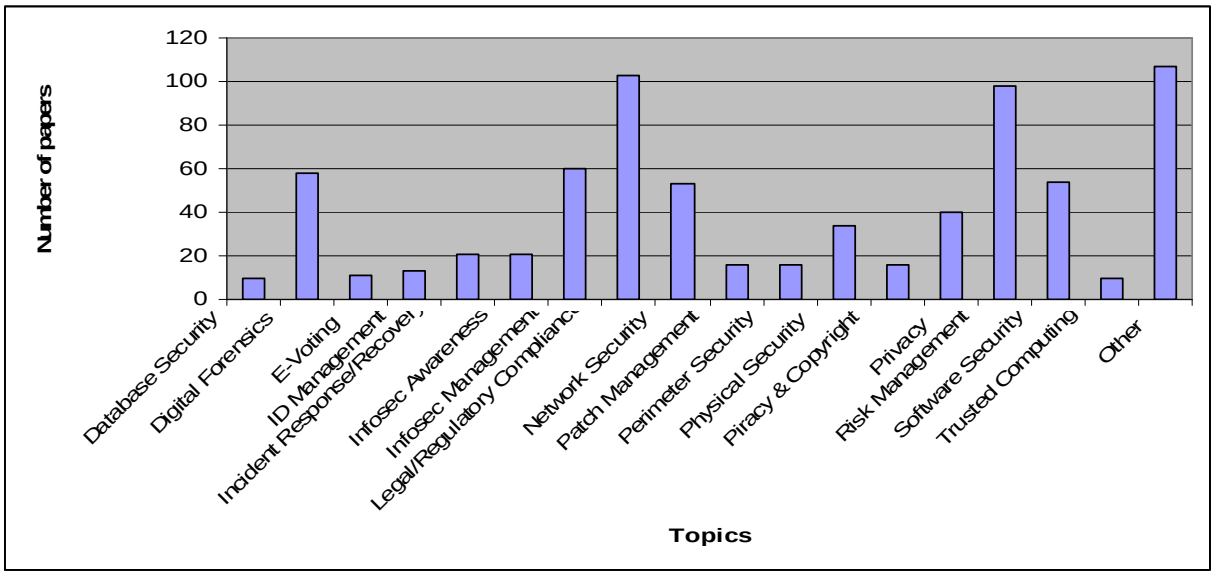


Figure 2.1: Importance of topics across all journals

When investigating each of the journals separately, it is interesting to note that different topics were emphasized by each journal.

Table 2.1 lists the top five topics in each of the journals in priority order with 1 being the most published topic for that specific journal.

Table 2.1: The Top Five in all the publications

	Computer Fraud & Security	**Computers & Security**	**IEEE Security & Privacy**	**Information Management & Computer Security**
Digital Forensics	3 (23)	2 (30)		
ID Management				5 (3)
Information Security Awareness			5 (9)	
Information Security Management		5 (14)	4 (23)	1 (12)
Legal & Regulatory Compliance	2 (40)	1 (56)		5 (3)
Network Security	4 (21)		4 (23)	4 (4)
Other		3 (27)	1 (41)	2 (11)
Perimeter Security				3 (5)
Physical Security	5 (20)			
Privacy			3 (28)	4 (4)
Risk Management	1 (67)	4 (22)		3 (5)
Software Security			2 (35)	3 (5)

Outstanding in the results of the Computers Fraud & Security publication is that risk management took the lead with 67 articles, followed by legal and compliance regulatory issues at 40, digital forensics at 23, network security at 21 and physical security at 20 to constitute the top five.

In the Computers & Security publication, articles on legal and regulatory compliance issues were more than all the other categories at 56, followed by digital forensics at 30, other at 27, risk

management at 22 and information security management at 14 closing the top five most discussed topics.

The IEEE Security & Privacy publication focused on amongst others on software security with 35, privacy at 28, then network security and information security management are tied at 23 and information security awareness at nine.

Lastly in the Information Management & Computer Security publication information security management took the lead at 12, with *other* at 11, followed by risk management, perimeter security and software security tied at five, then network security and privacy tied at four and in the fifth place legal and regulatory compliance and identity management at three.

2.3.4 Surveys of the CSI/FBI and SANS reports (Phase 2)

In this subsection the study considers two well established surveys that had been gathering statistics and trends on information security for many years. These are the CSI/FBI computer crime and security survey and the SAN institute survey. However, the focus is only on the 2006 results.

The CSI/FBI survey has been gathering information security statistics for the past 12 years and they have developed significant experience in the field. Their results are based on the answers of survey respondents, which mainly consist of security practitioners from almost all industrial sectors in the United States. The US respondents' answers may not represent the true picture of information security worldwide, but they do provide valuable insights. The CSI/FBI (2006) data on the most critical security issues for 2007 and 2008 is used by the authors to compile a graph as shown in *Figure 2.2*.

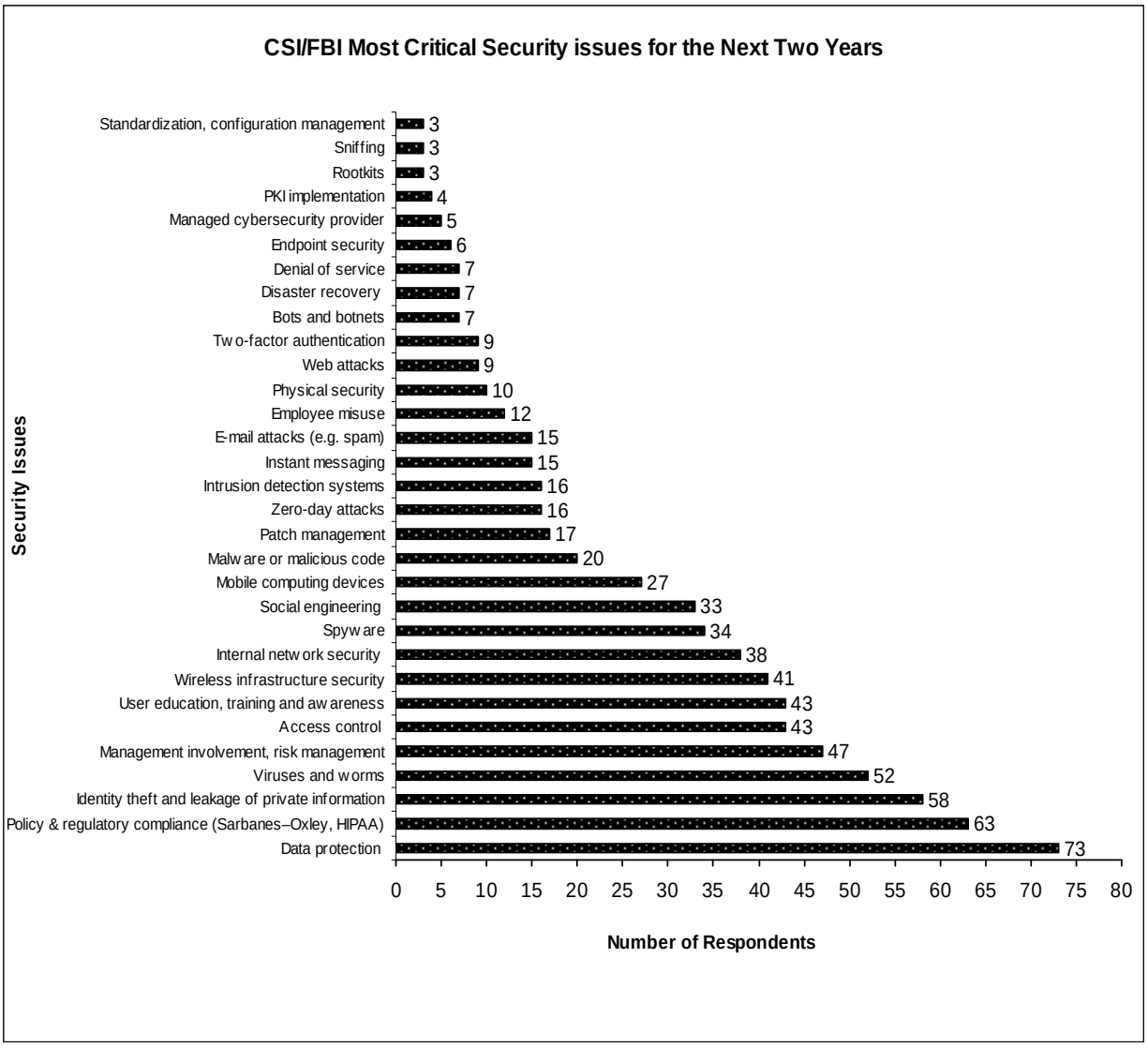


Figure 2.2: Graph drawn from statistics/data provided by CSI/FBI (2006) (Gordon et al, 2006)

The SANS Institute (2006) report is based on twenty most respected leaders in cyber-security who developed a list of ten most important trends in predicting the future of information security. Unlike the CSI/FBI, the SAN report is a good representation of the worldwide situation of information security because it involves not only the US security practitioners but cyber-security leaders from all over the world. The top five issues in both reports are summarised in the following table in ascending order.

Table 2.2: The top five issues of both security surveys

CSI/FBI computer crime survey	SANS Institute Survey
1. Data Protection	1. Laptop or mobile hardware devices encryption
2. Policy and regulatory Compliance	2. Significant growth in theft of PDA smart phones
3. Identity theft and Leakage of private information	3. More legislation governing the protection of customer information
4. Worms and viruses	4. Increase in targeted attacks
5. Management involvement and risk management	5. Increase in cell phone worms

Table 2.2 shows data protection at the top of the CSI/FBI survey, followed closely by policy and regulatory compliance and placed third is identity theft and leakage of private information. These are the three hot topics which are so critical to information security. The issue of worms and viruses is no longer like it was in the early 1990s. This is because cyber criminals are now targeting and stealing information such as credit and debit card numbers, trade secrets and personal identifiable information for financial gains. The issue of risk management is slowly moving up the list of security priorities.

On the other end of table 2.2, the SANS Institute survey reports encryption of mobile devices as a primary concern, followed by the issue of growing theft of smart phones, and then the legislation for the protection of customer information to prevent identity theft and related threats. Perched third is the growing number of targeted attacks and the invasion of cell phones by viruses and worms rightly so because of the converging networks and the capacity of smart phones. More discussion on these and other results follows in next subsection.

2.3.5 Discussion and Analysis of Results

This section compares and discusses the results of the publications survey with the CSI/FBI and SAN 2006 reports on the future information security predictions. Notable in the findings is that most of the publications are written by security experts for the computer and information security community. Hence, one would expect to find most of the articles on database security, physical

security and many other technical issues directly related to security technologies. However, this is not the case. Does this mean information security has changed?

No, information security has not changed per se, but it has since gained a broader and wider focus. This has caused information security experts to change their focus too. From the early days of computing, information security has been put in the hands of security experts, but of late things are changing - as are clear from the results.

2.3.5.1 The Most Prominent Topics

The results show a strong emphasis on three aspects: legal and regulatory compliance, risk management and information security management. This indicates that the information security responsibility is widening to also include risk managers, forensic specialists, compliance regulators and other stakeholders. This involves a major shift from pure reactive technical measures towards a more proactive strategic approach (Volker, 2007). Also in support of the study findings are the predictions of the CSI/FBI (2006) report which points towards a strategic approach.

- **Legal and Regulatory Compliance -** The survey reveals that the Computers & Security publication put most emphasis on legal and regulatory compliance. In comparison to the others, legal and regulatory compliance is ranked second in the Computer Fraud & Security publication, third in the SANS institute (2006) report, second in the CSI/FBI (2006) report and fifth in Information Management & Computer Security. Data protection, which is ranked first in the CSI/FBI report, also falls in this category. This shows that computer crime authorities around the world are working hard to find solutions for combating the rise in cyber-crime (Sophos, 2007).

- **Regulatory compliance** goes hand in hand with legal issues as it ensures that standards are implemented and adhered to. Its main objective is to assess whether organisations have enough controls, are doing the right things, and are doing the right things the right way (Gelbestein, 2006). Regulatory compliance authorities enforce control by ensuring

that organisations that do not comply with set standards face penalties and legal consequences and those that do, are awarded certificates in recognition. In as much as regulatory compliance enforces the use of appropriate security controls, its main target are the human factor of security.

- **Risk Management** - The Computer Fraud & Security publication results show a main emphasis on risk management, which is ranked fourth in Computers & Security, fifth in the CSI/FBI (2006) report, third in Information Management & Computer Security and does not appear on the top five list of SANS Institute's (2006) report and the IEEE Security & Privacy publication. Information security experts are beginning to see the bigger picture. This is an indication that the debate is moving from an operational and tactical level towards a strategic level of risk management. However, this does not necessarily mean that the technical paradigm no longer has a role in information security.

Today's information security threats are forcing organisations to become more adaptable and flexible with regards to the people, process and technology risks. It is through such risks that information security is a standard item on the agenda of senior management's meetings nowadays.

- **Information Security Management** - The survey results further show that information security management is another focus area in the information security press. This topic is ranked first in Information Management & Computer Security, third in IEEE Security & Privacy, fifth in Computers & Security and CSI/FBI (2006). However, it is not a high priority in the other publications. This could be due to several biases that could be as a result of the audience and the focus of the publications. Information security management is a critical factor to get information security issues discussed in board rooms. Furthermore, information security management is a means to a strategic information security approach.

- **Network Security** - The survey results also show network security as another topic that has received attention in the information security press. It is ranked fourth in Computer

Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security publications. This issue is just as important nowadays as it has ever been as networks are converging with their inherent risks. It is therefore very critical for the information security experts to address network security issues. Again this is an indication that technical issues are still applicable in the current and future information security landscape.

- **Digital Forensics** - The other issue of concern in the information security press is digital forensics; a critical issue ranked third in the Computer Fraud & Security, second in the Computers & Security. However, it does not appear in the other two publications, CSI/FBI and the SAN top five. Digital forensics connects the law and information security. It ensures that evidence collected on the crime scene gets to the courts in an unhampered or uncontaminated state to facilitate the apprehension of criminals. However, such initiatives are undermined by inappropriate penalties stipulated in current laws. Hence, many computer crime perpetrators have been given inordinately light sentences for serious crimes. For example, the UK's Information Commissioner (2006) reports that between 2002 and 2006, only two out of 22 cases resulted to penalties amounting to only about £5000. A call has since been made to raise cyber crime penalties (Information Commissioner, 2006) and to increase the coordination between information security, digital forensics, government and law enforcements in order to best track and convict cyber criminals.

- **Identity Theft and Leakage of Private Information** - Ranked third in the CSI/FBI (2006) report is the issue of identity theft and the leakage of private information. Directly linked to identity theft and leakage of private information is privacy which is ranked third in IEEE Security & Privacy and Information Management & Computer Security. It is encouraging to see these issues being on the top five list of information security issues being discussed. More so after Gunter Ollmann (cited in the editorial news section of Computer Fraud & Security, 2007), reported that in the underground identities are selling for much more than credit card numbers. This is another critical area that security practitioners need to look at in order to address current and future threats.

- **Software Security** - Software security is ranked second in IEEE Security & Privacy and third in Information Management & Computer Security but not covered in the other publications. Software security is a major issue that underlies insecure systems. The expectation would be to have more publications addressing software security.

- **Theft of mobile devices** - The theft of laptops, smart phones, personal digital assistants (PDAs) and other mobile devices is on the rise (SAN, 2006). However, what attract most thieves are not just the devices per se but the data held in them. It is therefore no coincidence that the issue of laptop or mobile hardware encryption is at the top of the five most important security trends of the report by the SANS Institute (2006). This is an effort to ensure that even if such devices get stolen, the critical and valuable data they hold will not be compromised. Moreover, the SANS institute reported legislation governing the protection of such data or information to ensure that organisations that lose or compromise such data would face legal consequences. Data protection, which is ranked first in the CSI/FBI report, also supports the SAN institute's findings. Preserving privacy, preventing identity theft and leakage of private information is critical nowadays.

- **Targeted Attacks** - Furthermore, the SANS report predicts an increase in targeted attacks and cell phone worms. The former is concerned with purposeful attacks mainly driven by financial motives. The latter shows that the target is moving towards new environments as it spreads to exploit cellular networks. The CSI/FBI (2006) report shows that worms and viruses will continue to be a big threat to information systems in the next few years. These threats are finding new exploits to infect and they are becoming increasingly sophisticated and thus hard to detect. Such threats cause the scope of information security to continue widening.

2.3.5.2 Less Significant Topics

Physical security, information security awareness, identity management and perimeter security are also in the top five topics discussed even though not extensively. These are the issues that security experts are expected to be more concerned with. However, this is unfortunately not the case.

These research results show the current direction of information security. It is clear that information security research is moving towards a strategic approach. However, this is not a complete switch as technical measures remain applicable. The end result is that information security's focus is widening and deepening.

2.4. The direction for this dissertation

To summarise the findings, the following two aspects are important for this research project.

- Firstly, the current information security landscape is moving towards a more strategic approach also referred to as Information Security Governance and
- Secondly, information security has emerged as a paradigm that requires a multidisciplinary approach within and across the silos of business, science and social sciences.

Revisiting the overall goal of this research as re-stated at the beginning of this chapter; the direction that this research seeks to take based on the current state of the art which is deduced from results of the surveys more specifically the above two is as follows:

- **A strategic approach**: The dissertation focuses on information security management as one of means towards a strategic approach. Information security management is one of the topics that were identified as most prominent in the journals survey, more especially in the Information Management & Computer Security journal. There is more work that needs to be done under this topic to ensure the information security governance approach. This research builds on information security management by taking a close look at the cost effectiveness of

investments in information security activities and how it can contribute to the strategic information security knowledge domain.

- **A multidisciplinary approach**: The current state of the art has revealed a shift towards new insights on how to integrate theory and principles from other disciples to achieve the strategic information security. In taking that direction, this research focuses on applying the principles and theory of the field of economics to information security at the strategic management level. The main aim is to integrate the fields of economics and information security in a bid to adequately allocate resources to information security activities as part of the overall goal of this research.

- **A legal and regulatory compliance approach:** the survey results have also shown that legal and regulatory mandates form part of the current and most prominent discussions in the information security arena. Therefore, it is very important that the move towards the strategic and multidisciplinary approach should also ensure adherence and compliance to the legal and regulatory mandates.

2.5 Conclusion

The threat landscape has also changed drastically, from fame-driven and harmless attacks to more financial motivated and targeted ones. The results of the survey show that today's attacks target the human beings more than the information systems. Hence, most of today's information security challenges are to a greater extent related to the human and organisational aspects of security and not so much to the pure technologies.

This chapter has revealed the past and current information security trends and issues. What remains is to make concrete suggestions and to identify possible solutions. There is a surging need for new research strategies to address the new challenges. New research efforts are required to minimise the gap between regulatory issues and technical implementations.

Chapter 3

Literature Review – Information security investment

3.0 Introduction

In order to contribute to the main goal of this research i.e. investigate on how to effectively and optimally allocate limited funds to information security activities; the previous chapter has laid the foundation by identifying the current information security trends. Firstly, the trends revealed that information security is moving towards a strategic governance approach. Secondly, the trends revealed that information security requires a multidisciplinary approach. On the basis of the findings of the previous chapter and as part of addressing the overall goal of this research; this dissertation focuses further on the economics of information security.

Therefore, this chapter provides a review of literature on the current state-of-the-art economics of information security investment in order to identify and acknowledge existing work in the field and gaps to build on. This chapter is structured as follows: Section 3.1 discusses the motivation for choosing the economics of information security. Section 3.2 gives a brief overview of the economics of information security to highlight some of the issues that are being discussed in this field. The next section i.e. Section 3.3 delves in to discuss more details of an information security investment. This is followed by a discussion on the short-comings identified in the reviewed literature in section 3.4. Section 3.5 concludes the chapter.

3.1 Why Economics of Information Security?

Given the on-going economic crisis and possible recession, today's organisations must implement a well structured information security program that will minimise and mitigate the overall business risk with a minimum budget. Organisations are called onto scrutinise their spending; become more conservative and vigilant; more so on overheads such as information

security expenditure which are the first to feel the pressures and effects of cost cutting measures (Heiser, 2009; Researchandmarkets, 2007; Timms, 2004; Tipton & Krause, 2003).

The current economic situation comes with changing priorities. Information security risks that were once considered unacceptable become acceptable as organisations shrink their budgets to improve their revenue. Heiser (2009) argues that information security managers will be marginalised if they overestimate or underestimate the risks in comparison to other financial and market risks. Heiser further argues that those who cannot demonstrate the business benefit of investing on information security should anticipate huge budget cuts.

Furthermore and sadly so, within the on-going global economic turmoil and developments in information security, a recent survey conducted by Symantec has reported in 2008 that the global underground economy is booming at millions of dollars in advertised goods and services (Symantec, 2008; Ko, 2008). While the whole world is in the worst economic crisis, the underground economy continues to flourish. As a result organisations, governments, private and public sector and individuals are losing large amounts of money to the "bad guys" apart from the losses due to the deteriorating global economic markets.

Melek (2009) and Chapman (2009) argue that the current economic crisis is continually increasing the risk to information assets. More so with the thousands of job losses and cost cutting measures that are reported on almost a daily basis, disgruntled employees resort to malicious activities to supplement their shrinking salaries and job losses.

Despite all the years of hard work on information security technology improvements, harsh compliance regulatory penalties and more coordinated law enforcements, information security breaches are still ubiquitous, likely to increase because of the economic turmoil and have seriously damaging consequences (Grossklags, Chuang & Christin, 2008; Fumey-Nassah, 2007; Schneier, 2002). Clearly something is not working effectively in the information security arena.

Are the organisations putting in enough effort to protect their information assets or are they not taking any precautions? In case where there are protection measures in place; how much are

organisations actually spending on information security? Is it less or just enough or more? How much is really enough? A technical approach has little or nothing to offer in this regard.

These questions require a strategic approach to information security that is in-line with the overall business strategy, one which van Kessel (2008) argues organisations are struggling to achieve. These issues can be best dealt with at the information security management level, mainly because decision makers at this level are still struggling to quantify information security investments in terms of (direct and indirect) costs and benefits, the likelihood of risk and potential loss among other things. This has heightened the need for a new perspective on applying sound economic principles when evaluating information security investments and designing adequate programs for the complex domain of securing information assets (Gibbs, 2009; Anderson, 2008; Anderson & Moore, 2007; Anderson, 2001).

Cavusoglu, Cavusoglu and Raghunathan (2005), and Anderson (2001), cited in Liu, Tanaka and Matsuura (2007) states that information security managers and other decision makers are changing their focus from technical viable solutions towards economical viable ones in a bid to take a strategic approach to information security. In order to strengthen and build on current research, the focus of this dissertation is on applying economics principles in the allocation of budgets to information security activities at the strategic level.

In summary, the economic crisis and the flourishing underground economy have heightened the need for organisations to achieve more with less. Organisations are required to optimally and cost-effectively utilize shrinking budgets to implement a well structured information security plan that will greatly mitigate business information risks. A new dimension has been added to information security. Information security solutions are now to be chosen not only because of their technical feasibility but most importantly because of their economic viability. It is therefore very important to consider the field of the economics of information security. For this reason the next section discusses an overview of the economics of information security.

3.2 An Overview of the Economics of Information Security

The work of Catherine Wolfram, Dan Geer, Larry Gordon and Martin Loeb in 2001 laid a solid foundation for the field of economics of information security (Willemson, 2006). A year later, the Workshop on the Economics of Information Security (WEIS) was held for the first time at the University of California-Berkeley, spearheaded by Ross Anderson and Hal Varian. Since then the economics of information security has become an important field of study (Tsiakis & Stephanides, 2005; Huang, Hu and Behara, 2006; Anderson & Moore, 2006; Anderson & Moore, 2007).

This fast-growing field embraces a multidisciplinary approach towards addressing information security failures. It brings together scholars, practitioners and academics from various disciplines to discuss and address the economic challenges, trade-offs, opportunities and incentives of information security. For the past seven year researchers have identified several topics of interest such as the **economics of vulnerability disclosure** (Ozment, 2004; Kannan & Telang, 2004; Cavusoglu et al., 2005; Anderson & Moore, 2006; Johnson & Dynes, 2007; Choi Fershtman & Gandal, 2007; Miller, 2007; Zhao , Chen & Whinston., 2007; Romanowsky, Telang & Acquisti, 2008); **insurance on information security** (Adkin, 2004; Bohme, 2005; Ogut, Menon & Raghunathan, 2005; Herath & Herath, 2007; Bolot & Lelarge, 2008); **the economics of privacy** (Vila, Greenstadt & Molnar, 2003; Syverson, 2003; Huberman, Adar & Fine, 2005; Acquisti & Grossklags, 2005; Challappa & Sin, 2008); **the economics of digital rights management** (Lewis, 2003; Jamkhedkar & Heilman, 2005, Bae & Choi, 2008) **and the economics of information security investment** (Gordon & Loeb, 2002; Camp, 2006; Anderson & Moore, 2006; Grossklags, Christin & Chuang, 2008; Hulthen, 2008) among other topics.

Under the umbrella of the field of the economics of information security, this dissertation focuses and builds on the last topic on the economics of information security investment aspect. The following section discusses the current state-of-the-art information security investments

3.3 Information Security Investment

An investment in information security is viewed from two opposing perspectives: either from the system defenders' or the attackers' point of view.

Investing in information security on the defence side is a trade-off; organisations can either choose to invest in security or not to invest (Anderson, 2001; Ioannidis, Pym & Williams, 2009). There are both direct and indirect benefits and costs involved. Directly, investing in information security reduces the risk exposure but at an opportunity cost of other profitable investment. Not investing in information security guarantees more money but at an opportunity cost of not having secure information assets. Indirectly investing in information security can help those who have not invested to "a free ride". For those who invest, they could easily become victims of threats coming from those who fail to invest (just like environmental pollution, from an individual's pollution everybody suffers the consequences). Akerlof (1970) has more insights on these issues. Information security practitioners have to consider the trade-offs and such issues when scrutinising and making information security investment decisions.

Given the current threat landscape, the consequences of not investing in information security can prove to be more costly and devastating than investing (Fumey-Nassah, 2007). Chapman (2009) reporting on a survey conducted by McAfee highlights that organisations are losing billions of dollars because of information security breaches. These include the amount of time and effort that is involved in recovering from an information security breach. Moreover, there are also compliance fines and penalties.

Therefore, the consequences of not investing in information security are just overwhelming and organisations have been left with no option but to invest in information security. This is confirmed by industry-related surveys such as the 2008 Ernst & Young Global Information Security Survey (van Kessel, 2008), which indicates that despite the economic pressures, organisations will continue to invest in information security. In actual fact over 50% of respondents were reported to be planning to increase their investment in information security as a percentage of total expenditure in the Ernst & Young survey.

Until recently, most organisations have allocated resources to information security in an ad hoc and distributed way by providing the funds as a part of other budgets, such as IT in general. This, amongst other reasons, has made it difficult to determine the exact amount of money that organisations are really spending on information security. Since around 1998, information security experts have been deliberating the analysis of information security investment from an economic perspective (Abrams et al, 1998). The focus has been put on how to reasonably and adequately allocate financial resources to information security. Many researchers have applied economic models to investigate the cost-effectiveness of information security investment and their point of optimality. However, there are some challenges that researchers need to overcome before they find the solution.

3.3.1 Information Security Investment Challenges

Researchers have identified several challenges that managers face when allocating resources to information security investments. Abrams et al. (1998), Conrad (2005), Pfleeger and Pfleeger (2007:578) and Wei et al. (2008), argues that information security managers and other decision makers are required to make precise decisions for allocating funds to information security activities with incomplete and uncertain information. They argue that information security variables such as the probability of threats, the impact of threats, and the cost of security controls are associated with a lot of uncertainties that make modelling very difficult. Srinidhi, Yan & Tayi, (2008) agree with the above and argues that this is because most of the risks are intangible, uncertain and probabilistic in nature.

Conrad (2005) proposes the use of Monte-Carlo simulations to analyse and eliminate the uncertainty of information security investment estimates. These simulations may not be perfect, but they do reduce uncertainty to a certain extent.

Moreover, information security's benefits and losses cannot be easily attached to a specific monetary value. For example, it is difficult to determine the monetary cost of delays caused by

information systems going down for an hour. Abrams et al. (1998) also reports that the risks affecting information assets keeps increasing yet the funds remain constant.

Furthermore, there are currently no general acceptable formulas for allocating funds to information security. Researchers have tried to evaluate information security investments by using financial analysis tools such as return on (security) investment (ROI/ROSI), net present value (NPV), internal rate of return (IRR) and payback. The majority of the research efforts focus on ROI/ROSI analysis (Sygate, 2002; Geer, 2002; Pappa, 2002; Aceituno, 2003; Purser, 2004; Davis, 2005; Melillo, 2006; Buck, Das & Hanf, 2008). Despite some critical comments on this approach (Wood and Parker, 2004; Forte and Power, 2004; Pfleeger and Pfleeger, 2007:574), the results are still not satisfying and lack industry acceptance (Wood & Parker, 2004).

The work of Wood and Parker (2004) provides interesting yet critical insights into employing financial methods for evaluating the allocation of financial resources to information security. They argued that financial methods are failing because there is no reliable actuarial loss statistics in the information security arena. They therefore contend that, rather than relying on such tools, the "standard of due care" strategy must be used for selecting the controls to be deployed. This approach is based on adopting and investing in the same controls and practices as other organisations in similar circumstances. Although this strategy ensures compliance, organisations must do more than merely comply with regulatory mandates (van Kessel, 2008). Information security is not just about reaching the finish line, but rather about going beyond the finish line.

3.3.2 An Optimal Allocation of Funds to Information Security

Even though none of the reviewed literature seems to make the distinction between the two dimensions of information security investment (one on the cost side and the other the benefits side); in this chapter we acknowledge and distinguish between them. Further unpacking an information security investment, this chapter is focused on the cost side i.e. the allocation of financial resources to information security. From this point on, an information security spending, information security budget or information security investment will be used interchangeably to

mean the same thing i.e. information security investment on the cost side (allocation of funds to information security).

Organisations need adequate information security at a reasonable cost. For information security to make business sense; organisations must strike the right balance between the likelihood of risk and the cost to reduce the risk (Su, 2006). This has proven not an easy task to do. Goetz and Johnson (2006) points out that a majority of executives view information security as a "bottomless pit that never gets full" and some as "necessary evil that hinders productivity" (Conray-Murray, 2003). This is mainly due to the failure of information security managers to quantify their expenditures, the likelihood of the risk faced by the information assets materialising and the nature of information security which prevents users to access unauthorised materials. This has led executives to ask "how much is really enough for information security?"

In answering the fore-going question and contrary to the views of "a bottomless information security pit that never gets full"; researchers argue that there is actually an optimal point for information security spending (Anderson, 2001; Huang, Hu and Behara, 2008), which several researchers have tried to determine. They argue that it is not advisable to invest below or beyond this point.

Huang et al. (2006) proposed an economic model to determine an optimal information security spending. Their findings show that there is a minimum vulnerability level below which information security spending is zero. They also show that there is a point beyond which an investment in recovery from loss is more feasible than an investment to defend against certain vulnerabilities. They argue that organisations need to invest in different information security controls to fight different types of threats. However, given a small budget, there is a need to focus the budget on the class of attacks that pose high risk. In a nutshell – they use economic modelling to analyse optimal information security investment decisions for organisations under multiple attacks. Modelling with variables such as system vulnerability, potential loss, budget and investment effectiveness, they demonstrate how to optimally allocate information security investments.

Wang and Song (2008) proposed modelling with information security requirements, opportunity costs of the risks and budget constraints using a multi-objective decision making framework to determine the optimal information security investment. Unfortunately, the modelling approaches discussed in both Huang et al. (2006) and Wang and Song (2008) do not provide a definite figure or the exact point of optimality for an information security investment. Srinidhi et al. (2008) also presents a model to assist information security managers to optimally allocate financial resources on information security to guarantee productivity and information assets' safety.

Gordon and Loeb (2002) proposed and presented an economic model (which we call G&L hereafter) to determine the optimal allocation of funds among different assets with different vulnerabilities to information security. Unlike the work of Huang et al. (2006) and Wang and Song (2008), their findings show that the optimal investment for protecting an information asset must at least be less than or equal to 37% of the total loss expected of the information asset. The G&L model also contends that "the optimal amount to invest in information security does not always increase with the level of vulnerability". Gordon and Loeb's work has received significant interest from other researchers in the economics of information security space.

Willemson (2006) reviewed and refuted the G&L model's claim. Relaxing this model's assumptions, Willemson provided a function that suggests an investment of up to 50% and even up to 100% of the expected loss of an information asset which is much higher than the 37% stipulated in the G&L model.

Tanaka, Matsuura and Sudoh (2005) conducted an extensive empirical study using the G&L model. This work investigates the relationship between information sharing and vulnerability levels and how it influences the decisions on information security investments. Liu et al. (2007) also conducted an empirical study on the G&L model to verify the relationship between the effects of an information security investment and the vulnerability level.

Matsuura (2008) realized that the G&L model derive its economic benefit from the threat reduction. Matsuura concluded that this was not enough and then extended the G&L model to include a measure of productivity.

Huang et al. (2008) extended the G&L model to include a risk-averse decision maker instead of a risk-neutral decision maker and adopted the expected utility theory. They modelled the relationship between the potential loss, extent of risk aversion and the effectiveness of an information security investment.

Several researchers' efforts are underway to determine an optimal information security investment, yet very little has been done to determine whether such optimal investments are cost-effectiveness. In this research the emphasis is on both an optimal and cost-effective information security investment.

For the purposes of this research:

- An optimal information security investment is defined as one that best utilizes budget resources (be it sufficient or insufficient) to yield the best possible information risk mitigation strategies.

- A cost-effective information security investment is defined as one that ensures spending only on the relevant, appropriate and necessary information security measures.

The next sub-section discusses the current body of knowledge regarding the cost-effectiveness of information security investment.

3.3.3 Cost-Effective Information Security Investments

The current information security landscape requires experienced and influential information security decision makers to ensure that information assets are protected adequately and cost-effectively in the face of increasing risks and diminishing budgets (Heiser, 2009). In order to adequately protect information assets, today's information security decision makers are required to identify appropriate information security goals that are inline with the overall business goals to fulfil and execute cost-effective defence strategies to fulfil the identified goals.

Wei et al. (2005) provide the most related and relevant research when considering the above approach. They proposed a layered decision model (LDM) that takes business goals and the threat landscape as input to determine the best cost-effective defence strategies and tactics from a bigger set of strategies to thwart a given threat. Their model considers multiple levels of decision making similar to what is proposed in this dissertation. This dissertation is based on multiple levels of an organisation i.e. strategic, tactical and operational, unlike Wei et al.'s work which is based on an information security policy (Layer 0), defence strategies (Layer 1) and defence tactics (Layer 2). Their work takes into account the iterations between the levels to show the how decisions in one layer affects decision on other layers. Moreover, Wei et al.'s work seeks to determine cost-effective security measures to support consistent and connected decisions at all three levels, similar to the case in point in this dissertation.

Wei et al. (2007) extends their earlier work (Wei et al., 2005) by adopting a simulation approach based on face validity techniques to validate the LDM's rationality. Their model's rationality is based on consistency, free from blocked execution paths (BEP) and optimality (in terms of the best cost-effective strategy). This work demonstrate the application of the LDM in the decision making process for cost-effective defence strategies on the three layers and their relationships.

Wei et al. (2008) further extends their earlier work (Wei et al., 2005; Wei et al. 2007) by conducting a case study to demonstrate the application of the LDM in a real world scenario in a manner that meets the model's rationality requirements. They applied the model in a real-world e-commerce scenario to provide a concrete example to demonstrate the usage of the LDM in selecting the best cost-effective defence strategy from a pool of other strategies.

The distinct difference from the work of Wei et al. (2005), (2007) and (2008) and this research, is that this dissertation considers information security standards and classifies information security controls into three broad controls to be implemented in accordance with organisational levels whilst they use three specific layers. They do not consider the overall information security architecture whilst our model is based on one. Even though it does not come out clear in their work how they calculate the benefit of their investments, their model makes the final decision based on a cost-benefit analysis. Due to the intangibles associated with the benefits of

information security our work refrains from using a cost-benefit analysis and concentrate on the cost side before an attack occurs (what is referred as pre-occurrence in work of Wei et al., 2005; 2007 and 2008). Their model considers both cases, the preventative cost before it occur and the cost of recovery after an attack has already occurred which they respectively refer to as pre-occurrence and post-occurrence.

In summary the reviewed literature on information security investment, including the above, has shown that there is a wide range of tools, models, techniques, methodologies and theoretical approaches for defining, describing and measuring information security investments. However, several main shortcomings still exist as pointed out in the next paragraph.

3.4 Existing Gaps Identified in the Current Body of Knowledge

The problem with the current body of knowledge with regards to an information security investment is that it does not provide or recommend a set of all en-compassing requirements that information security decision makers have to consider when they develop their budgeting models.

Researchers in the field of requirements engineering argue that in almost all projects that fail to meet performance, business and cost goals, inadequate requirements had played a pivotal role resulting in such failure (Dorfman, 1997). Hence, all systems, models and frameworks development should be based and centred on design requirements. These requirements act as a bridge between existing models and the proposed model. Requirements are necessary in any attempts taken by decision makers to solve the problem of how to achieve an optimal and cost-effective resource allocation to information security.

Furthermore, information security managers and other decision makers need to provide evidence of the success or failure of their information security spending. Due to the difficulty in establishing the monetary value of information security benefits, requirements can also be used to act as the measure of success or failure of models for the allocation of resources. A

requirements elicitation process is therefore an acceptable first step in any attempts to find the solutions to the optimal and cost-effective allocation of funds for information security.

The current body of knowledge on information security investment also does not provide guidelines for the allocation of funds to different types (broad categories) of controls. Most of the covered literature agrees that information security must be implemented on the strategic, tactical and operational levels (Eloff, 2005). But how must the funds be appropriately allocated for the implementation of controls on each level? How does one distribute the available funds between the different components of information security, sometimes referred to as people, processes and technology (Theoharidou et al., 2005)? These questions have not been answered. Moreover, the current body of knowledge does not take cognisance of internationally accepted standards, regulations and codes of best practice, as well as of specific characteristics (views) of individual organisations in order to meet their unique needs.

Chapter 4 will discuss the gaps identified in this chapter in terms of all-encompassing requirements to become inputs in the proposed solution. This is structured in such a way that the gaps identified in this chapter become requirements in the next chapter. The next section concludes this chapter.

3.5 Conclusion

This chapter has revealed the current state-of-the-art economics of information security and has also identified the gaps and shortcomings thereof. Within the field of economics of information security this chapter focused on the work that is being done in the information security investment with particular reference to the cost of an investment excluding the benefit side for scoping purposes. Drilling further down within information security investment, this chapter reviewed literature on the optimality of such investment which showed more emphasis on the G&L model. This chapter has also discussed the cost-effectiveness of information security investments. The results of the covered literature are still not satisfactory. There are still gaps and short-comings that require more investigation in order to achieve the desired results of an optimal and cost-effective information security investment.

The contribution of this chapter to the overall goal of the research at hand comes in providing the current state-of-the-art on the economics of information security investment.

The next chapter seeks to investigate and determine a set of all en-compassing requirements for modelling an optimal and cost-effective information security investment. These requirements will be based on the gaps and short-comings of the existing literature. The requirements will provide guidance at the design phase and also act as the key performance indicator for the success or failure of the proposed solution. The design and validation process can be a very daunting task without the guiding requirements. It is therefore very important for the next chapter to solely concentrate on the requirements elicitation process.

Chapter 4

Requirements Elicitation for the Proposed BC3I Model

4.0 Introduction

As a contribution to the overall goal of this research, the previous chapter provided an investigation of the current state-of-the-art economics of information security investment and existing gaps thereof. This creates the need to address the gaps identified in existing literature in the previous chapter and advance the current state-of-the-art. The identified gaps provide input to the requirement elicitation process for developing the proposed BC3I model. Therefore, in an attempt to advance the current state-of-the-art, this chapter investigates and identifies a set of encompassing requirements to be considered as input when modelling an optimal and cost-effective information security budget. This is to set the scene in preparation for the design of the proposed solution.

The elicitation of requirements for preparing an information security budget as proposed in this chapter is structured as follows: Section 4.1 briefly discusses the requirements drawn from the current state-of-the-art work covered in the previous chapter; an indication that this research does not exist in isolation but it is based on relevant and related existing research work. Section 4.2 discusses additional requirements that are based on the concept of information security architecture. This is to ensure that the budget covers an organisation in a holistic manner. This section ends by outlining other non-functional requirements. Section 4.3 provides a summary of the requirements. Section 4.4 discusses the information security broad control categories to be considered in the design of the model in the chapter five and section 4.5 concludes the chapter.

4.1 Requirements gleaned from existing approaches

Below is a list of requirements that were identified following the gaps identified in the literature review in the previous chapter:

- Information security should be viewed as a strategic and multi-disciplinary field and therefore the budget should reflect implementation issues across the spectrum of people, process and technology (Lipari, 2009; Volker, 2007; Gordon et al., 2006; Tsiakis & Stephanides, 2005). Instead of concentrating on only one or two aspects leaving the organisation wide open on the other; the budget should be spent optimally on all aspects and at all levels of an organisation.

- The budget should reflect implementation issues on the defence as well as attack side, i.e. proactive and reactive (Lipari, 2009). An information security budget should cover current threats and also be proactive by anticipating the costs of emerging and future threats. It is difficult to precisely predict future budgets, but extrapolating on the current information security budget can give an indication of the budget to counter emerging and future threats.

- Careful consideration should be given towards striking the right balance between the "standard-of-due-care" versus a risk assessment approach (Wood & Parker, 2004). When considering information security issues, it is not enough to only do what other organisations in similar positions do. Organisations must consider what the other organisations are doing (best practices), and moreover they should consider their own risk exposure if they are to differentiate themselves from the rest and gain a competitive edge over their competitors.

- Regulatory compliance is one of the major drivers for the increasing information security budget (Melek & MacKinnon, 2005; Berinato & Ware, 2005; Holmes, 2006; van Kessel, 2006, 2007; Berinato, 2007). However, an information security budget should address more than merely regulatory and standards compliance. Organisations differ in many aspects, from the information assets that require protection to the manner in which they want to protect

them. Therefore an information security budget should also consider the interest, goals and values of an organisation.

- An information security budget should be based on assumptions clearly communicated to senior management with specific reference to the % coverage of vulnerability exposure as well as the % acceptable risk levels (Gordon & Loeb, 2002). This requirement bridges the gap between senior management and security experts. If this requirement is appropriately met, it could easily ensure that security experts get the necessary buy-in and commitment from senior management.

It has been discovered that the current body of knowledge does not take cognisance of some other requirements that should play a role in determining an information security budget within an organisation. These are requirements that relate to the structure of the organisation itself and the way information security is implemented in organisations. On that basis, the next section outlines and briefly discusses these as additional requirements.

4.2 Further requirements

Based on the general structure of organisations and information security architecture, the following additional requirements have been identified as vital for the preparation of an information security budget:

4.2.1 Taking cognisance of the three organisational levels
4.2.2 Based on a well defined Information Security Architecture
4.2.3 Non-functional requirements such as flexibility and adaptability of the model

These requirements were chosen to ensure that the budget holistically covers all the levels of an organisation and follow a well laid out information security architecture.

Apart from the functional requirements, there are also non-functional requirements that must be considered. When modelling, it is vital for the designers to consider both the internal and external factors to ensure the completeness of the model and avoid flaws from the unforeseen external factors. It is for this reason that the proposed model should also consider non-functional factors.

4.2.1 Taking cognizance of the three organisational levels

The model design should take cognizance of the three well-known organisational levels, namely strategic, tactical and operational levels. These levels are to be used as a framework for organising the proposed requirements (Rolfsdotter Karlson, 2008).

4.2.1.1 Strategic level

On the strategic level the budget for information security should be aligned with the vision statement of the organisation, the business goals, legal obligations, overall risk appetite and policy statements. The vision and values of an organisation may not directly influence information security spending; however, any money spent should be in direct support of realistic and reachable business goals and priorities of the organisation. Since the business goals are derived from the vision and values of an organisation, they can be translated into the critical success factors (Rolfsdotter Karlson, 2008) which when they can be met would ensure that information security programs are tightly coupled to the overall business strategy.

Legal obligations are stipulated in national and international regulatory requirements and laws. Organisations are required to adhere to these mandates or face prosecution if they do not. For example, in South Africa the 'Promotion of Access to Information Act' (SA, 2000:2) requires the "Mandatory protection of the privacy of a third party who is a natural person". This means that an organisation (public or private) must refuse access to such information if it can result in the unreasonable disclosure of a third party's personal information. Unauthorized access must not

be allowed and organisations need to take precautions to prevent it. Refusal of access to private information also requires the encryption of information sent over any public networks.

The international regulatory requirement; Sarbanes-Oxley Act (SOX, 2002) in the USA was promulgated in essence to protect investors by improving the accuracy and reliability of the financial information disclosed by corporations.

Industry related laws and regulations must also be taken into account. For example, in the financial sector, banks usually publish on their web sites to which laws and regulations they comply as well as any disclaimers (FNB, 2009; ABSA Bank, 2009; Barclays Bank, 2009; ZKB, 2009). The Banking Council of South Africa published a Code of Banking Practice (COBP, 2009) for banks in South Africa to adhere to.

Policy documents may also confirm the intent of an organisation; for example to protect the privacy of third parties. A policy describes the specific steps that an organisation will take and expect its employees to adhere to in order to reach its business goals.

Compliance to national and international standards and laws will also influence the cost of information security. The ISO/IEC 27002: 2005 Information technology - Security techniques - Code of practice for information security management, contains best practice recommendations on the overall management of information security (ISO/IEC 27002, 2005). Many countries have equivalent standards on national level that reflects ISO/IEC 27002, such as the British Standard BS ISO/IEC 27002:2005 and the AS/NZS ISO/IEC 17799:2006 standard in New Zealand and Australia. The Basel II Accord (2003) is an international banking standard developed by the Federal Reserve Board to ensure that banks put enough money aside in order to alleviate financial and operational risks. Compliance to standards will also influence the spending on information security.

It must be mentioned though that complying with these mandates and laws could create false sense of security. These mandates form a baseline for implementing security and they achieve

minimal security. A strategic approach would be for organisations to spend on compliance and go beyond that to spend on security controls that are in-line with their business strategy.

4.2.1.2 Tactical level

The tactical level includes risk analysis for the identification of threats, standards and any compliance requirements. Risk Analysis plays an important role in identifying all threats to the security of information assets. Even though a risk analysis does not answer all the information security questions, it can still play a guiding role in order to decide 'how much' to spend and on 'what'. Butler (2003) also identified other shortcomings of risk analysis, for example to make exact investment decisions based on 'guesstimated' information.

4.2.1.3 Operational level

On the operational level both operational requirements and technological requirements need to be considered.

Operational requirements include aspects such as affordability of manpower, resources, optimal protection levels and feasibility. Furthermore, the operational level includes administrative requirements referring to guiding the user's actions to meet business goals and objectives as specified on the strategic level.

Technological requirements include both ICT infrastructure components such as controls on the hardware and software levels. When selecting controls, identification of an optimal mix of controls is of vital importance.

4.2.2 Requirement based on an Information Security Architecture

Eloff and Eloff (2005) proposed a number of requirements for the establishment of an information security architecture. These requirements originally defined for developing

information security architecture can also be translated into requirements for information security budgets. These requirements states that an information security architecture should adhere to the following requirements:

- Be holistic and encompassing: The budget for Information Security should indeed be holistic with reference to the full spectrum of controls to be implemented. The requirement of holism refers to the inclusion and consideration of all aspects when budgeting and spending for security. Pattersen (2003) coined the phrase 'holistic security', referring to the integrated mix of technology, people and procedures. According to Zucatto (2007), holistic means that the three dimensions of business, technology and society should be considered. Information Security spending should not focus on isolated aspects but on all aspects.

- Make suggestions on how different controls can be synchronized and integrated to achieve maximum effect: Very few organisations today spend enough time on the synchronization and integration of controls resulting in a potential over expenditure duplicating controls. For example: confidentiality on the database level can be implemented by means of physical separation and / or logical separation. Furthermore it might be more cost effective to first implement confidentiality by means of proper access control facilities, which is then later followed with crypto facilities. The synchronization and integration of controls in most cases are organisation specific.

- Include a comprehensive approach to information security risk management: The relation between a comprehensive approach for risk management and the information security budget is self explanatory as the budget for information security should very clearly indicate how much risk mitigation is planned for as well as the acceptable risk that the organisation will endure.

- Be measurable to demonstrate adherence to the requirements as set out. Research has shown that it is somehow difficult to establish the monetary value of information security controls and the benefits derived (Abrams et al., 1998; Conrad, 2005; Pfleeger & Pfleeger, 2007;

Srinidhi et al, 2008). Despite the difficulties, the results should be expressed in monetary terms.

4.2.3 Non-functional requirements

Non-functional requirements are viewed as those that impose constraints on the compilation of the budget for information security. Non-functional requirements are applicable on all three organisational levels. Previous work in which the author of this research co-authored, as reported in Dlamini, Eloff, Eloff & Hone (2009), suggests the following high level non-functional requirements:

- **Flexibility**: The non-functional requirements of flexibility and adaptability demands that when anything on any of the three organisational levels change, then information security budgeting and spending should also be easy to change and still yield acceptable results. The flexibility and adaptability requirement recognize the fact that organisations are different and they exist in different sectors and context. One prescribed set of information security controls will not satisfy the requirements of all organisations. Organisations from different sectors will have different information security requirements, for example a hospital as opposed to a bank.

- **Cost effectiveness:** this requirement stipulates that organisations must be able to identify and implement those controls that will protect their information resources in the most cost effective way – implementing all the controls may be overkill and could create more complexity. Organisations must only implement "enough" i.e. all relevant and necessary controls and nothing more.

Lastly, the existing and current information security budget must not be ignored as a valuable input into the future budget. The existing and current budget can highlight over-expenditure on unimportant items, as well as under-expenditure on high risk areas. The existing investment will also shape where recurring costs must be budgeted for, e.g. licensing fees on information security tools, hardware upgrades on information security technology.

The next section investigates existing information security control categories at macro (high) level and further goes on to propose a new categorization to be used in this research to facilitate the modelling process in the next chapter.

4.3 Information Security Broad Control Categories

This section reviews the currently existing categorisation of information security controls. The reason for this exercise is to provide input into the difficult task of identifying an adequate set of controls.

Several categories of information security controls are found in literature, for example in the National Institute of Standards and Technology's (NIST, 2005) special publication 800-12, the Red Hat Enterprise Linux Guide, and categorisations proposed by Killmeyer (2006:15), Purcell (2007) and Gerber and von Solms (2005).

The NIST (2005) special publication outlines the categories of controls as management, operational and technical controls. This publication describes management controls as those controls that focus on the high-level management of computer and information security, and business risk. Operational controls focus on controls that are designed, implemented and executed by human beings who have the required technical expertise. Technical controls focus on controls that computer systems execute automatically. According to the NIST publication, these broad control categories are interdependent. This is the same control interdependency that Eloff and Eloff (2005) argue must be considered in drafting and implementing an information security strategy.

The Red Hat Enterprise Linux Security Guide, Killmeyer (2006:15) and Purcell (2007) broadly categorise information security controls as administrative, technical and physical. The Red Hat Guide defines administrative controls as those that focus on the human factor of security. Technical controls are defined as those that use technologies for controlling access to data and

information, while physical controls are those that prevent physical access to unauthorised information and systems.

According to Killmeyer, administrative controls include security policies/procedures and data/resource ownership. Physical controls are those controls that constrain direct physical access to information and its infrastructure. Technical controls are implemented through hardware or software that can work without human intervention. Killmeyer further divides each of the categories into preventive and detective. Preventive controls attempt to stop security breaches before they occur, while detective controls attempt to correct security breaches after they have occurred. Killmeyer argues that "these controls must be used collectively to meet the challenges of realistic business risk", but unfortunately provides no details of how this can be done.

Purcell (2007) argues that there are two ways to categorise information security controls:

- Based on what the controls are, e.g. administrative policy, technical firewall and physical fence.
- Based on what the controls do, e.g. detective, preventive, corrective, etc.

In Purcell (2007), administrative controls are defined as policies, guidelines and procedures put in place to define and guide employee actions in accessing the organisation's resources as they perform their duties. Technical controls are logical controls, i.e. software and hardware devices, processes, protocols and other measures. Physical controls are defined as devices and means to control physical access to information resources. Based on what the control does, Purcell goes on to define preventive, detective, corrective, recovery, deterrent and directive controls. His work also addresses the issue of inter-dependency between controls, however not in a comprehensive manner.

Gerber and von Solms (2005) agree that information protection requires physical, technical and operational controls. However, they do not go into detail to explain each of the categories.

Based on the reviewed literature, this research proposes the following broad control categories for information security:

- Administrative controls – high-level controls that guide the user's actions in executing duties to meet business goals and objectives.
- Operational controls – implemented through software or hardware systems that execute automatically and with minimal intervention, or without a human operator.
- Environmental controls – controls that restrict physical access to information and its infrastructure.

Hence, the above will be referred to as the broad control categories in the remainder of this dissertation. These broad control categories are required to provide support during the process of compiling budgets for information security. The ultimate question with regard to an information security budget is – how much should be allocated to each of the three broad control categories to cost effectively protect the information assets? This will be addressed in the next chapter. The next section summarizes the requirements.

4.4 Summary

In summary, the proposed list of requirements for preparing an information security budget as identified in this chapter is as follows:

- The budget should clearly reflect that information security is multi-disciplinary in nature.
- The budget should provide for defence as well as attack strategies.
- The budget should strive to strike the right balance between the "standard of due care" and risk assessment approaches.
- The budget should address more than just regulatory and compliance issues.
- The budget should clearly document assumptions made in the budgeting process such as the % of vulnerability coverage as well as the % of risk acceptance. It is important to include both the percentage vulnerability coverage and risk acceptance in the risk assessment, which in turn is included when preparing the budget for information security.
- When preparing the information security budget careful consideration should be given to the three organisational levels.

- Use a well-defined Information Security Architecture as framework for preparing the budget.
- Address non-functional issues such as flexibility and cost effectiveness.

The UML diagram depicted in Figure 4.1 shows the requirements to be considered in preparing an information security budget. More specifically, a use case diagram is employed showing what should be done without discussing how it should be done. Furthermore this diagram, as shown, also makes an attempt in demonstrating the collaboration between the different components.

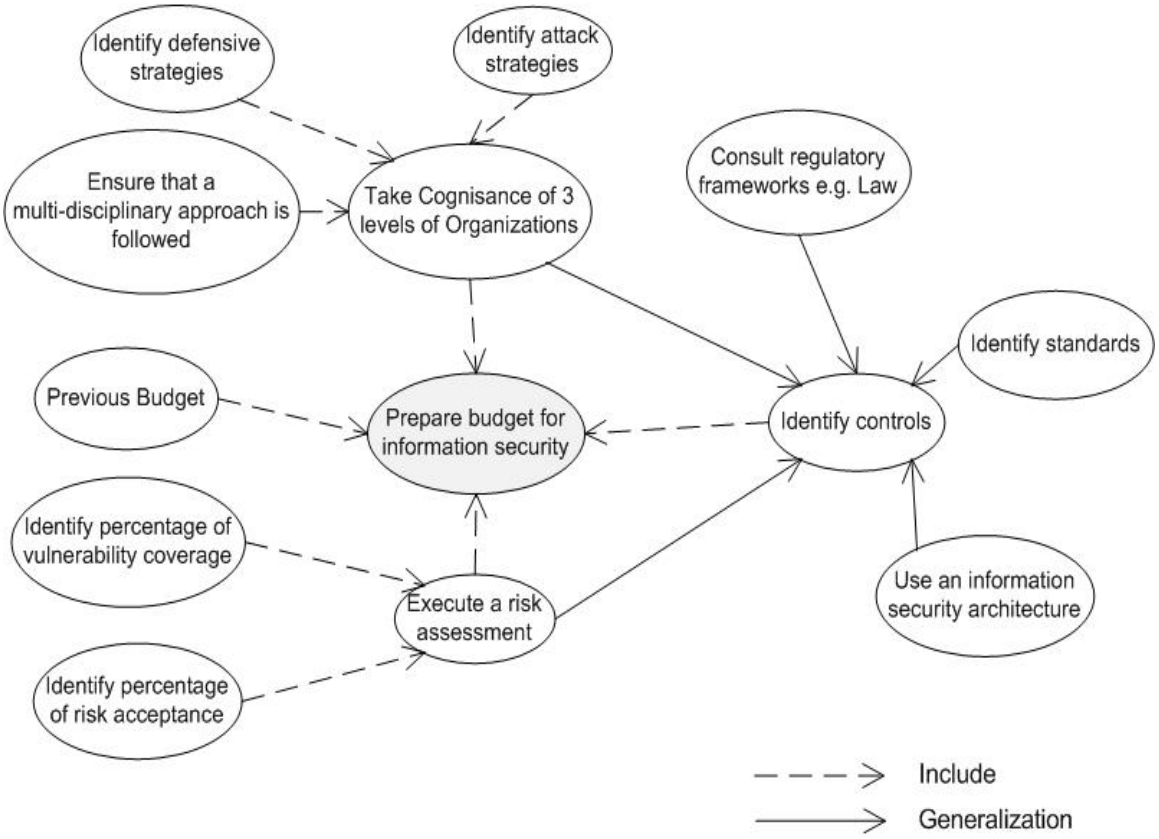


Figure 4.1: Diagram depicting the requirements for preparing an information security budget (Dlamini et al. 2009)

Consider the diagram in figure 4.1: the identification of controls can be generalized as being the outputs of activities such as controls identified by means of regulatory investigations, standards,

use of information security architecture, risk analysis as well as the cognizance of the three organisational levels. These generalizations are depicted by fixed lines whereas the broken lines show activities that should be included in the activity when preparing a budget for information security.

4.5 Conclusion

Current models, methodologies and approaches (as identified in chapter three) used to determine how much to spend in order to securely safeguard information assets do not consider the total picture of an organisation's environment and context in which it operates in terms of all-encompassing requirements. This chapter has approached and addressed this problem by identifying the all-encompassing requirements to consider when preparing information security budgets. These requirements are presented in a "use case" diagram illustrating the potential interaction between the different components.

System design, be it architectural, software or any design for that matter, must all begin with a requirements elicitation process. The results of this process are clear requirements that become an input for the development phase. These requirements act as guidelines, benchmarks or key success factors of the system. The proposed model in this research is no different; it also begins with the requirements elicitation process. The next chapter take cognisance of the identified all encompassing requirements and implement them in an information security budget model called the BC3I.

Chapter 5

BC3I – A Model for Information Security Budget

5.0 Introduction

The previous chapter identified the requirements to consider when preparing information security budgets and summarised them in a use case diagram. This chapter proposes the BC3I model to determine the cost indicators for a cost effective information security budget that focuses on an adequate mix of controls. The cost indicators' goal is to assist in selecting or recommending an appropriate set of controls that are expected to yield the best possible outcome with the available financial resources. This is to aid the decision-making process regarding information security budget by supplying substantiated information. The results of the model also seek to provide guidance to decision makers in their efforts to justify and receive funding for information security.

The question with regard to information security funding has always been – how much to invest in information security? In this dissertation the author acknowledges the plethora of possible solutions proposed by several researchers in the field of the economics of information security. In an attempt to drill further down and advance the current state-of-the-art, this research's ultimate question is - how much should be allocated to each of the three broad control categories as identified in the previous chapter i.e. administrative, operational and environmental controls in order to cost effectively protect an organisation's information assets at all levels? For example – should the focus be more on administrative as opposed to environmental and operational controls, or on both? The main goal of this research is to find a balanced information security budget across all three broad control categories. The requirements from the previous chapter form the basis for the design and development of the BC3I (Broad Control Category Cost Indicators) model to achieve the research goal.

In order to achieve the goal of this research based on the proposed high level requirements, the remainder of this chapter is structured as follows: Section 5.1 recaps and highlights the requirements for the design and development of the model. Section 5.2 begins with a brief description of the high level requirements. It further develops and discusses the proposed BC3I model. Section 5.2 concludes by highlighting the limitations of the BC3I model. In closing, section 5.3 concludes the chapter and provides pointers to the discussion of the next chapter.

5.1 The requirements for the BC3I model

This chapter presents the proposed BC3I model to achieve the research goal, answer and give meaningful guidance with regards to the main research question. As mentioned earlier, the BC3I model is based on the requirements as outlined in the previous chapter. For modelling purposes and due to the overlaps on the requirements, the related requirements have been grouped into four high level requirements i.e. (1) take cognisance of the business goals; (2) take a holistic approach towards the implementation of information security; (3) be flexible and (4) cost effective. The BC3I model considers only these four high level requirements. However, it is important at this point to acknowledge the overlaps that exist within these high level requirements. The following diagram illustrates the high level requirements drawn from the requirements in the previous chapter.

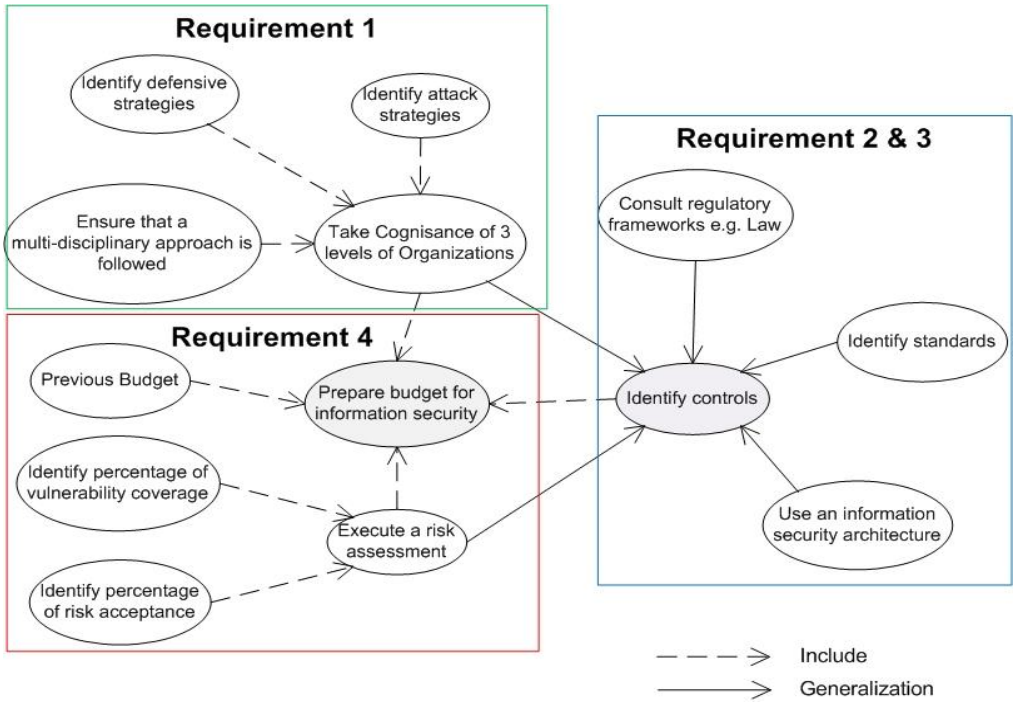


Figure 5.1: Diagram depicting high-level requirements for preparing an information security budget

5.2 The BC3I Model

5.2.1 High-level Requirements for BC3I

Below is a brief description of each of the four high-level requirements for the envisaged BC3I model:

5.2.1.1 Requirement 1: Cognisance of the business goals of an organisation

This requirement ensures that all aspects of an information security budget are aligned and geared towards achieving the overall business goals of the organisation. Thus, the emphasis here is placed on an information security budget that focuses only on controls that seeks to achieve those goals and help the organisation gain competitive advantage. This requirement requires a clear understanding of the attacks vectors and their defence strategies at all three levels of an organisation.

5.2.1.2 Requirement 2: A holistic approach towards the implementation of information security

Adopt a holistic approach in protecting the information assets. A holistic approach in the context of the BC3I model implies that controls are selected from all three broad control categories, i.e. Administrative, Operational and Environmental controls to cover all three levels of an organisation, i.e. strategic, tactical and technical levels. The controls must come from a wide selection of information security standards, regulatory frameworks and from an organisation's information security architecture.

5.2.1.3 Requirement 3: Flexibility

Information security must be managed in a flexible manner. A one-size-fits-all strategy does not work, as different organisations respond to information security risks differently. Organisations from different sectors, such as manufacturing and retail, will implement controls prescribed in accordance with different information security standards. Moreover, organisations also implement different custom-made controls depending on their specific needs and requirements.

5.2.1.4 Requirement 4: Cost Effectiveness

Organisations must comply only with those standards that are truly pertinent to their information security. If organisations were to comply with all of the many information security standards, they would have to unnecessarily increase their security budget. This is ineffective and creates overheads from a cost point of view, as many standards overlap. The BC3I model must also take cognisance of the previous budget, percentage vulnerability and risk acceptance

The BC3I model seeks to achieve the overall goal of this research by implementing the above requirements. These requirements will help determine the cost indicators that will give guidance

on the amount to be spent on administrative, operational and environmental controls in order to achieve an appropriate balance between them and in a cost-effective manner.

The next section discusses the components of the BC3I model i.e. variables, constraints and objectives. It further goes on to the design and development of the model.

5.2.2 Variables

5.2.2.1 Broad Control Categories

Let x_{ij} be an information security control.

Furthermore:

$\{\forall x_{ij} \mid x_{ij}$ is an element of a standard or a customised control within the organisation (made specifically for that particular organisation and not taken from any standard, guideline or best practice)$\}$.

X_1: Broad control category consisting of administrative controls

Let x_{1_i} be an administrative control.

Furthermore:

Let $X_1 = \{x_{1_1}, x_{1_2}, \ldots, x_{1_i}\}$

Note:

For example: $n(X_1) = 4$, $X_1 = \{$policy, standards, guidelines, procedures$\}$

X_2: Broad control category consisting of operational controls

Let x_{2_m} be an operational control.

Furthermore:

Let $X_2 = \{x_{2_1}, x_{2_2}, \ldots, x_{2_m}\}$

Note:

For example: $n(X_2) = 3$, X_2 = {firewall, anti-virus, two-factor authentication}

X_3: Broad control category consisting of environmental controls

Let x_{3_n} be an environmental control.

Furthermore:

Let $X_3 = \{x_{3_1}, x_{3_2}, \ldots, x_{3_n}\}$

Note:

For example: $n(X_3) = 3$, X_3 = {surveillance cameras, office buildings, security guards}

and

$$\{\forall\, x_{i_j} \mid \exists\, (x_{i_j} \in X_1 \vee x_{i_j} \in X_2 \vee x_{i_j} \in X_3)\},\ \forall\, i{:}1 \leq i \leq .3 \text{ and } \forall j{:}1 \leq j \leq (l \vee m \vee n)$$

The implication is that each and every control will come from either one of the above three supersets X_1, X_2 and X_3.

5.2.2.2 The Universal Set of Broad Control Categories

Let U be the universal set of all information security controls over all broad control categories.

Furthermore:

$U = \{X_1, X_2, X_3\}$

where:

$$X_1 \cap X_2 \cap X_3 = \phi$$

implying that the sets X_1, X_2, X_3 are disjoint and do not intersect. Each specific control belongs to one and only one set and cannot belong to any other set.

5.2.2.3 Information Security Standards

Let s_k be an information security standard.

Furthermore:

$S=\{s_1, s_2, s_3, s_4, \ldots\ldots, s_k\}$ this is a set of all information security standards.

where:

s_k consists of the following three subsets:

$X_1^{S_k}$ denotes broad administrative controls

$X_2^{S_k}$ denotes broad operational controls and

$X_3^{S_k}$ denotes broad environmental controls

and:

$$\{\forall\ X_1^{S_k}, X_2^{S_k}, X_3^{S_k} \mid X_1^{S_k} \subset X_1 \wedge X_2^{S_k} \subset X_2 \wedge X_3^{S_k} \subset X_3\}.$$

Note:

For example: n(S) = 2, S={ISO 27002, BASEL II}

An information security standard for the purposes of the BC3I model may also include other documents such as guidelines and codes of good practice.

5.2.2.4 Weights of Importance of Information Security Standards as viewed by an Organisation

Let $\omega_k^{S_k}$ be the weight of importance of standard s_k as decided upon by an organisation.

Furthermore:

$$0 \leq \omega_k^{S_k} \leq 1\ \forall k\,.$$

Note:

Different organisations perceive and respond to security risks differently. Organisations are exposed to different risks and therefore the information security standards they may want to or have to comply with, will always differ. In addressing these risks, organisations are required to prioritise according to their compliance strategy and business goals.

5.2.2.5 Weights of Importance of Broad Control Categories within each Information Security Standard

Let a_{ki} be the weight of importance within standard s_k of the broad control category subset $X_i^{S_k}$

Furthermore:

$A_k=\{a_{k1}, a_{k2}, a_{k3}\}$, a set of the weights of importance of the broad control categories within an information security standard

and:

$0 \leq a_{ki} \leq 1 \ \forall i,k$.

Note:

Weights of importance are determined by computing how much emphasis is placed on each broad control category by each standard s_k. It is accepted and acknowledged that this is a subjective process and the results depend on the expertise of the person who analyses the standard. However, it should be viewed as discovering certain trends found in standards as opposed to ascertaining factual information. For example, the ISO 27002 standard consists of a total of 138 controls, of which 31% are in the X_1 (administrative), 54% in the X_2 (operational) and 14% in the X_3 (environmental) control category. It has already been acknowledged that someone else might have a different view. If this standard is denoted as s_1 then:

$A_1=\{0.31, 0.54, 0.14\}$

5.2.2.6 The Universal Set of Broad Control Category Costs

Let X_{ic} be the total cost associated with broad control category X_i.

and:

x_{ijc} is the cost of control x_{ij}

Furthermore:

$U_c = \{X_{1c}, X_{2c}, X_{3c}\}$.

Note:

The total cost for each broad control category is calculated as follows:

$$\overline{X_i^c} = \sum_{i=1}^{3} \sum_{j=1}^{l \vee n \vee m} x_{ijc}$$

5.2.2.7 Cost Indicators

Let $\underline{X_i^c}$ be the cost indicator for the monetary amount to be spent on applicable/appropriate controls, as selected by an organisation from the broad control category set X_i.
Furthermore:

$$\underline{X_i^c} < \overline{X_i^c} \quad \forall i \,|\, 1 \leq i \leq 3$$

5.2.2.8 Budget

Let ***B*** be the monetary amount (budget) to be spent on the implementation of security controls.
Furthermore:

$\overline{B}$ is the total budget, should all the controls within all broad control categories be implemented.

$\overline{B}$ is calculated as follows:

$$\overline{B} = \sum_{j=1}^{l} x_{1\,jc} + \sum_{j=1}^{m} x_{2\,jc} + \sum_{j=1}^{n} x_{3\,jc}$$

and:

$\underline{B}$ is the total budget for the selected controls, i.e. those controls viewed as appropriate/applicable by an organisation.

$$\underline{B} < \overline{B}$$

5.2.2.9 Potential Loss

Let ***P*** be the total expected potential loss expressed as a monetary amount.

Note:

B should somehow be related to the expected potential loss (***P***). There are several ways to compute ***P***, but its computation is outside the scope of this research.

5.2.3 Constraints

5.2.3.1 Budget (B) Constraints

For the BC3I model the cost effective ***B*** is based on the G&L model, which stipulates that not more than 37% of the expected potential loss ***P*** should be spent on implementing controls to secure information assets (Gordon & Loeb, 2002). This percentage can however be changed and is dependent on the risk profile of an organisation. Budget constraints clearly support the implementation of cost effectiveness as one of the BC3I model requirements (Requirement 4).

Therefore:

$\underline{B}$ = (37/100) ***P***

5.2.3.2 Non-negativity Constraints

There are either zero or more controls in place (never less than zero). Hence, the model considers non-negativity constraints on the weight of importance of broad control categories within a standard; weight of importance of a standard as viewed by an organisation; cost indicators; unknown cost variables and cumulative costs.

$0 \leq a_{ki}$, $\omega_k^{S_k} \leq 1$ and $\underline{X_i^c}, \overline{X_i^c} \geq 0 \quad \forall k, i$

The next section describes the objectives of the BC3I model.

5.2.4 The objective

The overall objective of the BC3I model is to determine cost indicators for an appropriate set of controls that consists of a mix of administrative ($\underline{X_1^c}$), operational ($\underline{X_2^c}$) and environmental ($\underline{X_3^c}$) controls.

In an ideal world (utopian world) where organisations are required to comply with a number of regulatory mandates, it would be preferable to implement all the controls as depicted in all the relevant mandates of all the three broad control categories, yet within the budget for security which is related to the overall potential loss. Thus:

$$\overline{X_1^c} + \overline{X_2^c} + \overline{X_3^c} = \overline{B}$$

Due to the cost of controls and the magnitude of controls available, this is an impractical scenario. Hence, organisations need to select only the relevant and applicable/appropriate controls. This is also where the fourth requirement comes in on the cost effectiveness of information security budget.

The objective of the BC3I model can thus be stated as follows:

$$\underline{\delta X_1^c} + \underline{\beta X_2^c} + \underline{\gamma X_3^c} \leq \underline{B}$$

where:

δ, β and γ are the coefficient weights of importance of the broad control categories as viewed by an organisation.

Note:

The inequality supports the cost effectiveness of an information security budget. As minimal as the budget can be, the fourth requirement (Requirement 4) stipulates that it should span all the broad controls categories. The inequality also supports the implementation of a holistic approach (Requirement 2) as one of the BC3I model requirements. The information security implementation strategy should include the administrative, operational and environmental control measures and within a cost effective budget. The coefficients support the requirement

about the model being cognisant of business goals (Requirement 1). Depending on the strength of on organisation information security, different organisations will put emphasis on the controls that will best support its business goals.

5.2.5 Determining values for $\underline{X_1^c}$, $\underline{X_2^c}$ and $\underline{X_3^c}$

Requirement 3, namely flexibility of the BC3I model, states that different organisations put different weights of importance on different standards, depending on the type of organisation as well as its business objectives. The BC3I model provides some degree of flexibility, which makes it adjustable to individual circumstances in terms of the following:

- Its applicability to various organisations from different sectors
- The standards to be considered
- The weight of importance of standards to organisations

The modelling of this requirement is as follows:

$\omega_k^{S_k}$ denotes the weight of importance for implementing the controls of a specific standard s_k by an organisation. Thus the security budget (***B***) is dependent on $\omega_k^{S_k}$ and hence

$\underline{B} \propto \omega_k^{S_k} \boldsymbol{B}$ ($\underline{B}$ is directly proportional to ***B***).

Requirement 2 of the BC3I model states that a holistic approach is required. Therefore, standards that are chosen for implementation in an organisation need to be considered, depending on the emphasis placed by that standard on controls coming from the administrative, operational and environmental sets. The modelling of this requirement is as follows:

Each standard s_k puts different weights of importance a_{ki} on different broad control categories X_i. Therefore, for each standard s_k the unknown cost variable X_i^c of each broad control category X_i is dependent on a_{ki} and their relationship to the cost indicators $\underline{X_i^c}$ is as shown below:

$\underline{X_i^c} \propto a_{ki} X_i^c$ ($\underline{X_i^c}$ is directly proportional to X_i^c)

The following is a generalised representation of the BC3I model:

$$\sum_{k=1}^{f} \sum_{i=1}^{3} a_{ki} X_i^c \leq \omega_k^{S_k} \boldsymbol{B}; \quad \forall i | 1 \leq i \leq 3 \text{ and } \forall f | 1 \leq k \leq f \qquad (1)$$

where:

X_i^c is the unknown cost variable for each broad control category X_i and $X_i^c \geq 0 \ \forall i$

a_{ki} is the weight of importance of a broad control category as reflected in an information security standard $0 \leq a_{ki} \leq 1 \quad \forall k, i$

$\omega_k^{S_k}$ is the weight of importance of each standard s_k as viewed by an organisation

B is the budget taking as input ***P*** the potential loss, using the G&L model (***B*** = 37% of ***P***)

And f is the number of all the standards to be considered by an organisation.

A system of linear inequalities derived from (1) is as follows:

$a_{11} X_1^c + a_{12} X_2^c + a_{13} X_3^c \leq \omega_1^{S_1} \boldsymbol{B}$ for $s_1 \in S$

$a_{21} X_1^c + a_{22} X_2^c + a_{23} X_3^c \leq \omega_2^{S_2} \boldsymbol{B}$ for $s_2 \in S$

$a_{31} X_1^c + a_{32} X_2^c + a_{33} X_3^c \leq \omega_3^{S_3} \boldsymbol{B}$ for $s_3 \in S$

. + . + . ≤ .

. + . + . ≤ .

$a_{k1} X_1^c + a_{k2} X_2^c + a_{k3} X_3^c \leq \omega_k^{S_k} \boldsymbol{B}$ for $s_k \in S \qquad 0 \leq a_{ki} \leq 1 \quad \forall k, i \qquad (2)$

Taking any three (or more) information security standards, we can now rewrite (2) as follows:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} X_1^c \\ X_2^c \\ X_3^c \end{bmatrix} \leq \begin{bmatrix} \omega_1^{S_1} B \\ \omega_2^{S_2} B \\ \omega_3^{S_3} B \end{bmatrix}$$

subject to:

$X_i^c \geq 0$ and $0 \leq a_{ki} \leq 1 \quad \forall i, k \qquad (3)$

The coefficient weights of importance (i.e. δ, β and γ) together with the results of the system of linear inequalities (3) i.e. $\underline{X_i^c}$ can then be used in the objective function $\underline{\delta X_1^c} + \underline{\beta X_2^c} + \underline{\gamma X_3^c} \leq \underline{B}$ to determine the actual amount to be spent in all the types of controls to be implemented. This should be less or equally to the stipulated cost-effective budget in a particular organisation. The next section outlines some of the model's limitations.

5.2.6 Limitations

Just like all other models come with some limitations, the BC3I model has limitations too.

- Firstly, it does not address the interdependences and sequence of implementing information security controls. To illustrate the point on information security control interdependencies, consider the case of an online banking system; it would be useless to implement very strong authentication and authorization measures if the sensitive client information is stored in an unsecured server and is transmitted in clear text without any encryption over an unsecured network. Taking a similar case to that of an online banking system, the first point to secure would be the storage, then the access point and finally the network. If one of these points is not secured, it makes the entire system vulnerable.

- Secondly, even though the BC3I model uses results of the G&L model of an optimal information security investment, it is not necessarily an optimised information security budgeting strategy, but only a guide towards one.

- Thirdly, it puts more emphasis on compliance mandates, yet "compliance" does not guarantee "security"; it is just a good starting point but not enough to achieve the illusion of perfect security (Christodonte, 2008; Kilcourse & Rowen, 2007). Compliance to standards provides a baseline or minimal level of security and is not enough to keep organisations safe.

- Another limitation is that the BC3I model follows the "garbage-in garbage-out strategy"; it can only provide appropriate results if appropriate inputs have been supplied. Further research could extend this research by addressing these limitations.

5.3 Conclusion

As regulatory compliance continues to be the main driver for the increasing information security spending, it becomes vital for decision makers to ensure that regulatory mandates are taken into considerations in drafting information security budgets. To this purpose, the BC3I model shows how to determine cost indicators for a cost effective information security budget across multiple standards and/or regulations. The cost indicators are derived from the weights of importance of standards, as well as the organisational views of such standards, and must be in accordance with business goals and objectives. Moreover, they are tightly linked to the overall information security budget and based on the G&L model of an optimal security investment. The cost indicators reflect how and where specifically to focus information security budget across multiple standards and/or regulations in order to achieve a cost effective information security strategy.

A thorough breakdown of the information security budget according to the cost indicators can provide good guidance to information security managers as they seek to establish a consistent set of controls across all the broad control categories derived from relevant standards. This can be argued to be a good start towards the selection of appropriate controls to cost effectively protect organisations' information assets and simultaneously achieve compliance to a number of regulatory mandates. The next chapter provide a real-world scenario of the implementation of the BC3I model.

Chapter 6

Proof of Concept - Application of the BC3I Model

6.0 Introduction

This chapter provides scenarios to illustrate the application of the BC3I model, as proof of concept. The main goal is to show that the BC3I model's results are not only theoretically, but also practically sound and are applicable in the real-world scenarios. The model is illustrated for a fictitious organisation A which is from the financial sector; being the hardest hit by the economic crisis. The financial sector is chosen because of its high reliance on information security for obvious reasons; the financial sectors deals with money and confidential customer information. Furthermore, the model has been discussed and reviewed by industry experts from the financial sector.

This chapter is structured as follows: Section 6.1 explains the steps to be followed when applying the BC3I model. Section 6.2 discusses the background of the fictitious organisation that is used as a case study and the first scenario. Sections 6.3 and 6.4 discuss the second and third scenarios respectively. Section 6.5 outlines the reviews of the industry experts and section 6.6 provides concluding remarks.

6.1 Steps to Apply the BC3I Model

The activity diagram below illustrates all the necessary steps that an organisation needs to follow in order to correctly apply the BC3I model.

Activity Diagram for the BC3I Model

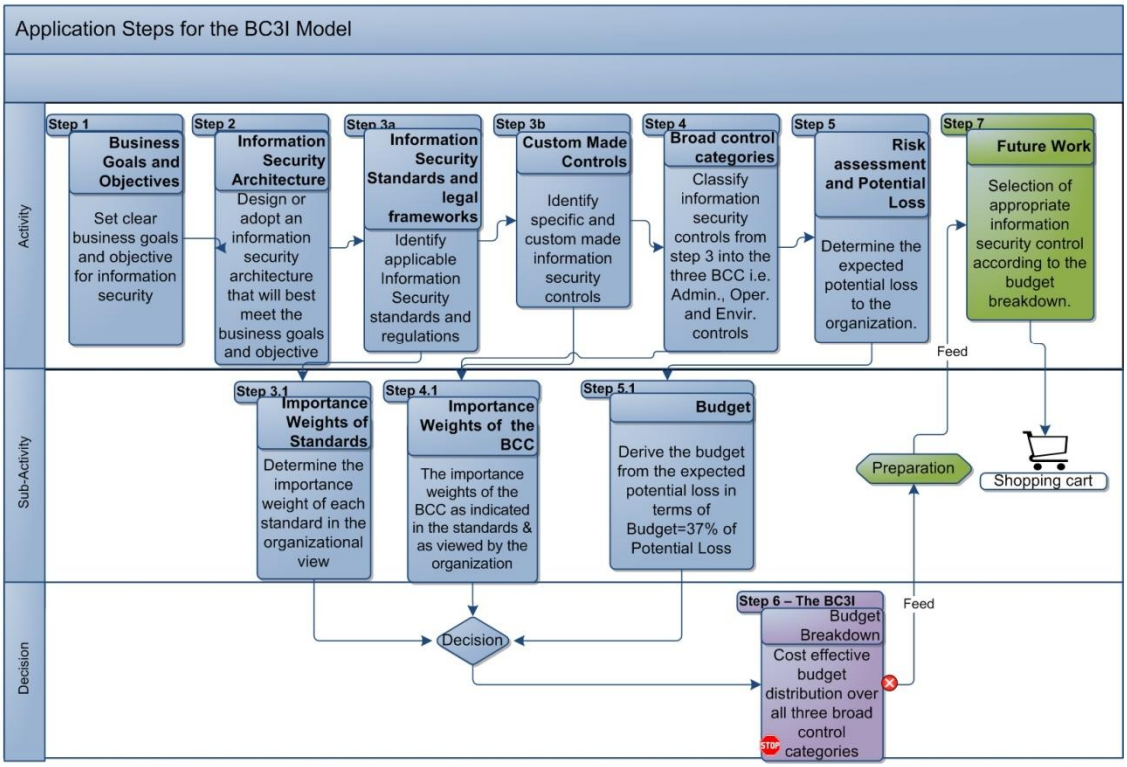


Figure 6.1: Activity diagram for the BC3I model

Figure 6.1 has three different layers i.e. activity, sub-activity and decision layers. This follows a sequential top-down approach starting from business goals and objectives from which information security goals and objectives are derived. It follows then that the information security team design or adopt an information security architecture that will best achieve the stated goals and objectives. This is followed by the identification of applicable and relevant information security standards along with custom made controls. The next activity is to classify the controls from the standards and custom-made controls into the three broad control categories i.e. Administrative, Operational and Environmental controls. A risk assessment must be conducted to determine the potential loss to the organisation due to threats.

Step 3a, 3b, 4 and 5 feeds into the next layer which is sub-activities. In the sub-activity layer, the activities occur in parallel not sequentially and there are no links between them. Step 3.1, 4.1 and 5.1 are then put into a linear programming model as variables to compute the overall budget

breakdown over the three broad control categories in the decision layer. Equipped with the budget breakdown, an information security manager can then prepare for the selection of the appropriate controls to buy. In order to further unpack the activity diagram, the following sub-sections briefly discuss each of the steps with respect to the fictitious organisation A.

6.2 Case Study – The Background of Organisation A

Organisation A is a financial institution operating in South Africa, which is one of the world's fast emerging economies along with Brazil, Russia, India and China. Organisation A's main line of business is banking, investments, lending, mortgage, and credit and debit card facilities. Organisation A has been operating in South Africa for the past 25 years and boasts a proven track record. Organisation A has 60 000 employees working in its 35 main branches and has 3500 automatic teller machines spread across South Africa's nine provinces. Their headquarters are located in Johannesburg. This organisation targets the middle and upper class market segment. Organisation A's vision is to become the bank of choice and help create a better world for all. Several business goals and objectives have been put forward to achieve this vision.

6.2.1 Step 1: Business Goals and Objectives

Organisation A has set clear and achievable business goals and objectives based on their overall vision. The business goals and objective form the basis for the specific information security goals and objectives. For instance;

Vision

- To become the bank of choice and help create a better world for all

Overall Business Goals and Objectives

- Expand into new target market segment
- Improve and sustain customer growth
- Deliver the fastest profit growth consistently and sustainably
- Embrace and participate in community development projects for the disadvantaged communities.

Information Security Goals

- Organisation A's first goal is to implement a cost effective information security program.
- The second goal is for Organisation A to implement a holistic information security strategy that seeks to minimize the risk posed by people, processes and technology on its business information assets.

Information Security Objectives

- In line with the first information security goal, organisation A's information security strategy must reduce threats by 50% by the end of the 2010 fiscal year.
- The second objective is to be at least 50% compliant with the key information security standards for the financial sector by the end of 2010 fiscal year.

Figure 6.2 illustrates the relationships between the overall business goals and objectives, and the information security goals and objectives to achieve the vision of organisation A.

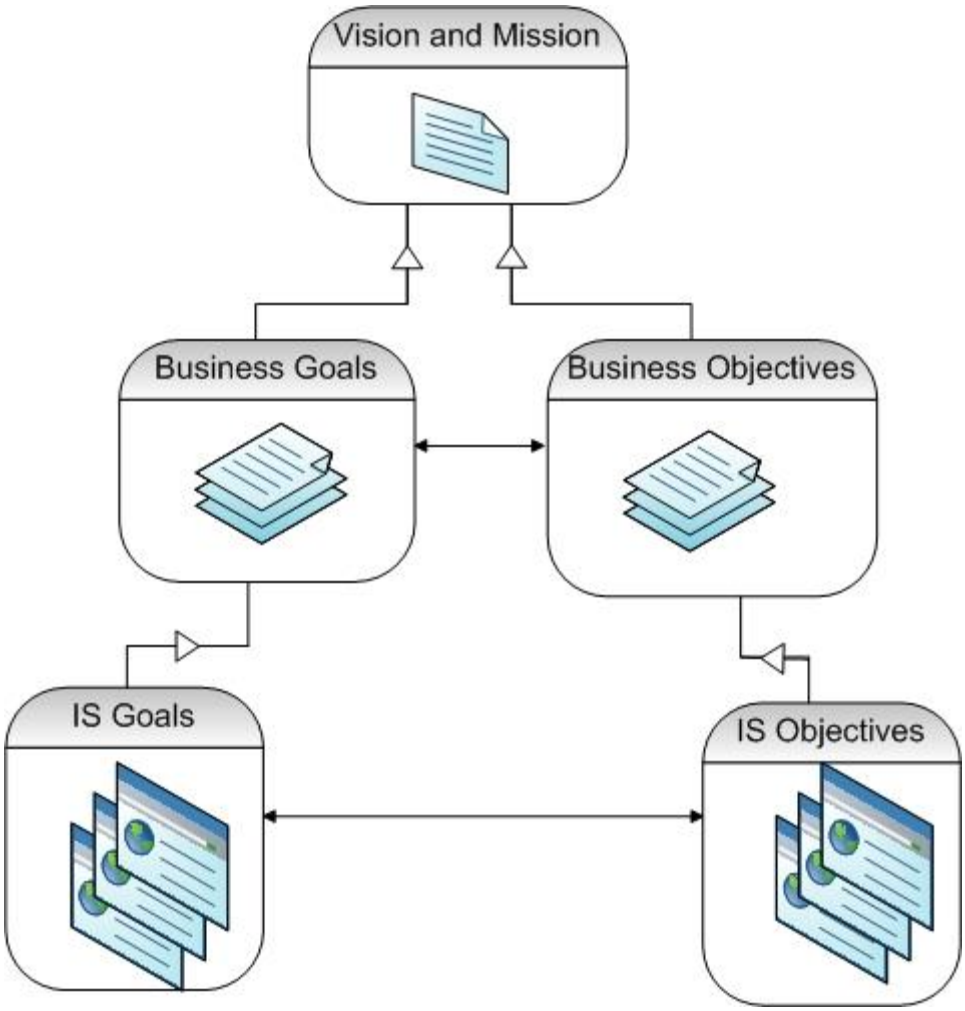


Figure 6.2: Relationships of the information security goals and objectives, business goals and objectives with the vision of organisation A

From the above, it is then vital to design or adopt an information security architecture to ensure that the information security goals and objectives are met. The next sub-section highlights the architecture that is to be considered.

6.2.2 Step 2: Information security architecture

The implementing organisation must then go on to design or adopt an information security architecture based on and in line with their business goals and objectives. Organisation A decides to adopt Killmeyer's information security architecture with five components i.e. security organisation/infrastructure security policies, standards and procedures; security baseline and risk

assessment; security awareness and training program and compliance which are in line with their business goals and objectives (Killmeyer, 2006). Implementing this architecture will best achieve the vision of organisation A.

6.2.3 Step 3: Standards, legal and regulatory frameworks and custom made controls

Harsh regulatory compliance penalties have ensured that compliance takes precedence in most of today's organisations. For this reason, organisations must identify applicable and relevant information security standards and regulations that they are to be compliant with so as to avoid the penalties.

In the case of organisation A which is from the financial sector, there are a number of applicable standards and/or regulations, such as the Basel II Framework; ISO 27002; PCIDSS (Payment Card Industry Data Security Standard); ISF (Information Security Forum; The Standard of Good Practice); Sarbanes-Oxley Act of 2002 (SOX); Gramm-Leach-Bliley Act (GLBA) and Financial Information Security Management Act (FISMA). The ideal situation is for organisation A to try and comply with all these standards among others. However, as already mentioned in the previous chapter, this is impractical as it assumes unlimited financial resources.

Within this elusive goal of complying with all the standards, organisation A is required to identify a set of relevant and applicable standards that best fit and apply to its context and have direct effect on its bottom line. For this reason organisation A can choose to comply with only a subset of these standards that best meet their goals and objective.

Assume for illustration purposes that organisation A has chosen to implement two standards, namely ISO 27002 and PCIDSS. The controls prescribed therein only form a baseline for an information security program; they do not guarantee a secure business environment. Over and above the prescribed controls, organisation A decides to also identify custom-made controls that are specific to their business environment in order to complement the prescribed controls. This

would ensure that organisation A gain a competitive edge to stay ahead of their competitors; who only implement the prescribed controls.

6.2.4 Step 4: Broad control categories

For modelling purposes, organisation A must classify the prescribed information security controls from the standards and regulations, along with the custom made controls into the three broad control categories i.e. Administrative, Operational and Environmental controls. The table below is an extract of this classification for the ISF standard of good practice for information security and a full classification can be found in Appendix A.

Table 6.1. An extract of the classification of the broad control categories for the ISF standard of good practice for information security of 2007

Principle	Administrative Control	Operational Control	Environmental Control
CI4.5 User Authentication		✓	
CI5.1 Local security co-ordination	✓		
CI5.2 Security Awareness		✓	
CI5.3 Information Classification	✓		
CI5.4 Information risk analysis	✓	✓	
CI5.5 Security Audit		✓	
CI6.1 Contingency plans	✓		
CI6.2 Contingency arrangements	✓		
CI6.3 Validation and maintenance		✓	
NW1.1 Role and responsibilities	✓		
NW1.2 Network design		✓	
NW1.3 Network Resilience			✓
NW1.4 Network documentation	✓		
NW1.5 Service providers	✓		
NW2.1 Configuring network devices		✓	

One could also adopt an already existing classification. However, due to the subjectivity of this exercise, it is not advisable to do so.

6.2.5 Step 5: Risk assessment and potential loss

Organisation A is required to conduct a risk assessment exercise to determine the potential loss expected if the risks were to materialize and also to determine the amount of risk that the organisation is willing to accept. As mentioned in the previous chapter (chapter five), this exercise is however, out of the scope of this research. It is only fair then to assume that after organisation A has done this exercise they come to conclude that their potential loss expected is $10 000 000.00.

6.2.6 Step 3.1: Determine the Weights of Importance of the Standards as viewed by the Organisation.

The next step is to determine the weights of importance of each standard within the organisation. This is linked to the legal and regulatory compliance environment and non-compliance penalties thereof, which greatly influence organisation A's weighting of standards. The decision would also be influenced by the second business objective; i.e. Organisation A must be at least 50% compliant with the key information security standards for the financial sector by the end of 2010 fiscal year. In a scale of zero to one, assume that organisation A's weight of importance for standards s_1 and s_2 are:

$\omega_1^{S_1}$ = 0.3 and $\omega_2^{S_2}$ = 0.4. Moreover, the organization also determines the weight of importance of the custom made controls which for illustration purposes is called s_1 to be $\omega_3^{S_3}$ = 0.3.

6.2.7 Step 4.1: Determine the Weights of Importance of the Broad Control Categories within Standards.

This step computes the weights of importance of each broad control category within each information security standard and the custom made controls.

The ISO 27002 (denoted s_1) standard consists of a total of 133 controls, of which 31% are in the X_1 (administrative), 55% in the X_2 (operational) and 14% in the X_3 (environmental) control category as shown in appendix A.

The PCIDSS (denoted s_2) consists of 189 controls, of which 25% are in category X_1, 59% in X_2 and 15% in X_3 as shown in appendix B.

Assume that organisation A has 12 custom-made controls (denoted s_3) that are specific to its business and that 35% of these controls are in category X_1, 30% are in category X_2 and 35% are in category X_3. The summary is shown in the following table.

Table 6.2. The weights of importance of the broad control categories within standards.

Standards	**Administrative Controls %**	**Operational Controls %**	**Environmental Controls %**
ISO 27002	31	55	14
PCIDSS	25	59	15
Custom made	35	30	35

In summary:

With $0 \leq a_{ki} \leq 1$, a_{ki} being the weighting of the broad control categories as indicated in the standards; then the left-hand side of the system of linear inequalities becomes:

$0.31\,X_1^c + 0.55\,X_2^c + 0.14\,X_3^c \quad s_1$

$0.25\,X_1^c + 0.59\,X_2^c + 0.15\,X_3^c \quad s_2$

$0.35\,X_1^c + 0.30\,X_2^c + 0.35\,X_3^c \quad s_3$

6.2.8 Step 5.1: Determine the Overall Security Budget

Next it is necessary to determine the budget that organisation A is willing to spend on its information security program. Having done a risk assessment and analysis, they identified an overall potential loss estimated to be $10 000 000. Using the G&L model, organisation A needs to spend at most 37% of this amount on its security budget i.e. $3 700 000.00.

Therefore, the right-hand side of the system of linear inequalities becomes:
0.3 x 37/100 x $10 000 000 = $1 110 000
0.4 x 37/100 x $10 000 000 = $1 480 000
0.3 x 37/100 x $10 000 000 = $1 110 000

6.2.8.1 Step 5.1.1: The System of Linear Inequalities

The following is a system of linear constraint inequalities:

$$0.31\,X_1^c + 0.54\,X_2^c + 0.14\,X_3^c \leq \$1\ 110\ 000$$

$$0.25\,X_1^c + 0.59\,X_2^c + 0.15\,X_3^c \leq \$1\ 480\ 000$$

$$0.35\,X_1^c + 0.30\,X_2^c + 0.35\,X_3^c \leq \$1\ 110\ 000 \qquad (1)$$

6.2.8.2 Step 5.1.2: The Objective Function

This step determines the weight of importance of each broad control category as viewed by the organisation. This should also be aligned with the business goals and objectives. On a scale of one to ten, organisation A's weights of importance for each broad control category X_1, X_2 and X_3 are:

δ= 2.3, β= 5.5 and ɤ= 2.2 respectively.

δ, β and γ are the coefficient importance weights of the broad control categories as viewed by an organisation.

Then the objective function becomes:

$$2.3\underline{X}_1^c + 5.5\underline{X}_2^c + 2.2\underline{X}_3^c \leq 3\ 700\ 000 \text{ (37\% of \$10 000 000.00)} \qquad (2)$$

Modelling with (1) and (2) we obtain the results in the following sub-section.

6.2.9 Step 6. Discussion of the Results for Organisation A

The following are the results of applying the BC3I model.

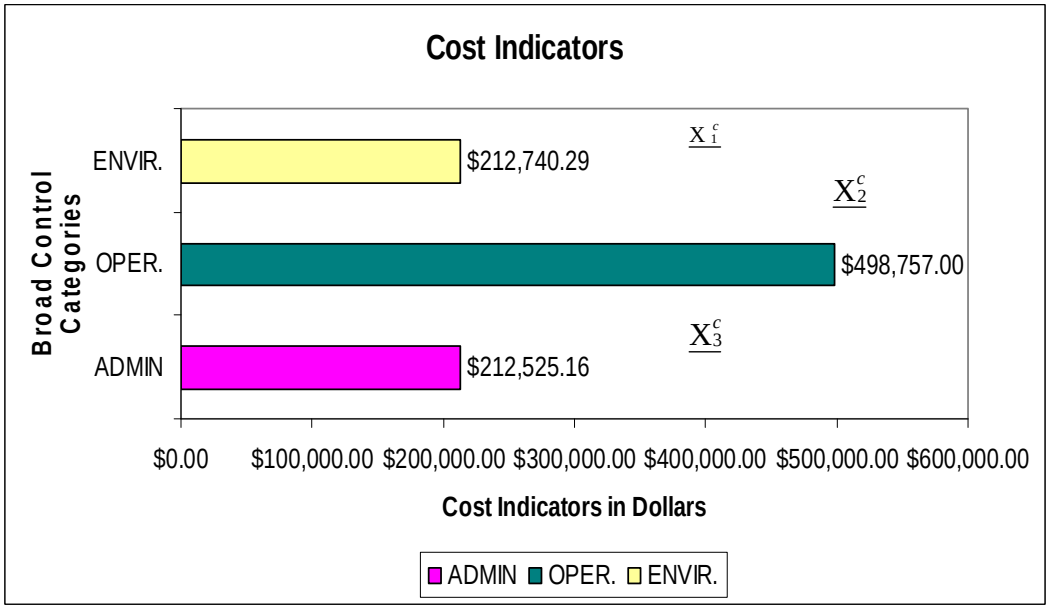


Figure 6.3: Cost indicators for each of the broad control categories in organisation A

Figure 6.3 shows that the Operational controls take the bigger share with $498 757.00, followed by Administrative controls at $212 740.29 and Environmental controls at $212 525.16. However, this is before taking into consideration the weight of importance for each broad control as viewed by the organisation in the objective function. The latter is a critical factor, considering the fact that organisations (depending on their line of business and preferences) place different emphasis on different types of controls. This also explains the subjective nature of the whole exercise.

The cost indicators after taking into consideration the weights of importance as viewed by the organisation in the objective function are illustrated in Figure 6.4.

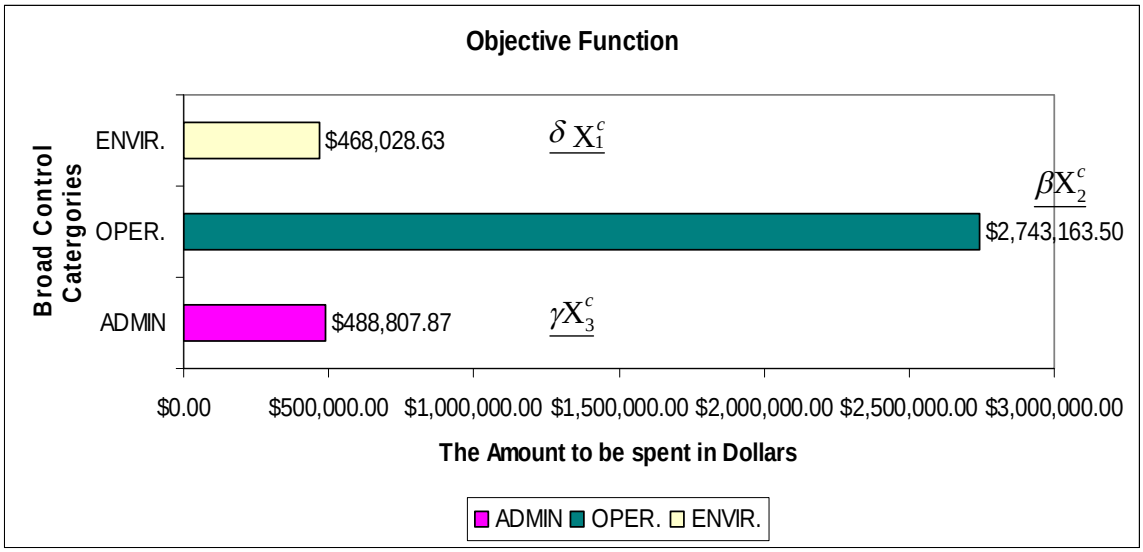


Figure 6.4: The proportional amounts to be spent on each of the broad control categories in organisation A

After applying the weights of importance as viewed by the organisation, Operational controls still take a bigger share of the budget at $2 743 163.50 This is now followed by Administrative controls at $488 807.87 instead of Environmental controls, which now come in last at $468 028.63. According to the results, organisation A puts more emphasis on Operational than on Administrative and Environmental controls.

6.3 Scenario Two

Now consider organisation A using the same standards and custom made controls. They follow the same procedure as in the scenario one; which basically means most of the variables remain unchanged. But on top of the other information security goals and objectives i.e.:

Goals

- Organisation A's first goal is to implement a cost effective information security.
- The second goal is for Organisation A to implement a holistic information security strategy

that seeks to minimize the risk posed by people, processes and technology on its business information assets.

Objectives

- The information security strategy must reduce information security threats by 50% by the end of the fiscal year 2010.
- The second objective is that by the end of 2010 fiscal year, Organisation A must at least be 50% compliant with the key information security standards for the financial sector.

They decided to add another goal with a much high priority over the others i.e.

- *Organisation A must increase its competitive edge over their competitors to differentiate itself from its competitors and stay ahead in the financial sector.*

In a bid to achieve the above additional goal along with the other goals and objectives, organisation A decides to change its strategy and put different weightings on the standards and custom made controls. They decide to strengthen and put more emphasis on the custom made controls (s_3) followed by PCIDSS standard (s_2) and lastly the ISO 27002 (s_1) with the ratio of 0.5:0.4:0.1 respectively. Without necessarily changing the standards and hence the weightings of the broad control categories within each one of them, the right-hand side of the system of linear inequalities therefore becomes:

0.1 x 37/100 x \$10 000 000 = \$370 000.00 for s_1

0.4 x 37/100 x \$10 000 000 = \$1 480 000.00 for s_2

0.5 x 37/100 x \$10 000 000 = \$1 850 000.00 for s_3

This new goal has caused changes in priorities and this has resulted to a bigger chunk of the budget shifting towards custom made controls.

The left-hand side of the system of linear inequalities remain unchanged. The only change is on the right-hand side as shown below.

Then the system of linear constraint inequalities becomes:

$0.31\,X_1^c + 0.54\,X_2^c + 0.14\,X_3^c \leq \$370\,000.00$

$0.25\,X_1^c + 0.59\,X_2^c + 0.15\,X_3^c \leq \$1\,480\,000.00$

$0.35\,X_1^c + 0.30\,X_2^c + 0.35\,X_3^c \leq \$1\,850\,000.00$

The system of linear constraint inequalities shows an increase in the budget allocated for the custom-made controls. Furthermore, organisation A decides to choose different weightings of the broad control categories but only in the objective function. Unlike in the first scenario and based on their additional goal they now decide to focus more on the environmental controls than the other two with the following ratio 2.0:2.5:5.5 for Administrative, Operational and Environmental respectively.

Then the objective function becomes:

$$2.0\,\underline{X}_1^c + 2.5\,\underline{X}_2^c + 5.5\,\underline{X}_3^c \leq 3\,700\,000$$

The results of these seemingly minor changes have big ripple effects on the cost indicators and the final results of the model. The next section discusses the results after effecting these minor changes to the importance weights of the standards and importance weights of the broad control categories in the objective function.

6.3.1 Discussion of the Results for Scenario 2

Figure 6.5 presents the results of the changes made by organisation A on the cost indicators.

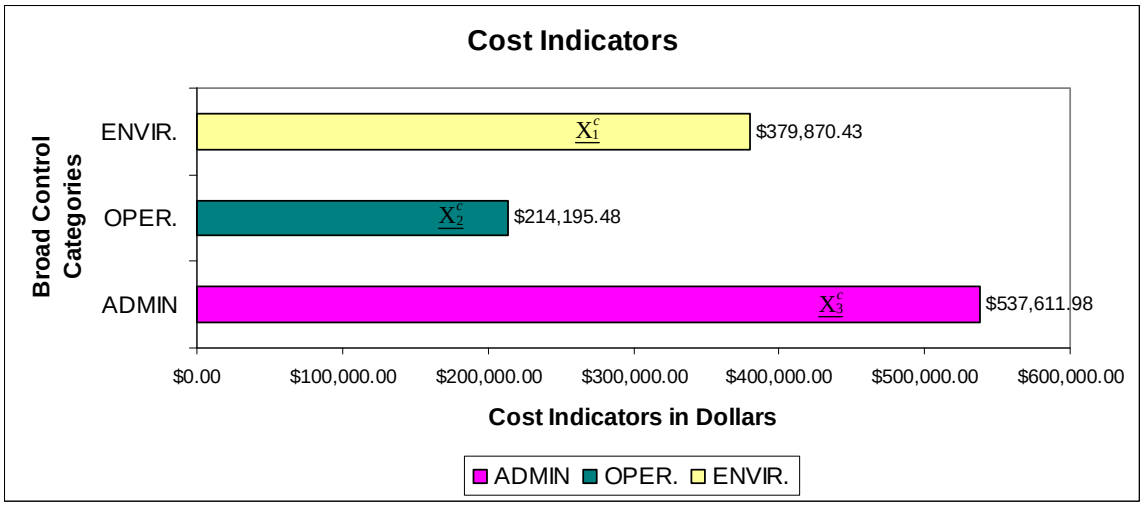


Figure 6.5: Cost indicators for each of the broad control categories in organisation A for Scenario 2

In figure 6.5 the bigger share of the budget ($537,611.98) goes to the Administrative control in terms of the considered standards and custom made controls. This is followed by the Environmental controls at $379,870.43 and then the Operational controls at $214,195.48. However, this is only the cost indicators before the organisation could apply their weightings on each of the broad control categories.

Figure 6.6 depicts the cost indicators after applying the weights of importance of each broad control category as viewed by organisation A in the objective function.

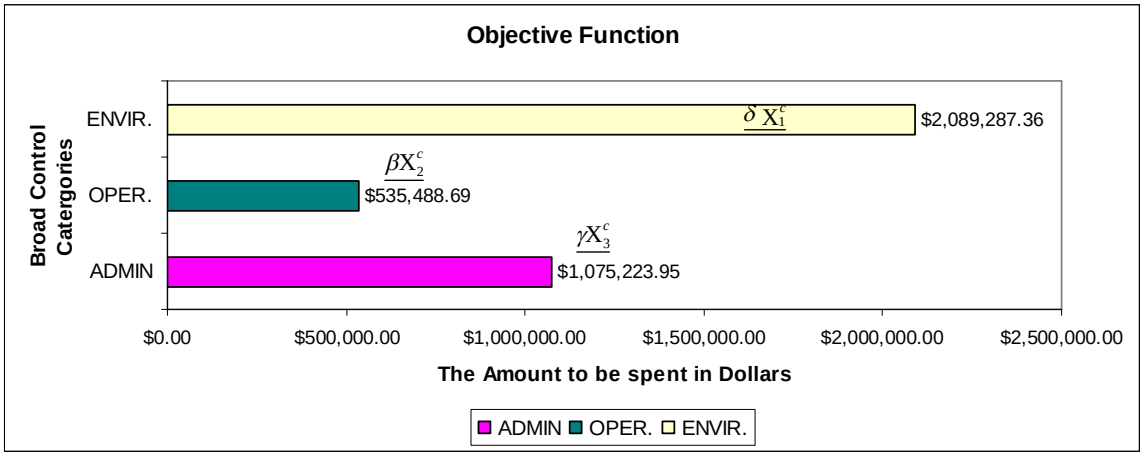


Figure 6.6: The proportional amounts to be spent on each of the broad control categories in organisation A for Scenario 2

Interestingly and also to show the impact of considering the weights of importance on the broad control categories as viewed by the organisation, the Environmental controls take a bigger portion of the budget at $2,089,287.36, followed by the Administrative controls at $1,075,223.95 and lastly the Operational controls at $535,488.69. This is an indication that the weights of importance of the broad control categories as viewed by the organisation contributes significantly to the information security budget decision making process. This also demonstrates the direct effects of business goals and objectives on information security spending.

6.4 Scenario 3

In this scenario, organisation A is subjected to external pressure from the financial regulators to implement and be compliant with the industry's best practices, which is in this case the ISF (Information Security Forum) – the standard of good practice of 2007. This is testing the agility and flexibility of organisation A's budgeting model. It forces organisation A to again change its business goals and objectives and hence its information security strategy. The focus shifts from the custom-made controls back to regulatory compliance with standards; more so to the industry standard of good practice. This is a call for organisation A to again adjust its information security budget accordingly.

The ISF-standard of good practice of 2007 (denoted s_4) consists of 166 controls, of which 38% are in category X_1, 49% in X_2 and 13% in X_3 as shown in appendix B. This additional standard changes the system of linear constraint inequalities. Instead of three, there are now four of them. The left hand side of the system of linear inequalities become:

$$0.31\,X_1^c + 0.55\,X_2^c + 0.14\,X_3^c \quad s_1$$

$$0.25\,X_1^c + 0.59\,X_2^c + 0.15\,X_3^c \quad s_2$$

$$0.35\,X_1^c + 0.30\,X_2^c + 0.35\,X_3^c \quad s_3$$

$$0.48\,X_1^c + 0.49\,X_2^c + 0.13\,X_3^c \quad s_4$$

Keeping all the other variables constant, Organisation A decides to effect changes on the weightings of standards along with that of custom made controls. With compliance regulators behind their back they decide to evenly spread the budget on the standards (s_1, s_2 and s_4) and reduce it on the custom made controls (s_3) in the following ratio; 0.3:0.3:0.3:0.1 respectively. The right hand side of the system of linear constraint inequalities become:

0.3 x 37/100 x \$10 000 000 = \$1 110 000 s_1
0.3 x 37/100 x \$10 000 000 = \$1 110 000 s_2
0.1 x 37/100 x \$10 000 000 = \$ 370 000 s_3
0.3 x 37/100 x \$10 000 000 = \$1 110 000 s_4

Therefore, the entire system of linear constraint inequalities becomes:

$$0.31\,X_1^c + 0.55\,X_2^c + 0.14\,X_3^c \leq \$1\ 110\ 000$$
$$0.25\,X_1^c + 0.59\,X_2^c + 0.15\,X_3^c \leq \$1\ 110\ 000$$
$$0.35\,X_1^c + 0.30\,X_2^c + 0.35\,X_3^c \leq \$\ \ 370\ 000$$
$$0.48\,X_1^c + 0.49\,X_2^c + 0.13\,X_3^c \leq \$1\ 110\ 000$$

The objective function remains constant to the case in scenario one:

$$2.3\,\underline{X}_1^c + 5.5\,\underline{X}_2^c + 2.2\,\underline{X}_3^c \leq 3\ 700\ 000 \text{ (37\% of \$10 000 000.00)}$$

The next section discusses the result after these changes have been made. That is after an additional standard has been added and the standards weightings have also been changed.

6.4.1 Discussion of the Results for Scenario 3

Figure 6.7 below presents the results of the BC3I model after organisation A effected the changes in terms of the cost indicators.

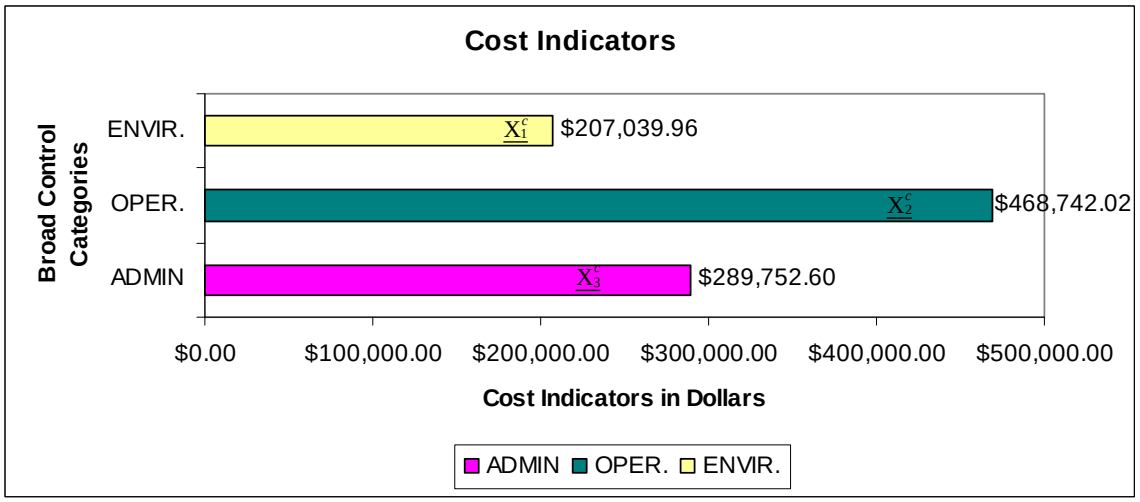


Figure 6.7: Cost indicators for each of the broad control categories in organisation A for Scenario 3

Figure 6.7 shows that most of the budget now goes to the Operational controls ($468,742.02), followed by the Administrative controls ($289,752.60) and lastly the Environmental controls ($207,039.96). This is before organisation A applies their weights of importance on each broad control category.

Figure 6.8 depicts the cost indicators after organisation A has applied the weights of importance of each broad control category on the objective function.

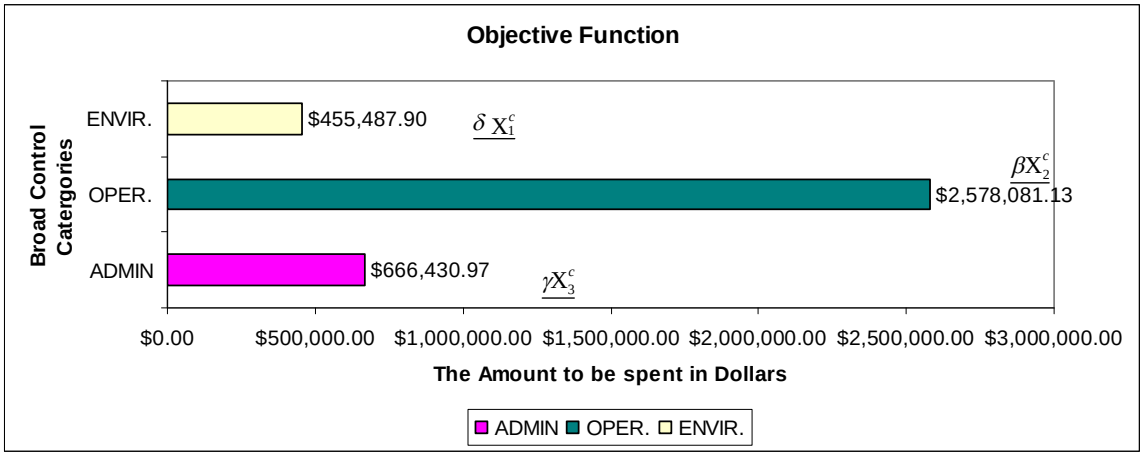


Figure 6.8: The proportional amounts to be spent on each of the broad control categories in organisation A for Scenario 3

Figure 6.8 above shows that most of the budget is directed to the Operational controls at $2,578,081.13 followed by the Administrative controls at $666,430.97 and then the Environmental controls at $455,487.90. These are the effects of adding another standards and changing the weights of importance of the standards, without changing all the other variables. This shows that changing standards has a direct impact in information security budget.

Apart from the above scenarios, the BC3I model has been discussed and reviewed by an industry expert from the financial sector. The next section discusses the industry expert reviews and evaluations.

6.5 Industry Validation of the BC3I Model

In order to put the BC3I model into the financial industry perspective, it was discussed with industry experts from this sector. The discussions were conducted with an information security expert in an investment bank and another information security expert in a commercial bank. The following are their reviews and evaluation on the BC3I model.

6.5.1 Investment Bank Industry Expert

Moving step by step on the activity diagram, the discussions and reviews started with the vision, business goals and objectives, from those the industry expert helped derive the information security goals and objectives (step 1). The expert suggested the linkage between the information security architecture (step 2) and the information security goals and objectives.

In terms of step 3a and 3b i.e. information security standards and legal frameworks and custom made controls respectively, the industry experts also mentioned the issue of subjectivity of the whole exercise of choosing standards to comply with. In most cases, it depends so much on the person who is in charge of the information security team to choose which standards to comply with. In this discussion, the issue of compliance regulatory penalties also surfaced and more emphasis was put on it as another important driver for choosing standards. Standards that carry

huge penalties get a lot of endorsement from most companies. The case of the PCIDSS penalties on financial institutions that deals with card payments was given as an example of a standard with serious penalties.

The industry expert agreed to the use of custom-made controls (step 3b) to gain competitive edge and mentioned that these differ from one environment to another and they also differ from sector to sector. The emphasis on this part was put on going beyond compliance mandates and implementing controls that best minimizes the overall risk on business information and its systems. The inclusion of custom-made controls in the BC3I model is said to be of vital importance.

On step 4 (classification of the broad control categories), the industry expert also raised the issue of subjectivity and mentioned that it allows for flexibility in the model to work in different settings. Very little was discussed on step 5 (risk assessment and potential loss) as risk assessment is outside the scope of this research. However, the linkage of potential loss and risk assessment was emphasised by the industry expert a key to the model.

On step 3.1 (importance weight of standards), the industry expert as in step 3a and 3b emphasised the subjectivity of the exercise which is mainly driven by the preferences of the person who leads the information security team. The subjectivity of this exercise could be minimized by taking the decision as a consensus of team not as an individual.

On step 4.1 (importance weights of the broad control categories), the industry expert agreed with the use of the combination of what is stipulated and prescribed in standards in conjunction with the organisational views which depends on the overall business goals and objectives.

The use of Gordon and Loeb's model results (in step 5.1) on the potential loss was also agreed on by the industry expert, even though this was not extensively dealt with. Putting all these variables together to come up with the overall budget breakdown was agreed to be the right approach.

6.5.2 Commercial Bank Industry Expert

This exercise was also conducted on a step by step approach. The industry expert from the commercial bank expressed concerns on the business goals and objectives along with the information security goals and objectives (step 1). The argument was that it is an ideal thing to base an information security goals and objectives on the overall business goals and objectives. However, the main concern he expressed was that it is very difficult to prove that by achieving the information security goals and objective you would have also made a significant contribution towards addressing and achieving the overall business goals. It is an accepted fact that it is very difficult to quantify the benefits of an information security program and he acknowledged that.

On step two (information security architecture), the commercial bank industry expert wanted to know the meaning of an architecture as it differs in different domains. Otherwise, there were no problems with this step.

On step 3a, the commercial bank industry expert's view was that compliance is not necessarily the main driver for information security spending. He was of the opinion that risk management as a whole is the main driver for information security spending. However, he agreed that it must be included in the process of drafting a budget for information security. He also emphasized the point that compliance does not guarantee security of information assets. He could not agree more on step 3b as the step that ensures organisations go beyond compliance in securing their information and information systems.

He alluded to the subjectivity of step 4 and mentioned that information security risk is probabilistic and one cannot really run away from the subjective nature this exercise. He suggested that this must be acknowledged and stated in clear terms.

On step 5, the industry expert was concerned about the risk assessment exercise which is not really part of this research. He was concerned with the exercise of determining the overall potential loss which, in his opinion, is a very tedious exercise. This step was not covered in details because it is outside the scope of the research.

Step 3.1 focuses on determining the weights of importance of standards as viewed by the organisation. The industry expert agreed on this step and also stated that it is mostly influenced by harsh regulatory penalties. The more penalties an organisation is likely to face if not in compliance, the more emphasis they will put on such a standard. The industry expert also agreed that this also depends on the preferences of the information security team leader.

Step 4.1 on determining the importance weights of the broad control categories was agreed to be an important step especially in combination with the views of the organisation.

On step 5.1, the commercial bank expert argued that it would not make business sense to spend an amount equal to the potential loss expected. However, he was not sure if 37% of the potential loss as stipulated in the Gordon and Loeb model would be enough to protect all risks identified. The industry expert agreed with the way the budget breakdown is determined.

The main problem identified by the commercial industry expert was that the BC3I model seems to be a control based approach to information security. He argued that instead of looking at it in a control based approach, in the real world it would be practical to address this in a risk based approach. Identify the risks an organisation faces and then from these risks, identify the controls to be implemented. He suggested that the control based approach would definitely achieve compliance, but he wondered if it will be enough to cover all risk. Rightly so, the risk based approach is acknowledged as a shortcoming of this research.

Table 6.3: Summary of the industry experts' review answers for the steps of the BC3I model

	Expert 1				Expert 2			
Steps	Disagree	Agree Partially	Agree	Strongly Agree	Disagree	Agree Partially	Agree	Strongly Agree
1			✓			✓		
2			✓				✓	
3a			✓			✓		
3b			✓				✓	
3.1			✓				✓	
4			✓			✓		
4.1			✓				✓	
5		✓			✓			
5.1			✓			✓		
6			✓				✓	

In conclusion and according to the industry experts' reviews and evaluation the BC3I model reflects a true representation of an ideal information security budget breakdown that decision makers need to follow. It includes all the variables that are to be considered to implement a holistic, cost effective and optimal information security program. However, it would make more business sense if it were to be risk based instead of control based.

6.6 Conclusion

As a proof of concept, the three scenarios as discussed illustrate the appropriate approach to correctly implement the BC3I model in an organisation. This has been approved by the industry experts to be a good representation of the real world. These scenarios demonstrates how the BC3I model adapts and respond to changes in business goals and objectives, changes in regulatory compliance in terms of standards that an organisation should comply to and how it deals with changes in custom made controls. These three scenarios have also demonstrated the

flexibility of the model to work in all sorts of different scenarios. From the above it is clear that the BC3I model can make a real contribution in assisting information security managers when making decisions regarding the efficient and cost effective allocation of financial resources to information security activities. The next chapter provides the concluding remarks for the overall research.

Chapter 7

Conclusion

7.0 Introduction

The overall research question in this dissertation is the following: how can one effectively and optimally allocate an information security budget to an appropriate set of controls that has the potential to protect an organisation's information assets in a holistic manner? The main goal is to provide guidance to information security managers as they seek to establish – at a minimum cost – a consistent set of controls across all the broad control categories derived from relevant standards. The current study succeeded in achieving this goal and therefore this dissertation presents the BC3I information security budgeting model as its main contribution and answer to the overall research question. Chapter 7 therefore draws the dissertation to a logical and definite close and makes recommendations for further research.

The structure of this chapter is as follows: Section 7.1 begins with an overview of the contributions of each of the preceding chapters to the overall research goal. Section 7.2 provide a brief discussion on the publications that came out of this research and section 7.3 concludes the research by combining all the individual contributions and providing direction for future work.

7.1 Contributions by each chapter

This section discusses the steps that were taken in each chapter to achieve the overall research goal. The research was divided into two parts, i.e. Part 1 (consisting of Chapters 1, 2 and 3) and Part 2 (consisting of Chapters 4, 5, 6 and 7).

7.1.1 Part 1

Part 1 started off with Chapter 1 that discussed the background of information security spending and provided the rationale for the research, from which the overall research question was derived. To correctly address the main research question, three other subsidiary research questions were formulated:

- What are the current trends in information security?
- How much should be invested in information security?
- To what types of controls and at what proportions should spending in an information security budget be allocated?

(The first and second sub-research questions were answered in Chapters 2 and 3, while the third sub-research question was answered in Part 2, specifically in Chapters 4 and 5).

Chapter 2 discussed the current trends in information security, with the main aim of adopting the current research direction as a point of departure. The findings reflected drastic changes in the threat landscape and showed that the current research direction was moving from fame-driven and harmless attacks to financially motivated and targeted ones. It also showed that today's attacks rather target human beings than information systems. Hence, most of today's information security challenges are predominantly related to the human and organisational aspects of security and not so much to the pure technologies. From the above, it became clear that information security is moving towards a more strategic and multidisciplinary approach, while ensuring adherence and compliance to legal and regulatory mandates.

As part of the findings in Chapter 2, legal and regulatory mandates were discovered to be the main driver for the increase in information security spending. It is therefore vital for decision makers to ensure that legal and regulatory mandates are taken into considerations in drafting information security budgets (as already done in this research). The main purpose of Chapter 2 was to answer the research question, namely ***what are the current trends in information security?***

Chapter 3 reviewed the literature on current state-of-the-art information security management, more specifically the economics of information security. This was done in order to acknowledge existing work and identify gaps to build on within the field of the economics of information security. Within this field, Chapter 3 focused on the work that is being done in information security investment, with particular reference to the cost of an investment. Drilling further down within information security investment, this chapter reviewed literature on an optimal information security investment which leaned slightly more towards the G&L model. The G&L model has contributed significantly to the field of the economics of information security. Because of its contribution and credibility, this research also considered the G&L model in an attempt to answer the question of ***how much should be invested on information security.***

Chapter 3 went on to discuss the cost-effectiveness of information security investments. It was discovered that the current models, methodologies and approaches emerging from the available literature were not satisfactory and required more work if they were to achieve the desired results of an optimal and cost-effective information security budget. From the shortcomings that were identified, it seemed that the current models, methodologies and approaches did not consider the total picture of both the environment and context in which organisations were operating in terms of all-encompassing requirements.

7.1.2 Part 2

Chapter 4 approached and addressed the gaps and problems discovered in Chapter 3 by identifying and outlining the all-encompassing requirements to be considered when preparing information security budgets. The chapter provided these requirements as a requirement elicitation process and they became an input for the development phase of the BC3I model in Chapter 5.

Chapter 5 took due cognisance of the identified all-encompassing requirements for the design and development of the BC3I information security budget model. The BC3I model showed how to determine cost indicators for an optimal and cost-effective information security budget across

multiple standards and/or regulations. The cost indicators were derived from the weights of importance of standards, as well as the organisational views of such standards, and in accordance with the overall business goals and objectives. Moreover, the cost indicators were linked to the overall information security budget and based on the G&L model of an optimal security investment. The cost indicators reflected how and where to focus information security budget across multiple standards and/or regulations in order to achieve a cost-effective information security strategy. Chapters 4 and 5 in conjunction answered the question: ***to what types of controls and at what proportions should spending in an information security budget be allocated?***

Chapter 6 provided three different scenarios to illustrate and demonstrate the application of the BC3I model, as proof of concept. The main goal was to show that the BC3I model's results are not only theoretically but also practically sound and are applicable as demonstrated in the scenarios. The scenarios showed how the BC3I model adapts and responds to changes in business goals and objectives, changes in regulatory compliance in terms of standards that an organisation should comply with, and how it deals with changes in custom-made controls. These three scenarios also demonstrated the flexibility of the model to function in all sorts of different scenarios.

Chapter 6 lastly also provided an expert review of the BC3I model. This model has been approved by industry experts to be a good representation of a real-world situation. The current chapter (Chapter 7) provides concluding remarks based on the overall research and suggestions for future work.

7.2 Publications

As a proof of recognition there are two publications that came out of this research. One is a journal paper and the other is a conference paper. Below are the titles of each of the publications:

- Information security: The moving target (Computers & Security Journal) (Dlamini, Eloff & Eloff, 2009)

- BC3I – Towards requirements specification for preparing an Information Security budget (Information Security South Africa, ISSA 2009 Conference) (Dlamini, Eloff, Eloff & Hone, 2009)

The full papers are listed in Appendix D and E. Below is the brief description of each of these publications. The journal paper (i.e. Information security: The moving target) was meant to identify current trends in information security as a point of departure for this research. This paper investigated the evolution of information security; where it came from, where it is today and the direction in which it is moving. This paper explored literature on past security issues to set the scene. This was followed by the assessment and analysis of information security publications in conjunction with surveys conducted in industry. Results obtained were critically compared and analysed, with the aim of coming up with a comprehensive view regarding the current status of the information security landscape.

The findings showed that information security was indeed a moving target. Its focus was discovered to have shifted from a pure technical approach towards a more strategic and multi-disciplinary approach. Furthermore, this paper highlighted critical information security issues that are being overlooked or not being addressed by research efforts currently undertaken. The need for new research efforts that would minimise the gap between regulatory issues and technical implementations was also reflected in this paper. The findings also identified the need to minimise and mitigate business risk and scrutinise information security spending while ensuring compliance with regulatory mandates. Based on the results of this paper, this research took a strategic and multi-disciplinary approach to address information security budgeting issues and made an effort to minimise the gap between regulatory compliance and technical implementations by considering custom-made controls along with those from information security standards.

The paper titled “BC3I – Towards requirements specification for preparing an Information Security budget” outlined a number of requirements that are to be considered in this research for the design and development of the BC3I model. The main aim in this paper was to provide decision makers with a set of requirements to be considered when implementing a cost-effective

and optimal information security budget; in a manner that preserve organisations' information security posture and compliance status. The BC3I model in chapter 5 was designed based from these requirements.

The next section concludes and provides pointer to the possible future work that could take this research a step further.

7.3 Conclusion and future work

In 2008, world markets experienced an economic crisis. Most organisations froze their expenditure, implemented cost-cutting measures and numerous employees lost their jobs. It became vital for organisations to 'achieve more with less' in order to save their organisations from going bankrupt. In response, this research proposed the BC3I model, which is a step towards 'achieving more with less' within information security budgeting. The crumbling world markets and increased requirements for legal and regulatory compliance made this a timely and relevant research study that addressed a current, spot-on and world-wide problem. The BC3I model as the main outcome of this research has indeed come at the right time.

The BC3I model proposed in this research makes a real contribution towards assisting information security managers when they have to make decisions regarding the optimal and cost-effective allocation of financial resources to information security activities. It can be argued to be a good start towards the selection of appropriate controls to optimally and cost-effectively protect organisations' information assets and simultaneously achieve compliance with a number of legal and regulatory mandates.

Further research is however still needed to show that once information security managers are equipped with an appropriate budget breakdown on the broad control categories, they can go on to put into place appropriate information security measures with the potential to minimise business risks. More work is also required to put greater emphasis on a risk-based approach (this differs from the control-based approach that was followed in this dissertation). The present

research could be extended by devising ways of reducing the subjectivity of choosing standards with which to comply, and by assigning values to the importance weights of standards and broad control categories. In this research the focus was mainly on the cost side of an information security investment; further work is therefore required to focus on the benefit side of an information security investment.

8.0 References

Aceituno, V. (2003), Return on Security Investment, *FIST Conference*, October 2003, Madrid.

Abrams, M.D., Johnson, C.M., Kahn, J.J. and King, S.G. (1998). Considerations for Allocating Resources for Information Security, available at: www.c4i.org/caris.pdf, [accessed February 2009].

ABSA Bank Website, (2009). available online at http://www.absa.co.za/absacoza/, [accessed on 11 February 2009]

Acquisti, A. and Grossklags, J.(2005). Privacy and rationality in individual decision making, *Security & Privacy, IEEE*, 3(1): 26-33

Adkin, R. (2004), An Insurance Style Model for Determining the Appropriate Investment Level against Maximum Loss arising from a Security Breach, The Third Workshop on the Economics of Information Security, available at: http://www.dtc.umn.edu/cgi-bin/seminars.php?eventdesc=207&menu= agenda, [accessed 29 November 2007].

Akerlof, G.A. (1970), The Market for "Lemon": Quality Uncertainty and the Market Mechanism, *The Quarterly Journal of Economics*, 84(3), (Aug. 1970), pp. 488-500.

Anderson, R. (2001). Why Information Security is Hard – An Economic Perspective, the *17th Annual Computer Security Applications Conference*, December 10 -14, 2001, New Orleans, Louisiana, USA.

Anderson, R. (2002). Unsettling Parallels Between Security and the Environment, Paper presented at the Workshop on the Economics of Information Security (WEIS), University of California, Berkeley, May 16 – 17, 2002 available at: http://www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/37.txt [accessed 21 January 2009].

Anderson, R. (2008). Information Security Economics - and Beyond. In Proceedings of the 9th international Conference on Deontic Logic in Computer Science (Luxembourg, Luxembourg, July 15 - 18, 2008). R. Meyden and L. Torre, Eds. Lecture Notes In Artificial Intelligence, vol. 5076. Springer-Verlag, Berlin, Heidelberg, 49-49. DOI= http://dx.doi.org/10.1007/978-3-540-70525-3_5

Anderson, R. (in press), Security Engineering: A Guide to Building Dependable Distributed Systems.

Anderson, R. and Moore, T. (2006). The Economics of Information Security, Science 314(5799), pp.610-613, October 27, 2006.

Anderson, R. and Moore, T. (2007), The Economics of Information Security: A Survey And Open Questions. *The Fourth Bi-annual Conference on the Economics of the Software and Internet Industries*. January 19-20, 2007: Toulouse, France.

Bae, S.H. and Choi, P. (2008), Firms' Optimal Digital Rights Management (DRM) Strategies: The Effects of Public Copy Protection and DRM Compatibility, *The Seventh Workshop on the Economics of Information Security*, available at http://weis2008.econinfosec.org/program.html, [accessed 2 November 2008].

Barclays Bank Website, (2009). available online at http://www.barclays.co.uk/, [accessed 11 February 2009].

Basel II, (2003). Basel Committee on Banking Supervision. April 2003. *"The New Basel Capital Accord"*. Consultative Document

Berinato, S. (2007). The Global State of Information Security 2007: The End of Innocence, *A joint research of CIO and CSO in partnership with PricewaterhouseCoopers*, available at: www.pwc.com/en_BE/be/publications/**state**-of inf**security**-pwc-07.pdf, [accessed 27 November 2007]

Berinato, S. and Ware, L.C. (2005). The Global State of Information Security 2005: A worldwide study conducted by PricewaterhouseCoopers and CIO Magazine, *PricewaterhouseCoopers and CIO Magazine*, September 2005, available at: http://findarticles.com/p/articles/mi_kmcio/is_200509/ai_n15358341/, [accessed 04 November 2007]

Bodin, L.D., Gordon, L.A. and Loeb, M.P. (2005). Evaluating Information Security Investments Using the Analytic Hierarchy Process, *Communications of the ACM*, February 2005, 48(2), pp. 79 – 83.

Bohme, R. (2005), Cyber-Insurance Revisited, *The Fourth Workshop on the Economics of Information Security*, available at http://infosecom.net/workshop/schedule.php, [accessed 27 November 2007].

Bolot, J. and Lelarge, M. (2008), Cyber Insurance as an Incentive for IT Security, *The Seventh Workshop on the Economics of Information Security*, available at: http://weis2008.econinfosec.org/program.html, [accessed 2 November 2008].

Botha, R.A. and Gaadingwe, T.G. (2006), Reflecting on 20 SEC Conferences, *Computers & Security*, Vol. 25, pp- 247–256.

Brown, R.H., Good, M.L. and Prabhakar, A. (1993). Data Encryption Standard (DES), *Federal Information Processing Standard Publication 46-2, US. National Institute of Standards and Technology, (NIST)*, available at:

http://www.itl.nist.gov/fipspubs/fip46-2.htm, [accessed 04 November 2009].

Buck, K., Das, P. and Hanf, D. (2008). Applying ROI Analysis to Support SOA Information Security Investment Decisions, *The Proceedings of the 2008 IEEE Conference on Technologies for Homeland Security*, 12-13 May 2008, pp. 359-366.

Butler, S.A. (2003). Security Attribute Evaluation Method, PhD Thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA.

Cable, J. (2007). INPUT: Federal IT Security Spending to Reach $7.4 billion by 2012, Reston Va. Based INPUT, available at: http://www.govpro.com/News/Article/70706/, [accessed on 14 July 2008].

Camp, L.J. (2006). The state of Economics of Information Security, *I/S: Journal of Law and Policy*, 2(2), pp. 189-205.

Carey, L. (2008). The Evolution of Computer Virus and Anti Virus Protection, Available online at: http://www.identitytheftsecrets.com/the-evolution-of-computer-viruses-and anti-virus-p.html, [accessed 14 July 2008].

Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. (2005). Emerging Issues in Responsible Vulnerability Disclosure, *The Fourth Workshop on the Economics of Information Security*, available at http://infosecom.net/workshop/schedule.php, [accessed 27 November 2007].

Challappa, R. and Sin, R. (2008). Competition for Information under Privacy Concerns, *The Seventh Workshop on the Economics of Information Security*, June 25 -28, 2008, The Center for Digital Strategies, Tuck School of Business at Dartmouth College, Hanover, USA.

Chapman, G. (2009). Cybercrime losses top $US1 trillion, available at:http://www.australianit.news.com.au/story/0,24897,24997483-24169,00.html, [accessed 19 February 2009]

Choi, J.P., Fershtman, C. and Gandal, N. (2007). Network Security: Vulnerability Disclosure Policy, *WEIS 2007 – Sixth Workshop on Economics of Information Security*, Pittsburgh PA, 7-8 June 2007, Carnegie Mellon University, Pittsburgh, USA.

Christodonte, M. (2008). Security Beyond Compliance: A Proactive and Customized Security Framework, available at: http://www.searchsecurityasia.com/content/security-beyond-compliance-proactive-and-customized-security-framework, [accessed 12 May 2009].

COBP, (2009). Code of Banking Practice, available at: http://www.banking.org.za/our_industry/code_of_banking_practice/code_of_banking_practice.htm, [accessed 11 February 2009].

Computer Fraud & Security (2007). IDs Sell for Much More than Credit Card Numbers In the Underground, Editorial News, Computer Fraud & Security, 2007(12), pp. 2

Computer Fraud & Security News (2007). UK Police Bust Fraud Gang, Elsevier Ltd,

CompTIA (2008). Trend in Information Security: A CompTIA Analysis of IT Security and the Workforce [online], *Techweb digital library, Information Week Business TechnologyNetwork*, September 2008, available at: http://www.informationweek.com/whitepaper/government/security/trends-in information-security-a-comptia-analysi-wp1223489141665;jsessionid=JHZ4HVSD3S2LTQE1GHOSKHWATMY32JVN?articleID=42800003, [accessed 10 September 2008].

Conner, F.W. and Coviello, A.W. (2004). Information Security Governance: A Call to Action, Corporate Governance Task Force Report of 2004.

Conrad, J.R. (2005). Analyzing Risks of Information Security Investments with Monte-Carlo Simulations, *Fourth Workshop on the Economics of Information Security*, 2-3 June 2005, Kennedy School of Government, Harvard University.

Conray-Murray, A. (2003). Strategies & issues: justifying security spending. Available at: http://www.itarchitect.com/articles/NMG20020930S0002.html; [accessed 18 July 2007]

CSIA (2007). CSIA Compilation of Data Sources for Information on Cyber Security Issues. Available online at www.csialliance.org/resources, [accessed 13 August 2007].

Cybertrust (2005). Justifying Security Spending: How to Make a Business Case for Information Security, Available online at: http://www.cybertrust.com/media/white_papers/cybertrust_wp_security_spending.pdf, accessed 13 August 2007].

Davis, A. (2005). Return on Security Investment – Proving its Worth, *Computer Fraud & Security*, 2005(11).

Denning, E.D. (1999). Information Warfare and Security, ACM Press, United States of America.

Denning, P.J. (1991). Computers Under Attack: Intruders, Worms, and Viruses, Addison-Wesley Publishing Company, United States of America.

Dlamini, M., Eloff, J.H.P. and Eloff, M.M. (2009). Information Security: The Moving Target, *Computers & Security Journal*, 2009, 28(3-4), May – June 2009, pp. 189 – 198.

Dlamini, M., Eloff, J.H.P., Eloff, M.M. and Hone, K. (2009). BC3I – Towards Requirements Specification for Preparing an Information Security Budget, *Proceeding of the ISSA 2009 conference*, School of Tourism & Hospitality (sth), University of Johannesburg, Auckland park, Johannesburg, South Africa, 6th – 7th July 2009.

Dorfman, M. (1997). Requirements Engineering, *Institute of Electrical and Electronics Engineers, Inc*. Software Engineering Institute, Carnegie Mellon University, USA. Reprinted, with permission, from Software Requirements Engineering, Second Edition,

Richard H. Thayer and Merlin Dorfman, eds., pp. 7-22. Los Alamitos, California: IEEE Computer Society Press, 1977.

Eloff, J.H.P. (2005). Computer Science Lecture Notes, University of Pretoria, South Africa.

Eloff, J.H.P. and Eloff, M.M. (2005). Information Security Architecture, *Computer Fraud & Security*, 2005(11), pp. 10-16.

Eppel, N. (2005). Security Absurdity: The Complete, Unquestionable, and Total Failure of Information Security. Available online at http://www.securityabsurdity.com/failure.php, [accessed 16 July 2007].

FNB Website, (2009). First National Bank Website, available online at: https://www.fnb.co.za, [accessed 11 February 2009].

Forte, D. and Power, R. (2004). War and Peace in Cyberspace: The State of Information Security Towards the Close of the First Decade of the 21st Century, *Computer Fraud & Security*, 2007(10), pp. 15-19.

Fratto, M. (2008). 2008 Security Survey: We're Spending More, But Data's No Safer than Last Year, available at: http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=208800942, [accessed 01 October 2008].

Fumey-Nassah, G. (2007). The Management of Economic Ramification of Information and Network Security on an Organization, *Proceedings of the Information Security Curriculum development Conference '07*, September 28 – 29, 2007, Kennesaw, Georgia, USA.

Geer, D. (2002). Making Choices to Show ROI, *Secure Business Quarterly*, (1)2:1-5.

Gelbstein, E (2006). Information Security for Policy Makers: What it means- Why it matters- What to do about it? Available online at http://www.unitarny.org/mm/File/Webinars/Unitar%20eg%20presentation%2030_08.pdf, [accessed 14 August 2007].

Gerber, M. and von Solms, R. (2005). Management of Risk in the Information Age, Elsevier, *Computers & Security*, Vol. 24, pp. 16-30.

Gibbs, N. (2009). 25 People to Blame for the Financial Crisis, *Times Magazine*, available at: http://www.time.com/time/specials/packages/article/0,28804,1877351_1877350,00.html, [accessed 19 February 2009].

Goetz, E. and Johnson, M.E. (2006). Embedding Information Security Risk Management into the Extended Enterprise: An Executive Workshop, *MacNamee Center for Digital Strategies*, Tuck School of Business at Dartmouth University, USA, available at: http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CIO_RiskManage/Overview.pdf, [accessed 18 February 2009]

Gordon, L.A. and Loeb, M.P. (2002). The Economics of Information Security Investments, *ACM Transactions on Information and System Security*, (5)4: November 2002, pp. 438-457.

Gordon, L.A., Loeb M.P., Lucyshyn, W. and Richardson, R. (2006), CSI/FBI Computer Crime and Security Survey 2006 Report, Available online at www.abovesecurity.com/doc/CommuniquesPDF/FBISurvey2006.pdf, [accessed 6 May 2007].

Grossklags, J., Chuang, J., and Christin, N. (2008). Security Investment (Failures) in Five Economic Environments: A Comparison of Homogeneous and Heterogeneous User Agents, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Heiser, J. (2009). Four Risk Management Mistakes that Threaten Security Budget, *Gartner Research*, ID No. 00167541, available at: http://www.gartner.com/DisplayDocument?ref=g_search&id=994712&subref=simplesearch, [accessed 15 August 2009].

Herath, H.S.B. and Herath, T.C. (2007). Cyber-Insurance: Copula Pricing Framework and Implications for Risk Management, *WEIS 2007 – Sixth Workshop on Economics of Information Security*, Pittsburgh PA, 7-8 June 2007, Carnegie Mellon University, Pittsburgh, USA.

Holmes, A (2006). The Global State of Information Security 2006: Some things are getting better – slowly – but security practices are still immature and, in some cases regressing, *PricewaterhouseCoopers and CIO Magazine*, 15 September 2006.

Huang, C.D., Hu, Q. and Behara, R.S. (2006). Economics of Information Security Investment in the Case of Simultaneous Attacks, *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 26-28 January 2006, Robinson College, University of Cambridge, England.

Huang, C.D., Hu, Q. and Beraha, R.S. (2008). An Economic analysis of the optimal information security investment in the case of a risk averse firm, *The International Journal of Production Economics*, Vol. 2008, No. 114, pp. 793 - 804

Huberman, B.A., Adar, E. And Fine, L.R. (2005). Valuating Privacy, *The Fourth Workshop on the Economics of Information Security*, available at: http://infosecom.net/workshop/schedule.php, [accessed 27 November 2007].

Hulthen, R. (2008). Communicating the Economic Value of Security Investment: Value at Security Risk, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Humphreys, T., Snare, J., Plate, A., Kuiper, E. and Marshall, M. (2006). How to implement an ISO/IEC 27002 information security management system, International Organization for Standardization (ISO) Management Systems, May – June 2006, pp. – 40 – 44, available at www.iso.org/ims, [accessed 23 September 2008].

Information Commissioner (2006). What Price Privacy? The Unlawful Trade in Confidential Personal Information, Information Commissioner's Office, Available online at: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf, [accessed 14 July 2008].

Ioannidis, C., Pym, D. And Williams, J. (2009). Investments trade-offs in the Economics of Information Security, *the 13th Proceedings of the conference of Financial Cryptography and Data Security*, February 23 – 26, 2009, Barbados, USA.

Ioannidis, S., Markatos, E. and Kruegel, C. (2009). On Looking FORWARD, *ERCIM NEWS 70*, January 2009, available at: http://www.ict-forward.eu/media/publications/forward-ercim-news-76.pdf, [accessed 05 March 2009].

ISO/IEC 27002:2005, July 2007 *Information technology - Security techniques - Code of practice for information security management*, renumbered in 2007

Jamkhedkar, P.A. and Heileman, G.L. (2005). The Role of Architecture in DRM Vendor Economics, *The Fourth Workshop on the Economics of Information Security*, available at: http://infosecom.net/workshop/schedule.php, [accessed 27 November 2007].

Jegher, J. et al. (2007). IT Spending in Financial services: A Global Perspective, [Online] *CELENT LLC*, NY, USA, 28 December 2007, available at: http://reports.celent.com/PressReleases/200712282/GlobalITSpending.htm, [accessed 18 September 2008].

Johnson, M.E. and Dynes, S. (2007). Inadvert Disclosure – Information Leaks in the Extended Enterprise, *The Fifth Workshop on the Economics of Information Security*, available at: http://weis2007.econinfosec.org/program.htm, [accessed 27 November 2007].

Kaya, I. (2007). Global IT Spending in 2007 and Beyond: China and India on the Rise, Towergroup, February 2007, #V50:08B, USA.

Kilcourse, B. and Rowen, S. (2007). Customer Data Security: PCI and Beyond Benchmark Study 2008, *Retail Systems Research*, available at: http://searchstorage.bitpipe.com/detail/RES/1205868662_509.html, [accessed 26 June 2008].

Killmeyer, J. (2006). Information Security Architecture, Second Edition, Auerbach Publication Taylor & Francis Group, Florida, USA.

Ko, C. (2008). Underground Economy Booming Online, Says Symantec, *IDG News Service*, available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123142&source=rss_ind130, [accessed 10 January 2009].

LeClare, P (2008). Forrester: IT Security Spending on the Rise, Forrester Research, Press Release 4 September 2008, available at: www.forrester.com/ER/Press/Release/0,1769,1224,00.html, [accessed 16 September 2008].

Lewi, S.R. (2003). How Much is Strong DRM Worth, *The Second Workshop on the Economics of Information Security*, available at www.cpppe.umd.edu/rhsmith3/agenda.htm, [accessed 27 November 2007].

Lidow, J. and Stahl, S. (2007). Eight Steps to Protecting Sensitive Middle-Market Data, *CITADEL Information Group Inc*, Los Angeles, USA, available at: http://citadel-information.com/library/1/8-Steps-to-Protecting-Sensitive-Middle-Market-Data-CIG-0712.pdf, [accessed 16 September 2008].

Lipari, M.J. (2009). Implementing a Proactive, Strategic Information Security Plan, Ebiz, Data Security, available at: http://www.ebizq.net/topics/data_security/features/11032.html, [accessed 12 may 2009].

Liu, W., Tanaka, H. and Matsuura, K. (2007). Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, Regular Paper, *IPSJ Digital Courier*, Vol.3, pp. 585 – 599.

Liu,W., Takana, H. and Matsuura, K. (2006). An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan, *the fifth Workshop on the Economics of Information Security (WEIS 2006)*, 26 -28 June 2006, Robinson College, University of Cambridge, UK.

MacMillan, R. (2008). New Rootkit Uses Old Trick to Hide, IDG News Service, Available online at: http://www.pcworld.com/article/141300/new_rootkit_uses_old_trick_to_hide.html, [accessed 14 July 2008].

Marra, R.J. (2009). Three Men Indicted for Hacking into Five Corporate Entities, including Heartland, 7-Eleven, Hannaford, Wih over 130 Million Credit and Debit Card Numbers Stolen, available at: http://www.justice.gov/usao/nj/press/press/files/pdffiles/gonz0817%20rel.pdf, [accessed 04

November 2009].

MarketResearch.com (2008). Global IT Security Market Forecast to 2013. RNCOS, Pub ID:CICQ1831992 available at: http://www.marketresearch.com/product/display.asp?productid=1831992&SID=16965532-426498252-409536336, [accessed 23 February 2009].

Matsuura, K. (2008). Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Melek, A. (2009). Protecting what matters: the 6th Annual Global Security Survey, *Deloitte Touché Tohmatsu*, available at: http://www.deloitte.com/dtt/cda/doc/content/dtt_fsi_GlobalSecuritySurvey_0901.pdf; [accessed 23 February 2009]

Melek, A. and MacKinnon, M. (2005). 2005 Global Security Survey, Global Financial Services Industry, Deloitte Creative Studio, *Deloitte Touché Tohmatsu*, London, UK, AP #5071, available at: http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritySurvey_2005-07-21.pdf, [accessed 20August 2008].

Melek, A. and MacKinnon, M. (2006). 2006 Global Security Survey, Global Financial Services Industry, Deloitte Creative Studio, *Deloitte Touché Tohmatsu*, London, UK, Item # 6108, available at: http://www.deloitte.com/dtt/cda/doc/content//ca_%202006_GFSI_Survey.pdf, [accessed 20 August 2008].

Melek, A., MacKinnon, M. and Kantamneni, P. (2007). 2007 Global Security Survey: The Shifting Security Paradigm, Global Financial Services Industry, Deloitte Creative Studio, *Deloitte Touché Tohmatsu*, London, UK, Item # 7182, available at: http://www.deloitte.com.vn/dtt/cda/doc/content/rs_Deloitte_Global_Security_Survey_2007.pdf, [accessed 20 August 2008].

Melillo, L. (2006). Using ROI analysis to Prioritize Technology Purchases, available at: http://office.microsoft.com/en-us/excel/HA011999671033.aspx, [accessed 27 November 2007].

Miller, C. (2007). The Legitimate Vulnerability Market: The Secretive World of 0-Day Exploit Sales, *The Fifth Workshop on the Economics of Information Security*, available at: http://weis2007.econinfosec.org/program.htm, [accessed 27 November 2007].

Nash, K.S. (2008). The Global State of Information Security: But technology doesn't buy peace of mind, *A Joint Research Project of CIO and CSO in partnership with PriceWaterHouseCoopers (PWC), CXO Media 2008*, available at: http://www.pwc.com/en_GX/gx/information-security-

survey/pdf/pwcsurvey2008_cio_reprint.pdf, [accessed 21 January 2009].

National Institute of Standards and Technology (NIST) (1995). An Introduction to Computer Security: *The NIST Handbook Special Publication 800-12*, available at: http://csrc.nist.gov/publications/PubsSPs.html, [accessed 27 November 2007].

Ogut, H., Menon, N. and Raghunathan, S. (2005). Cyber Insurance and IT Security Investment: Impact of Interdependent Risk, *The Fourth Workshop on the Economics of Information Security*, available at http://infosecom.net/workshop/schedule.php, [accessed 27 November 2007].

Ormerod, P. (2003). Sunday Times Article, Available online at http://www.paulormerod.com/current.html, [accessed 05 May 2007].

Owen, S. (2008). Gaining Momentum: The 2008 Energy & Resources Global Security Survey, Enterprise Risk Services, *Deloitte Touché Tohmatsu*, available at: http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/dtt_2008energy&resourcesglobalsecuritysurvey.pdf, [accessed 21 January 2009].

Ozment, A. (2004), A Bug Auction: Vulnerability Markets Reconsidered, *The Third Workshop on the Economics of Information Security*, available at: http://www.dtc.umn.edu/cgi-bin/seminars.php?eventdesc=207&menu=agenda, [accessed 27 November 2007].

Pappa, A. (2002). Effective ROI – A Guide for Decision Makers, August 2002 Whitepaper, available at http://www.fujitsu.com/nz/whitepapers, [accessed 27 November 2007].

Patterson, T. (2003). Holistic Security: Why Doing More Can Cost You Less and Lower Your Risk. *Computer Fraud & Security*, Vol. 2003(6), June, pp13-15.

Pearson Education (2007). Computers and the Internet, Fact Monster, Available online at http://www.factmonster.com/ipka/A0872842.html, [accessed 04 July 2007] .

Pestcatore, J. et al. (2008). Gartner 2008 IT Security Threat projection Timeline, *Gartner Research*, ID No. G00160037, 26 August 2008, USA.

Petreley, N. (2004). Security Report: Windows vs. Linux, The Register, Available online at: http://www.theregister.co.uk/security/security_report_windows_vs_linux/, [accessed 14 July 2008].

Pfleeger, C.P. and Pfleeger, S.L. (2007). Security in Computing, 4th edition, Pearson Education, Inc, United States.

Pfleeger, S.L. and Rue, R. (2008). Cybersecurity Economic Issues: Clearing the Path to

Good Practice, *IEEE Software*, Vol. 25, Issue No.1, January – February 2008, pp. 35 – 42.

Purcell, J. (2007). Security Control Types and Operational Security, available at: http://www.giac.org/resources/whitepaper/operations/207.php, [accessed 29 November 2007].

Purser, S.A. (2004). Improving the ROI of the Security Management Process, *Computers & Security*, 23(7), pp. 542-546.

RAND (2008). Cybersecurity Economic Issues: Corporate Approaches and Challenges to Decision Making, Research Brief, *RAND Homeland Security*, November 2008, available at www.rand.org/pubs/research_briefs/2008/RAND_RB9365-1.pdf, [accessed 08 December 2008].

Research and Markets (2008). Federal Information Security Market Forecast 2008 - 2013, available at: http://www.researchandmarkets.com/research/a3bac2/federal_informatio [accessed 18 February 2009]

Researchandmarkets (2007). IT Security Market Report 2007, available at: http://www.bharatbook.com/productdetail.asp?id=11035, [accessed 18 February 2009]

Richardson, R. (2007). 2007 CSI Computer Crime & Security Survey [online], Computer Security Institute, available at: http://www.gocsi.com/, [accessed 03 July 2008].

Richardson, R. (2008). 2008 CSI Computer Crime & Security Survey: The latest results from the longest-running project of its kind [online], *Computer Security Institute*, available at: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf, [accessed 10 December 2008].

Rolfsdotter Karlsson, A., (2008). Managing Performance Measurement: A study of how to select and implement performance measures on a strategic, tactical and operational level, Master Thesis, University of Gävle, Sweden

Romer, H. and White, W. (2006). Security Inside Out, Oracle Security Solutions. Available online at www.oracle.com, [accessed 19 July 2007].

Romanowsky, S., Telang, R. and Acquisti, A. (2008). Do Data Breaches Disclosure Laws Reduce Identity Theft, *The Seventh Workshop on the Economics of Information Security*, 28 June 2008, Hanover, USA.

Rusell, D. and Gangemi, G.T. (1991). Computer Security Basics, O'Reilly& Associates, Inc. United States of America.

SANS Institute (2006). The Ten Most Important Security Trends of the Coming Year. Available online at http://www.sans.org/resources/10_security_trends.pdf, [accessed 04 July 2007].

Schneier, B. (2002). Computer Security: It's the Economics, Stupid, *1st Workshop on the Economics of Information Security*, May 16 -17 2002, University of California, Berkeley, USA.

Schneier, B (2003). The Speed of Security, IEEE Security and Privacy, 1(4), Jul/Aug 2003.

Sophos (2007). Sophos Security Threat Report July 2007. Available online at http://www.tradepub.com/free/w_soph08, [accessed 13 August 2007].

South Africa, (2000). *Promotion of Access to Information Act 2000*, (Act 2 of 2000) Government Gazette, 20852:416(95), 3 Feb 2000.

SOX (2002). Sarbanes, P. & Oxley, M. G. Sarbanes-Oxley Act 2002. available at: www.soxlaw.com [accessed 17 February 2009].

Soo Hoo, K. (2002). How Much Is Enough? A Risk Management Approach to Computer Security, Available at: www2.sims.berkeley.edu/resources/affiliates/econsecurity/econws/06.doc, [accessed 08 August 2007].

Speyer, M., Young, G.O., Pohlmann, T. & Brown, K. (2006). North America's 2006 Enterprise IT Spending Outlook, Forrester, February 3, 2006.

Srinidhi, B., Yan, J. and Tayi, G.K. (2008). Firm-level Resource Allocation to Information Security in the Presence of Financial Distress, Working paper Series 2008-17, School of Economic Sciences, Washington State University, USA, available at: www.ses.wsu.edu/PDFFiles/WorkingPapers/Yan/Srinidhi_Yan_GiriJune2008MISQ.pdf, [accessed 09 February 2009].

Stoll, C. (2000). The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, 1st Edition, Pocket, United States of America

Su, X. (2006). An Overview of Economic Approaches to Information Security Management, Technical Report TR-CTIT-06-30, *Centre for Telematics and Information Technology*, University of Twente, Information Systems Group, Enschede, ISSN 1381 – 3625, Netherlands.

Sural, S. (2006). Information Security: Brief History and Current Perspective. Available online at http://egovstandards.gov.in/, [accessed 08 August 2007].

Swanton, B. and Scott, F. (2005). High-Technology Industry Spending Profile 2005 – 2006: Focus on Operational Effectiveness of lean Supply Networks, AMR Research Market Analytix Report: IT Spending Series, *AMR Research Inc*, No. AMR-R-18539, Boston, MA, USA.

Sygate (2002). Is Return on Security Investment Impossible? Until Now Open Networks defeat all ROI-based Security Investments, available at: http://whitepapers.techrepublic.com.com, [accessed 28 November 2007].

Symantec (2008). Symantec Report on the Underground Economy (July 2007 – June 2008), Whitepaper, available at: eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf, [accessed 09 January 2009].

Symantec Internet Security Threat Report (2007). Trends for July – December 06, Vol. XI. Available online at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_emea_03_2007.en-us.pdf, [accessed 13 August 2007].

Syverson, P. (2003). The Paradoxical Value of Privacy, *The Second Workshop on the Economics of Information Security*, May 29 – 30, 2003, Robert H. Smith School of Business, University of Maryland, USA.

Tanaka, H., Matsuura, K. and Sudoh, O. (2005). Vulnerability and Information Security Investment: An Empirical Analysis of e-local Government in Japan, *Journal of Accounting and Public Policy*, Elsevier, Vol. 2005, No.24, pp. 37 -59.

Terzi, M. (2006). Information Based Economy and Educational System, TEKPOL WP 0612, *Science and Technology Policy Studies Center*, Middle East Technical University, available at: http://www.stps.metu.edu.tr/stpswp/series06/0612.pdf, [accessed 13 August 2009].

Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005). The Insider Threat to Information Systems and the Effectiveness of ISO 17799, *Computers & Security*, Vol. 24, pp. 472-484.

Timms, S. (2004). Information Security Breaches Survey 2004: Executive Summary, PriceWaterhouseCoopers, Department of Trade and Industry, UK, available at: http://www.entrust.com/resources/pdf/ukdti_infosecbreachessurvey2004_execsumm.pdf, [accessed 18 February 2009]

Tipton, H.F. and Krause, M. (2003). Information Security Management Handbook, 5th Edition, *Auerbach Publication*, New York, USA.

Tsiakis, T. and Stephanides, G. (2005). The Economic Approach of Information Security, *Computers & Security*, Vol. 24, No. 2, pp. 105-108.

Vadera, S.Vadera, S., Potter, C. and Beard, A (2008). 2008 Information Security Breaches Survey, Technical Report, PricewaterhouseCoopers, Department for Business, Enterprise & Regulatory Reforms (BERR), UK.

Van Kessel, P. (2006). Achieving Success in a Globalized World: Is Your Way Secure? 2006 Global Information Security Survey, *Ernst & Young*, EYG No. AU0022, available at: http://www.ey.com/Publication/vwLUAssets/Achieving_Success_in_a_Globalized_World:_Is_Your_Way_Secure_/$FILE/Achieving_success_globalized_world.pdf, [accessed 20 August 2008].

Van Kessel, P. (2007). 10th Annual Global Information Security Survey: Achieving a Balance of Risk and Performance, 2007 Global Information Security Survey, *Ernst & Young*, EYG No. DZ0033, available at: http://www.ey.com/Publication/vwLUAssets/EY_TSRS_GISS2007/$FILE/EY_TSRS_GISS2007.pdf, [accessed 20 August 2008].

Van Kessel, P. (2008). Moving Beyond Compliance, Ernst & Young's 2008 Global Information Security Survey, *Ernst & Young*, available at: http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf, [accessed 21 January 2009].

Vila, T., Greenstadt, R. and Molnar, D. (2003). Why We Can't Read Privacy Policies Models of Privacy Economics as a Lemons Market, *The Second Workshop on the Economics of Information Security*, May 29 – 30, 2003, Robert H. Smith School of Business, University of Maryland, USA

Volker, T. (2007). Security Goes From Tactical to Strategic. Available online at http://www.mydigitallife.co.za, [accessed on 13 August 2007].

von Solms, B. and von Solms, R. (2005). From information security to...business security? C*omputers & Security*, 2005(24), pp. 271 – 273.

Wang, Z. and Song, H. (2008). Towards an Optimal Information Security Investment Strategy, *The Proceedings of the IEEE International Conference on Networking, Sensing and Control*, Vol. 2008, 6-8 April 2008, pp. 756-761.

Wei, H., Frincke, D., Alves-Foss, J., Soule, T. and Pforsich, H. (2005). A Layer Decision Model for Cost-Effective Network Defense, *IRI-2005, IEEE International Conference on Information Reuse and Integration*, 15 – 17 August 2005, pp. 506 – 511.

Wei, H., Alves-Foss, J., Soule, T., Pforsich, H., Zhang, D., and Frincke, D. (2008). A Layered Decision Model for cost-effective system security. *International Journal of Information and Computer Security, Int. J. Inf. Comput. Secur.*DOI= http://dx.doi.org/10.1504/IJICS.2008.020607, 2(3), October 2008, Inderscience Publishers, Geneva, Switzerland, pp. 297-324.

Wei, H., Alves-Foss, J., Zhang, D. and Frincke, D. (2007). Rational Validation of a layered

Decision Model for Network Defense, *IRI-2007, IEEE International Conference on Information Reuse and Integration*, 13 – 15 August 2007, pp. 85 – 90.

Werlinger, R., Hawkey, K. and Beznosov, K. (2009). An Integrated View of Human, Organisational and Technological Challenges of IT Security Management, *The Journal of Information Management & Computer Security*, 17(1).

Willemson, J. (2006)., On the Gordon and Loeb Model for Information Security Investment, *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, University of Cambridge, UK, 26-28 June 2006, available at: http://www.ut.ee/~jan/publ/economics.ps, [accessed 27 November 2007].

Wood, C.C. and Parker, D.B. (2004). Why ROI and Similar Financial Tools are not Advisable for Evaluating the Merits of Security Projects, *Computer Fraud & Security*, 2004(5), pp. 8-10.

Zetter, K. (2003). Just Say No to Viruses and Worms, Available online at: http://www.wired.com/techbiz/it/news/2003/09/60391?currentPage=all, [accessed on 15 July 2008].

Zhao, X., Chen, J. and Whinston, A.B. (2007). A Reputation Mechanism for Software Vulnerability Disclosure and Patch Release, *WEIS 2007 – Sixth Workshop on Economics of Information Security*, Pittsburgh PA, 7-8 June 2007, Carnegie Mellon University, Pittsburgh, USA.

ZKB Zurich Kantonal Bank Website, (2009). Available online available at: http://www.zkb.ch/de/center_worlds/englishwindow.html, [accessed 11 February 2009].

Zuccato, A. (2007). Holistic security management framework applied in electronic commerce, *Computers & Security*, 26(3), May 2007, pp. 256-265

9.0 Appendices

Appendix A: Information technology – Security techniques – Code of practice for information security management - ISO/IEC 27002

Clause	Administrative Control	Operational Control	Environmental Control
5.1.1 Information security policy document	✓		
5.1.2 Review of information security policy	✓		
6.1.1 Management commitment to information security	✓		
6.1.2 Information security co-ordination	✓		
6.1.3 Allocation of information security responsibility	✓		
6.1.4 Authorization process for information processing facilities		✓	
6.1.5 Confidential agreements	✓		
6.1.6 Contact with authorities	✓		
6.1.7 Contact with special interest groups	✓		
6.18 Independent review of information security		✓	
6.2.1 Identification of risks to external parties		✓	
6.2.2 Addressing security when dealing with customers	✓		
6.2.3 Addressing security in third party agreements		✓	
7.1.1 Inventory of assets			✓
7.1.2 Ownership of assets			✓
7.1.3 Acceptable use of assets	✓		

Clause	Administrative Control	Operational Control	Environmental Control
7.2.1 Classification guidelines		✓	
7.2.2 Information labeling and handling	✓		
8.1.1 Roles and responsibilities		✓	
8.1.2 Screening		✓	
8.1.3 Terms and conditions of employment	✓		
8.2.1 Management responsibilities	✓		
8.2.2 Information security awareness, education, and training		✓	
8.2.3 Disciplinary process	✓		
8.3.1 Termination responsibilities	✓		
8.3.2 Return of assets	✓		
8.3.3 Removal of access rights	✓		
9.1.1 Physical security perimeter			✓
9.1.2 Physical entry controls			✓
9.1.3 Security offices, rooms , and facilities			✓
9.1.4 Protecting against external and environmental threats			✓
9.1.5 Working in secure areas			✓
9.1.6 Public access, delivery, and loading areas			✓
9.2.1 Equipment siting and protection			✓
9.2.2 Supporting utilities			✓
9.2.3 Cabling security			✓
9.2.4 Equipment maintenance			✓
9.2.5 Security of equipment off-premises			✓

Clause	Administrative Control	Operational Control	Environmental Control
9.2.6 Security disposal or re-use equipment			✓
9.2.7 Removal of property	✓		
10.1.1 Documented operating procedures		✓	
10.1.2 Change management		✓	
10.1.3 Segregation of duties		✓	
10.1.4 Separation of development, test, and operational facilities		✓	
10.2.1 Service delivery	✓		
10.2.2 Monitoring and review of third party services		✓	
10.2.3 Managing changes to third party services	✓		
10.3.1 Capacity management	✓		
10.3.2 System acceptance		✓	
10.4.1 Controls against malicious code		✓	
10.4.2 Control against mobile code		✓	
10.5.1 Information back-up		✓	
10.6.1 Network controls		✓	
10.6.2 Security of network services		✓	
10.7.1 Management of removable media	✓		
10.7.2 Disposal of media	✓		
10.7.3 Information handling procedures		✓	

Clause	Administrative Control	Operational Control	Environmental Control
10.7.4 Security of system documentation	✓		
10.8.1 Information exchange policies and procedures	✓		
10.8.2 Exchange agreements	✓		
10.8.3 Physical media in transit			✓
10.8.4 Electronic messaging		✓	
10.8.5 Business information systems	✓		
10.9.1 Electronic commerce		✓	
10.9.2 On-Line Transactions		✓	
10.9.3 Publicly available information	✓		
10.10.1 Audit logging		✓	
10.10.2 Monitoring system use		✓	
10.10.3 Protection of log information		✓	
10.10.4 Administrator and operator logs		✓	
10.10.5 Fault logging		✓	
10.10.6 Clock synchronization		✓	
11.1.1 Access control policy	✓		
11.2.1 User registration		✓	
11.2.2 Privilege management		✓	
11.2.3 User password management	✓		
11.2.4 Review of user access rights		✓	

Clause	Administrative Control	Operational Control	Environmental Control
11.3.1 Password use		✓	
11.3.2 Unattended use of equipment		✓	
11.3.3 clear desk and clear screen policy	✓		
11.4.1 Policy on use of network services	✓		
11.4.2 User authentication for external connections		✓	
11.4.3 Equipment identification in networks		✓	
11.4.4 Remote diagnostic and configuration port protection		✓	
11.4.5 Segregation in networks		✓	
11.4.6 Network connection control		✓	
11.4.7 Network routing control		✓	
11.5.1 Secure log-on procedure		✓	
11.5.2 User identification and authentication		✓	
11.5.3 Password management system		✓	
11.5.4 Use of system utilities		✓	
11.5.5 Session time-out		✓	
11.5.6 Limitation of connection time		✓	
11.6.1 Information access restriction	✓		
11.6.2 Sensitive system isolation			✓
11.7.1 Mobile computing and communications		✓	
11.7.2 Teleworking		✓	
12.1.1 Security requirement analysis and specification		✓	
12.2.1 Input data validation		✓	
12.2.2 Control of internal processing	✓		
12.2.3 Message integrity		✓	

Clause	Administrative Control	Operational Control	Environmental Control
12.2.4 Output data validation		✓	
12.3.1 Policy on the use of cryptographic controls	✓		
12.3.2 Key management		✓	
12.4.1 Control of operational software		✓	
12.4.2 Protection of system test data		✓	
12.4.3 Access control to program source code		✓	
12.5.1 Change control procedures		✓	
12.5.2 Technical review of applications after operating system changes		✓	
12.5.3 Restrictions on changes to software packages	✓		
12.5.4 Information leakage		✓	
12.5.5 Outsourced software development		✓	
12.6.1 Control of technical vulnerabilities		✓	
13.1.1 Reporting information security events		✓	
13.1.2 Reporting security weaknesses		✓	
13.2.1 Responsibilities and procedures		✓	
13.2.2 Learning from information security incidents	✓		
13.2.3 Collection of evidence		✓	
14.1.1 Including information security in the business continuity management process		✓	
14.1.2 Business continuity and risk assessment		✓	✓

Clause	Administrative Control	Operational Control	Environmental Control
14.1.3 Developing and implementing continuity plans including information security			✓
14.1.4 Business continuity planning framework			✓
14.1.5 Testing, maintaining and re-assessing business continuity plans		✓	
15.1.1 Identification of applicable legislation	✓		
15.1.2 Intellectual property right (IPR)	✓		
15.1.3 Protection of organisational records		✓	
15.1.4 Data protection and privacy of personal information		✓	
15.1.5 Prevention of misuse of information processing facilities		✓	
15.1.6 Regulation of cryptographic controls	✓		
15.2.1 Compliance with security policies and standards	✓		
15.2.2 Technical compliance checking		✓	
15.3.1 Information systems audit controls		✓	
15.3.2 Protection of information system audit tools		✓	

Appendix B: Classification of the ISF – The Standard of Good Practice for Information Security

Principle	Administrative Control	Operational Control	Environmental Control
SM1.1 Management commitment	✓		
SM1.2 Information security policy	✓		
SM1.3 Staff agreements	✓		
SM2.1 High-level control	✓		
SM2.2 Information security function	✓		
SM2.3 Local security co-ordination	✓		
SM2.4 Security awareness		✓	
SM2.5 Security education/training		✓	
SM3.1 Information classification	✓		
SM3.2 Ownership	✓		
SM3.3 Managing information risk analysis	✓		
SM3.4 Information risk analysis methodologies	✓		
SM3.5 Legal and regulatory compliance	✓		
SM4.1 Security architecture	✓		
SM4.2 Information privacy	✓		
SM4.3 Asset management			✓
SM4.4 Identity and access management			✓
SM4.5 Physical protection			✓
SM4.6 Information security incident management	✓		
SM4.7 Business continuity	✓		
SM5.1 Malware protection		✓	
SM5.2 Malware protection software			✓
SM5.3 Intrusion detection			✓

Clause	Administrative Control	Operational Control	Environmental Control
SM5.4 Emergency response	✓		
SM5.5 Forensic investigation	✓		
SM5.6 Patch management		✓	
SM6.1 Cryptographic solutions	✓	✓	
SM6.2 Public key infrastructure			✓
SM6.3 E-mail	✓	✓	✓
SM6.4 Remote working	✓	✓	✓
SM6.5 Third party access	✓		✓
SM6.6 Electronic commerce	✓		
SM6.7 Outsourcing	✓		
SM6.8 Instant messaging	✓	✓	✓
SM7.1 Security audit/review		✓	
SM7.2 Security monitoring		✓	
CB1.1 Confidentiality requirements		✓	
CB1.2 Integrity requirements		✓	
CB1.3 Availability requirements		✓	
CB 2.1 Roles and responsibilities	✓		
CB2.2 Application controls	✓	✓	
CB2.3 Change management	✓	✓	
CB2.4 Information security incident management		✓	
CB2.5 Business continuity	✓		
CB2.6 Sensitive information		✓	
CB3.1 Access control		✓	
CB3.2 Application sign-on process		✓	✓
CB3.3 Workstation protection	✓	✓	✓
CB3.4 Security awareness		✓	
CB4.1 Service agreements	✓		
CB4.2 Resilience		✓	✓
CB4.3 External connections	✓	✓	

Clause	Administrative Control	Operational Control	Environmental Control
CB4.4 Back-up		✓	
CB5.1 Local security co-ordination	✓		
CB5.2 Information classification	✓		
CB5.3 Information risk analysis		✓	
CB5.4 Security audit/review		✓	
CB6.1 Third party agreements	✓		
CB6.2 Cryptographic key management	✓	✓	
CB6.3 Public key infrastructure		✓	
CB6.4 Web-enabled applications		✓	
CI1.1 Roles and responsibilities	✓		
CI1.2 Service agreements	✓		
CI1.3 Asset management	✓	✓	
CI1.4 System monitoring		✓	
CI2.1 Installation design		✓	
CI2.2 Security event logging		✓	
CI2.3 Host system configuration		✓	
CI2.4 Workstation protection	✓	✓	✓
CI2.5 Resilience		✓	
CI2.6 Hazard protection			✓
CI2.7 Power supplies			✓
CI2.8 Physical access		✓	✓
CI3.1 Handling computer media		✓	
CI3.2 Back-up		✓	
CI3.3 Change management	✓	✓	
CI3.4 Information security incident management	✓	✓	
CI3.5 Emergency fixes	✓	✓	
CI3.6 Patch management	✓	✓	
CI4.1 Access control arrangements		✓	

Clause	Administrative Control	Operational Control	Environmental Control
CI4.2 User authorisation		✓	
CI4.3 Access privileges		✓	
CI4.4 Sign-on process		✓	
CI4.5 User authentication		✓	
CI5.1 Local security co-ordination	✓		
CI5.2 Security awareness		✓	
CI5.3 Information classification	✓		
CI5.4 Information risk analysis	✓	✓	
CI5.5 Security audit/review		✓	
CI6.1 Contingency plans	✓		
CI6.2 Contingency arrangements	✓		
CI6.3 Validation and maintenance		✓	
NW1.1 Roles and responsibilities	✓		
NW1.2 Network design		✓	
NW1.3 Network resilience			✓
NW1.4 Network documentation	✓		
NW1.5 Service providers	✓		
NW2.1 Configuring network devices		✓	
NW2.2 Firewalls		✓	
NW2.3 External access		✓	
NW2.4 Wireless access		✓	
NW3.1 Network monitoring		✓	
NW3.2 Change management	✓		
NW3.3 Information security incident management	✓	✓	
NW3.4 Physical security		✓	✓
NW3.5 Back-up		✓	
NW3.6 Service continuity	✓	✓	
NW3.7 Remote maintenance		✓	
NW4.1 Local security co-ordination	✓		

Clause	Administrative Control	Operational Control	Environmental Control
NW4.2 Security awareness	✓		
NW4.3 Information classification	✓		
NW4.4 Information risk analysis	✓	✓	
NW4.5 Security audit/review		✓	
NW5.1 Voice network documentation	✓		
NW5.2 Resilience of voice networks		✓	
NW5.3 Special voice network controls		✓	
NW5.4 Voice over IP (VoIP) networks	✓	✓	
SD1.1 Roles and responsibilities	✓		
SD1.2 Development methodology		✓	
SD1.3 Quality assurance		✓	
SD1.4 Development environment		✓	✓
SD2.1 Local security co-ordination	✓		
SD2.2 Security awareness	✓		
SD2.3 Security audit/review		✓	
SD3.1 Specification of requirements	✓		
SD3.2 Confidentiality requirements	✓		
SD3.3 Integrity requirements	✓		
SD3.4 Availability requirements	✓		
SD3.5 Information risk analysis		✓	
SD4.1 System design		✓	
SD4.2 Application controls		✓	
SD4.3 General security controls		✓	
SD4.4 Acquisition		✓	
SD4.5 System building		✓	
SD4.6 Web-enabled development		✓	
SD5.1 Testing process		✓	✓
SD5.2 Acceptance testing		✓	✓

Principle	Administrative Control	Operational Control	Environmental Control
SD6.1 System promotion criteria		✓	✓
SD6.2 Installation process		✓	
SD6.3 Post-implementation review		✓	
UE1.1 Roles and responsibilities	✓		
UE1.2 Security awareness	✓		
UE1.3 User training		✓	
UE1.4 Local security co-ordination	✓		
UE1.5 Information classification	✓		
UE2.1 Access control		✓	
UE2.2 Application sign-on		✓	
UE2.3 Change management		✓	
UE3.1 Inventory of desktop applications		✓	
UE3.2 Protection of spreadsheets		✓	
UE3.3 Protection of databases		✓	
UE3.4 Desktop application development		✓	
UE4.1 Workstation protection	✓	✓	✓
UE4.2 Hand-held devices	✓	✓	✓
UE4.3 Portable storage devices	✓	✓	✓
UE5.1 General controls	✓	✓	
UE5.2 E-mail	✓	✓	
UE5.3 Instant messaging	✓	✓	
UE5.4 Internet access	✓	✓	✓
UE5.5 Voice over IP (VoIP) networks	✓	✓	
UE5.6 Wireless access		✓	
UE6.1 Information privacy	✓		
UE6.2 Information security incident management		✓	
UE6.3 Back-up		✓	

Clause	Administrative Control	Operational Control	Environmental Control
UE6.4 Physical and environmental protection			✓
UE6.5 Business continuity		✓	

Appendix C: Payment Card Industry Data Security Standard Version 1.2.1

Payment Card Industry (PCI)
Data Security Standard - July 2009

Requirements
Version 1.2.1

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
1.1 Establish firewall and router configuration standards that include the following:			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	✓		
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks		✓	
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone		✓	
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	✓		
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	✓		
1.1.6 Requirement to review firewall and router rule sets at least every six months	✓		
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.			
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.		✓	
1.2.2 Secure and synchronize router configuration files.		✓	
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.			✓
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.			

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.			✓
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.			✓
1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.			✓
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.			✓
1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.			✓
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only ”established” connections are allowed into the network.)		✓	
1.3.7 Place the database in an internal network zone, segregated from the DMZ.			✓
1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).		✓	
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.		✓	
2.1 Always change vendor-supplied defaults **before** installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.		✓	
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults,		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.			
2.2.1 Implement only one primary function per server.		✓	
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).		✓	
2.2.3 Configure system security parameters to prevent misuse.		✓	
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.		✓	
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.		✓	
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in the additional PCI DSS Requirements for Shared Hosting Providers.		✓	✓
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	✓	✓	✓
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:		✓	
3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: ▪ *The cardholder's name,* ▪ *Primary account number (PAN),* ▪ *Expiration date, and* ▪ *Service code* *To minimize risk, store only these data elements as needed for business.*			
3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.		✓	
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.		✓	
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Notes:* ▪ *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.* ▪ *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.*		✓	
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography ▪ Truncation ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key-management processes and procedures The MINIMUM account information that must be rendered unreadable is the PAN.		✓ ✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.		✓	
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:			
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	✓		
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.		✓	✓
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	✓		
3.6.1 Generation of strong cryptographic keys		✓	
3.6.2 Secure cryptographic key distribution		✓	
3.6.3 Secure cryptographic key storage		✓	
3.6.4 Periodic cryptographic key changes ▪ As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically ▪ At least annually		✓	
3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys		✓	
3.6.6 Split knowledge and establishment of dual control of cryptographic keys		✓	
3.6.7 Prevention of unauthorized substitution of cryptographic keys		✓	
3.6.8 Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	✓		

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are:* ▪ *The Internet,* ▪ *Wireless technologies,* ▪ *Global System for Mobile communications (GSM), and* ▪ *General Packet Radio Service (GPRS).*		✓	
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. ▪ *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.* ▪ *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*		✓	✓
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).		✓	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).		✓	
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.		✓	
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.		✓	
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure*		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.			
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	✓		
6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:	✓	✓	
6.3.1 Testing of all security patches, and system and software configuration changes before deployment, including but not limited to the following:		✓	
6.3.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)		✓	
6.3.1.2 Validation of proper error handling		✓	
6.3.1.3 Validation of secure cryptographic storage		✓	
6.3.1.4 Validation of secure communications		✓	
6.3.1.5 Validation of proper role-based access control (RBAC)		✓	
6.3.2 Separate development/test and production environments			✓
6.3.3 Separation of duties between development/test and production environments			✓
6.3.4 Production data (live PANs) are not used for testing or development		✓	
6.3.5 Removal of test data and accounts before production systems become active		✓	
6.3.6 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers		✓	
6.3.7 Review of custom code prior		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
to release to production or customers in order to identify any potential coding vulnerability *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*			
6.4 Follow change control procedures for all changes to system components. The procedures must include the following:			
6.4.1 Documentation of impact	✓		
6.4.2 Management sign-off by appropriate parties	✓		
6.4.3 Testing of operational functionality		✓	
6.4.4 Back-out procedures		✓	
6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the *Open Web Application Security Project Guide*. Cover prevention of common coding vulnerabilities in software development processes, to include the following: *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when this version of PCI DSS was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.*		✓	
6.5.1 Cross-site scripting (XSS)		✓	
6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.		✓	
6.5.3 Malicious file execution		✓	
6.5.4 Insecure direct object references		✓	
6.5.5 Cross-site request forgery (CSRF)		✓	
6.5.6 Information leakage and		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
improper error handling			
6.5.7 Broken authentication and session management		✓	
6.5.8 Insecure cryptographic storage		✓	
6.5.9 Insecure communications		✓	
6.5.10 Failure to restrict URL access		✓	
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public-facing web applications		✓	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	✓	✓	
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	✓	✓	
7.1.2 Assignment of privileges is based on individual personnel's job classification and function	✓	✓	
7.1.3 Requirement for an authorization form signed by management that specifies required privileges	✓		
7.1.4 Implementation of an automated access control system		✓	
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:		✓	
7.2.1 Coverage of all system components		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
7.2.2 Assignment of privileges to individuals based on job classification and function	✓	✓	
7.2.3 Default "deny-all" setting		✓	
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.		✓	
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: ▪ Password or passphrase ▪ Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)		✓	
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.		✓	
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.		✓	
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.		✓	
8.5.2 Verify user identity before performing password resets.		✓	
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.		✓	
8.5.4 Immediately revoke access for any terminated users.		✓	
8.5.5 Remove/disable inactive user accounts at least every 90 days.		✓	
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
8.5.7 Communicate password procedures and policies to all users who have access to cardholder data.	✓		
8.5.8 Do not use group, shared, or generic accounts and passwords.		✓	
8.5.9 Change user passwords at least every 90 days.		✓	
8.5.10 Require a minimum password length of at least seven characters.		✓	
8.5.11 Use passwords containing both numeric and alphabetic characters.		✓	
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.		✓	
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.		✓	
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.		✓	
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.		✓	
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.		✓	
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.			✓
9.1.1 Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*			✓
9.1.2 Restrict physical access to publicly accessible network jacks.			✓
9.1.3 Restrict physical access to wireless access points, gateways, and			✓

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
handheld devices.			
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. *For purposes of this requirement, "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.*			✓
9.3 Make sure all visitors are handled as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained			✓
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employee			✓
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration			✓
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.			✓
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.			✓
9.6 Physically secure all paper and electronic media that contain cardholder data.			✓
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data, including the following:			✓
9.7.1 Classify the media so it can be identified as confidential.	✓		✓
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.			✓

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
9.8 Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals).	✓		
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.		✓	
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.		✓	
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:		✓	
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.		✓	
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.		✓	
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.		✓	
10.2 Implement automated audit trails for all system components to reconstruct the following events:			
10.2.1 All individual accesses to cardholder data		✓	
10.2.2 All actions taken by any individual with root or administrative privileges		✓	
10.2.3 Access to all audit trails		✓	
10.2.4 Invalid logical access attempts		✓	
10.2 5 Use of identification and authentication mechanisms		✓	
10.2.6 Initialization of the audit logs		✓	
10.2.7 Creation and deletion of system-level objects		✓	
10.3 Record at least the following audit trail entries for all system components for each event:			
10.3.1 User identification		✓	
10.3.2 Type of event		✓	
10.3.3 Date and time		✓	
10.3.4 Success or failure indication		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
10.3.5 Origination of event		✓	
10.3.6 Identity or name of affected data, system component, or resource		✓	
10.4 Synchronize all critical system clocks and times.		✓	
10.5 Secure audit trails so they cannot be altered.			
10.5.1 Limit viewing of audit trails to those with a job-related need.	✓	✓	
10.5.2 Protect audit trail files from unauthorized modifications.		✓	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.		✓	
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.		✓	
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).		✓	
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). *Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6*		✓	
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).		✓	
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.		✓	
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). *Note: Quarterly external vulnerability scans must be performed by an Approved*		✓	

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.			
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:		✓	
11.3.1 Network-layer penetration tests		✓	
11.3.2 Application-layer penetration tests		✓	
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.		✓	
11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*		✓	
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	✓		
12.1.1 Addresses all PCI DSS requirements.	✓		
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	✓		

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
12.1.3 Includes a review at least once a year and updates when the environment changes.	✓		
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	✓		
12.3 Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:			
12.3.1 Explicit management approval	✓		
12.3.2 Authentication for use of the technology	✓		
12.3.3 A list of all such devices and personnel with access	✓		
12.3.4 Labeling of devices with owner, contact information, and purpose	✓		✓
12.3.5 Acceptable uses of the technology	✓		
12.3.6 Acceptable network locations for the technologies	✓		
12.3.7 List of company-approved products	✓		
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	✓		
12.3.9 Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use	✓		
12.3.10 When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.	✓		
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	✓		
12.5 Assign to an individual or team	✓		

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
the following information security management responsibilities:			
12.5.1 Establish, document, and distribute security policies and procedures.	✓		
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	✓		
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	✓		
12.5.4 Administer user accounts, including additions, deletions, and modifications	✓		
12.5.5 Monitor and control all access to data.	✓	✓	
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	✓		
12.6.1 Educate employees upon hire and at least annually.	✓		
12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.	✓	✓	
12.7 Screen potential employees (see definition of "employee" at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. *For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	✓		
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:			
12.8.1 Maintain a list of service providers.	✓		
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	✓		

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	✓		
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status.	✓	✓	
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.			
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ▪ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ▪ Specific incident response procedures ▪ Business recovery and continuity procedures ▪ Data back-up processes ▪ Analysis of legal requirements for reporting compromises ▪ Coverage and responses of all critical system components ▪ Reference or inclusion of incident response procedures from the payment brands	✓		
12.9.2 Test the plan at least annually.	✓		
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	✓		
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	✓		
12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.		✓	
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	✓		
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these			

PCI DSS Requirements	Administrative Control	Operational Control	Environmental Control
requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity* must *comply with the PCI DSS and validate compliance as applicable.*			
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	✓		
A.1.2 Restrict each entity's access and privileges to own cardholder data environment only.	✓	✓	✓
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.		✓	
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.		✓	

Appendix D. INFORMATION SECURITY: THE MOVING TARGET

MT Dlamini[1*], JHP Eloff[2*], MM Eloff[3#]

{[1]mdlamini, [2]eloff}@cs.up.ac.za, [3]eloffmm@unisa.ac.za

[*]Information and Computer Security Architectures Research Group
Department of Computer Science
University of Pretoria
South Africa

[#]School of Computing,
UNISA
Pretoria
South Africa

Abstract

Information security has evolved from addressing minor and harmless security breaches to managing those with a huge impact on organisations' economic growth. This paper investigates the evolution of information security; where it came from, where it is today and the direction in which it is moving. It is argued that information security is not about looking at the past in anger of an attack once faced; neither is it about looking at the present in fear of being attacked; nor about looking at the future with uncertainty about what might befall us. The message is that organizations and individuals must be alert at all times. Research conducted for this paper explored literature on past security issues to set the scene. This is followed by the assessment and analysis of information security publications in conjunction with surveys conducted in industry. Results obtained are compared and analysed, enabling the development of a comprehensive view regarding the current status of the information security landscape. Furthermore, this paper also highlights critical information security issues that are being overlooked or not being addressed by research efforts currently undertaken. New research efforts is required that minimise the gap between regulatory issues and technical implementations.

Keywords Information security, information security topics, information security trends, security breaches

1. Introduction

In the early days of computing, security breaches mainly included viruses and worms that would flash a message or advertisement on the screen without causing any serious damage to the information or systems being used. However, rare cases of attacks with the potential to harm information did occur, such as the Friday 13th virus which was set to erase all the information on infected disk drives on a certain Friday 13th late in the 1980s (Denning, 1991). As times changed, attacks also changed. Since the turn of the century, information security breaches have gained an unprecedented potential to impact negatively on businesses' reputation, profitability, customer confidence and overall economic growth (Romer & White 2006). Cybertrust (2005) argue that this problem is two-fold: firstly it is due to the increase in economic and political uncertainty and secondly to the pressure from consumers and regulatory bodies.

As an example, a security breach such as the leakage of credit card information can imply an enormous damage to card payment companies due to the cancellation and re-issuing of compromised cards. This could also cost millions of dollars in penalties to regulatory compliance bodies. The case of a gang of Europeans who cloned 32000 credit cards worth £17 million was reported in the Computer Fraud & Security News (2007) as the

biggest (yet) uncovered credit card fraud. This is just a glimpse of losses related to today's threats.

It is therefore very important for companies to notice that their strength in attaining and sustaining competitiveness in the highly volatile, demanding and uncertain markets lies in their ability to securely protect their information assets and IT infrastructure. It is not by mistake that information security has become a lingua franca not only to the world of computing, but also to various other industries. Multiple workshops and conferences such as IFIP/SEC (2007), NSPW (2007), USEC (2007), and WEIS (2007) have surfaced recently with the sole aim of discussing information security issues.

Does this mean information security is a new field or just another "fad"? No, information security is neither new nor a "fad". What is new is its broader focus and wider appeal. For a long time most organisations would not recognise the importance of securing the infrastructure that holds and transmits their strategic information. Information security has been treated as a by-product, if not as a "necessary evil that hinders productivity" (Conray-Murray, 2003). Organisations would do it merely because everybody else is doing it. However, slowly but surely information security is getting into the forefront of things, and has been promoted from a by-product to an integral part of business operations (Conner & Coviello, 2004).

This paper gives an overview of the following:

- Where did information security come from? (the past)
- How did it get to where it is today? (the present)
- In what direction it is heading? (the future)

Information security is not about looking at the past in anger of an attack once faced; neither is it about looking at the present in fear of being attacked; nor about looking at the future with uncertainty about what might befall us. Security experts must be alert at all times. The aim is not to scare people but to make them aware of how information security has evolved over the past five decades. As remarked by Ormerod (2003), it is hard for anyone to navigate with a map if his or her current position is unclear. The future of information security can be realised only if its past and current positions are well understood (Botha & Gaadingwe, 2006).

Hence, section two discusses the past events and section three focuses on the current status of information security. This is followed by section four which concludes this paper and provides ideas for future work.

2. Information Security: Then

Information security came into existence even before the invention of a computer. Rusell and Gangemi (1991) argue that information security is as old as information itself. From the time when information began to be transmitted, stored and processed, it required

protection. This dates back to the time when human beings first learned how to write. Denning (1999) takes us back to the first century when Julius Caesar devised a secret code to protect (confidential) messages sent to his friends from being intercepted.

In the 1840s when the telegraph was invented (Rusell & Gangeni, 1991), an encryption code was developed to safeguard the secrecy of the transmitted telegrams. This was followed by the invention of the telephone and a year later legislation prohibiting wiretapping was put in place. Information security has moved from protecting the secrecy of hand written messages to telegrams, to telephone conversations and later to the world of computing. Information security originated with a main concern of protecting the secrecy or confidentiality of transmitted data and information.

The 1940s up to the 1950s marked the dawn of computing, when the first-generation computers came into existence. This was followed by the era of mainframe computers when only a few operators were permitted to use these computers. Other users would submit their jobs to the operator through protected slots (batch processing). The key security issue during this era was ensuring that only the privileged computer operator (one user one computer) would have access and that the physical computer was not stolen or damaged by outsiders. The scope of security gradually increased from the protection of secrecy or confidentiality of information, to safeguarding the information infrastructure (mainframe computers) that processed the information and storage media. Physical security was the basic principle underlying all security of computer systems.

Mainframe computers were isolated stand-alone units and networks were non-existent back then. Human messengers or physical mail was used to transfer programs and their data between computers. The only threat related to the transmission of information was that storage media could be lost or stolen. Even though it would take days to get information or data to its destination, data was safe.

The late 1960s until the early 1970s mark the beginning of dumb terminals. These enabled users (multiple users - one computer) to access and use remote data. This innovation introduced a new risk to remotely held data. Data could be accessed by unauthorized people or outsiders. Elementary physical security could not deal with this new risk. Therefore user identification and authentication came into play in the early 1970s. Physical access to terminals was screened by a security officer before the user could start the identification and authentication process. Since there were few terminals it was easy to keep track of all logged-in users and their activities.

However, since there were no security policies in place to enforce the use of strong passwords, password cracking was a big threat at this time. Password sharing posed another major problem. Guest and anonymous logins were still acceptable, as outsiders without much identification and authentication could access only limited resources inside the network.

The era of dumb terminals was succeeded by that of mini computers. The introduction of mini computers marked the beginning of networks, time-sharing and multi-user systems

which changed the rules of the game. The number of people with computer know-how increased with the drop in prices of modems and terminals. Access controls were introduced to prevent users from interfering with one another's workspace. The work of Harrison, Ruzzo and Ullman (the HRU model) was the pioneer of access controls. This was followed by the Bell-LaPadula confidentiality model for Multics (Pfleeger & Pfleeger, 2007) and digital signatures from around the late 1970s to early 1980s. The Biba Integrity model was introduced and built on the Bell-LaPadula model (Sural, 2006). Over and above confidentiality, the concern for integrity came on-board.

Also in the early 1970s public key cryptography came into existence. The Data Encryption Standard (DES) was adopted by the then National Bureau of Standards (NBS) of USA, which is now called the National Institute of Standards and Technology (NIST). This is around the same time that the ARPANET began, which aimed at providing a reliable and robust network to ensure the availability of computer systems (Denning, 1999). This innovation introduced a new dimension for the protection of information, and the goal posts were again moved on. In response the US government passed the Privacy Act of 1974 to safeguard personal information recorded in government systems (Rusell & Gangemi, 1991).

The 1980s marked the introduction of personal computers and suddenly every user had his/her own computer (Rusell & Gangemi, 1991). Again the number of people with computer know-how increased. Companies began to automate their operations and new security threats emerged as critical corporate data was now stored on easily accessible secondary storage. The scope of information security further widened. Hence, the 414 gang, the intruder (Markus Hess) who broke into computers at Stanford campus in the USA and the West German programmer who broke into the US military computers to steal documents were reported to be among the first intruder break-ins (Denning, 1991; Stoll, 2000).

This decade marked the rise of computer viruses, which spread through the use of diskettes. Denning (1991) reported viruses called “Elk Cloner” and “The Brain” to be among the first viruses ever created. The former was created by Rick Skrenta, targeting Apple II disks, and would display a poem on the screen. The latter of the two viruses flashed an advertisement for a Pakistani company and is believed to have been the work of two Pakistani brothers. Denning (1991) also cited Robert Morris to have created the first worm in 1988, arguing that even though it was harmless, it produced a massive scare. These were just a minor annoyance to the user but did not really do any harm to the information stored or processed, or to the infrastructure. Microsoft Windows and Local Area Networks (LANs) emerged in this decade.

The USA government issued the Computer Fraud and Abuse Act of 1984 to prosecute and establish harsh penalties for offenders (creators and authors of computer viruses). This Act came into practice following the conviction of Robert Morris, author of the first Internet worm (Russell & Gangemi, 1991; Denning, 1991; Denning, 1999). It was followed by the Computer Security Act of 1987, also from the USA, which dealt with the training of security personnel involved in the processing of sensitive information.

The late 1980s also saw the introduction of anti-virus software. Carey (2008) argues that the European Bernt Fix in 1987 made the first ever anti-virus. In 1988, Alan Solomon, of Great Brittan released an antivirus software called Dr. Solomon's Anti-Virus Toolkit.

What was conceived in the late 1960s and born in the early 1970s as the ARPANET grew in the 1990s as LANs and WANs merged in distributed systems. The 1990s was dominated by open systems and mobile computing. More and more personal computers connected to the Internet. This innovation brought new risks, as would be expected since open systems would also be open to abuse (Denning, 1991). The hacking community created freely available hacking tools, and hence virus and worm attacks intensified and script kiddies started showing their faces. Anti-virus products were a prime solution.

Carey (2008) claim that by the end of 1990, there were approximately nineteen anti virus software environments including Symantec's Norton Anti Virus, ViruScan by McAfee; and IBM's Anti Virus. However, there are conflicting views as Pearson (2007) claim that Norton and ViruScan were among the first anti-virus environments created to combat viruses and worms.

Towards the end of the 1990s attackers changed from using worms and viruses to more sophisticated attacks. The introduction of distributed denial of service and malicious code attached to business emails and web pages shifted the focus to gateways. This saw the introduction of filtering firewalls. Perimeter security came into existence to provide a wall around networks and keep outsiders out. But as the use of the Internet intensified, network boundaries disappeared and perimeter security vanished.

As we entered the 21st century, things changed. Attackers started hacking for financial gains and not just to show-cast their skills. IT infrastructure became pervasive in almost all industries (known as the era of pervasive computing). Every second word now began with an E, for example E-commerce, E-voting, E-business, E-government, etc., because everything had gone electronic. As all sorts of devices came on-board (Personal Digital Assistants, Smart phones, Laptops, Tablet PCs, etc.), it became difficult to clearly define a computer. Mobile computing (Bluetooth and Wi-Fi) also emerged to complicate things even further. Online payment systems and the usage of credit cards became highly popular and web-based applications intensified. However, the fact remains that all these new developments in technology were vulnerable and like all other good things came with side effects (risks).

3. …..and Now

The 21st century innovations and developments came along with a strong dependency on IT infrastructure. This opened new and attractive doors for the hacking community. Attackers have evolved from computer enthusiasts to professional hackers (Gelbstein, 2006). Bruce Schneier quoted in Anderson (in press) argues that “it is only amateurs who

still target machines; career criminals now target people who operate them not just for fun but for financial gains". Attackers have matured from using hacking skills to showing that they can circumvent the authentication process to access each other's files to use them in the theft of confidential information. This has resulted in information security threats like identity theft, social engineering, phishing, etc which can easily compromise authentication and authorization credentials. Nowadays the motive of an attacker is financial gains and in order to evade the "long arm of law", he/she will do everything to cover his/her tracks. As a solution and in addition to the authorization and authentication credentials, verification of users became necessary for access. Banks introduced chip-and-pin. Non-repudiation has since become a critical issue of the 21st century.

Viruses and worms have evolved from minor annoyances to having catastrophic impacts and can infect thousands of machines in seconds (Zetter, 2003; Petreley, 2004). Creators of these threats have opted for a new twist on an old trick (MacMillan, 2008). Simple attacks have matured to become sophisticated, automatic, subtle and very hard to detect (Schneier, 2003; Carey, 2008). There is also the evolution of spam and phishing from email to SMS (short message service) and MMS (multimedia message service) technology in mobile phones (Symantec Internet Security Threat Report, 2007). Attackers are on the verge of re-inventing the wheel. They use old tricks in new twisted ways (MacMillan, 2008) and therefore the history of information security is as critical as the uncertain road ahead.

The future of information security remains clouded with numerous uncertainties. However, two things remain certain – IT infrastructures are vulnerable and motivated attackers are always ready to exploit these vulnerabilities. It is therefore critical that securing information and infrastructures should not be considered in fear of inevitable attacks, but in preparation for the uncertain future. This requires innovative ideas and insightful analysis of security issues to appropriately respond to the challenges posed by new developments. Another challenge is that as information security moves to respond to new threats in current and future environments, it must also protect against well-known threats. The goal posts are not only moving, but they also widen each time, making it very difficult to protect information and its infrastructure.

3.1 The Current Information Security Trends

Despite several studies aimed at providing much needed statistical information on security trends and issues, there is still an urgent need to find one that is complete and reliable. CSIA (Cyber Security Industry Alliance) (CSIA, 2007) compiled a list of disparate sources of information and statistics related to information security issues and their trends. This includes an overview of the work of Symantec, Sophos, Deloitte global security survey, Ernst & Young global information security survey, CSI/FBI computer crime and security survey, SANS institute, etc. However, most of these target the US and UK communities and very few have the world community as their target. Security experts can gain a good understanding of the current information security trends and issues by using the results of the above surveys. It is unfortunate that there is still (to the authors'

knowledge) no work that pays attention to the aggregation of the above surveys to get a holistic picture of the global information security landscape.

To further develop a good understanding of the current information security landscape, this paper outlines the following two phases of research as conducted for this project:

- Phase 1 monitored, assessed and analysed articles covered in the following four journals: Computer & Security, Computer Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security. The main aim is to identify the critical issues currently being addressed by security professionals to gain a complete picture of today's information security posture. The survey is based on publications for the years 2005 until December 2006. The question can be asked why these four journals? There are many journals and publications available today which focus on information security related issues. However, the authors of this paper wanted to include journals that represent both an academic (Computers & Security, IEEE Security & Privacy, Information Management & Computer Security) as well as a business (Computer Fraud & Security) view on the matter. Furthermore, because the authors wanted to focus on identifying trends it was important to include journals that are well established and have been available for a long enough time e.g. Computers & Security. It was also decided to only include journals that have information security as its primary focus.

- Phase 2 made an analysis of the 2006 report issued by the Computer Security Institute/Federal Bureau Investigations (CSI/FBI) (2006) on computer crime and security (Gordon et al 2006) as well as the SANS Institute (2006) report. The reasons for including surveys conducted by these two institutes are as follows: both institutes have delivered for many years a service to the information security community in the large; they both provide a wealth of security related content free to the public; both institutes have extensive research archives.

3.1.1 Limitations of the Study

Phase 1

All the publications seem to be more common in university libraries than in chief security officers' offices. Hence, it is unlikely that this approach will capture the true picture of the current information security landscape. Whilst the publications to a lesser extent reflect current research, they do not really reflect on the breaking security issues faced by information security practitioners. This is because the publications go through a long peer review process which adds a long time lag to the publication route and hence, they tend to rather deal with long term issues than short-term issues. The publications seem to focus more on full papers than the small section on breaking security issues. As a result they are not so responsive to the current security trends and issues. Hence, they tend to be a following rather than a leading indicator of information security trends. However, the publications are published almost monthly and contain articles written and reviewed by

experts in the information security field which makes them relevant. They also to a certain extent reflect the latest developments in the information security field. Although these four publications do not at all represent the whole spectrum of information security publications, the authors believe that assessing them can provide valuable insights into the current state and trends of information security.

Phase 2

The SANS Institute and CSI/FBI reports are both based on survey respondents. There are several drawbacks in such surveys which involve survey respondents, more especially security experts. Firstly, survey respondents tend to be biased when reporting security breaches in fear of the consequences of legal liability, and of damaging customer confidence and company reputation. Organisations usually do not report or reveal exact security breaches as they occurred (Eppel, 2005). Secondly, criminals hide their successful attacks which makes some security breaches go undetected and never accounted for in such survey results. Thirdly and final, vendors exaggerate the risk to market their products (Eppel, 2005). Hence, (CSIA, 2007) argues that surveys may provide valuable insights but there are doubts about their authenticity, correctness and completeness.

It is therefore very difficult to get a true and comprehensive view of the current state of information security based on the results of such surveys. However, to remove such doubts the results from the survey respondents will be aggregated with those of Phase 1 to help in developing a holistic picture of the current security trends and issues.

3.1.2 Data Collection

This section investigates the computer and information security issues found in the Computers & Security, Computer Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security publications for the year 2005 and 2006.

3.1.2.1 Topics Covered in the journals (Phase 1)

The data collection process started with a brainstorming session where all sorts of information security related topics were identified. These were then grouped into broad category topics to accommodate most of the topics identified in the brainstorming sessions. For example, every topic that dealt with surveillance cameras, fences, security guards and the likes were grouped as ***physical security***. Information security budgets, spending, culture, behaviour and anything that pertains to the management of information security were categorized as ***information security management***. The same strategy applies to all the other broad topics. All the topics that appear not to be part of any of the broad topics were categorized as ***other***. This category included topics like: security outsourcing; critical infrastructures; anonymous protocols and end user security to name just a few.

Even with this general option ***other***, there are certain limitations of the study as some topics could sometimes fit into more than one broad category. For example, the case of digital forensics and legal issues often overlap. To correctly categorise such issues, the abstract and keywords of an article would be read to determine its key theme. If still unclear, the conclusion would be consulted. The same technique applies for topics that are unclear or ambiguous. What must be noted though is that the categorisation used in this study does not represent a standard scientific categorisation, but solely the views and opinions of the authors.

3.1.2.2 Results obtained from the journals

This sub-subsection outlines the profile of articles published in all four publications over the period investigated. Some of the publications (i.e. Computers & Security and Computer Fraud & Security) contain a section on brief news or short discussions that would otherwise not qualify to be called full articles. These are also included in the survey results because they provide qualitative information about current security issues. Figure 1 summarises the amount of coverage given to each topic by all the journals included for this survey.

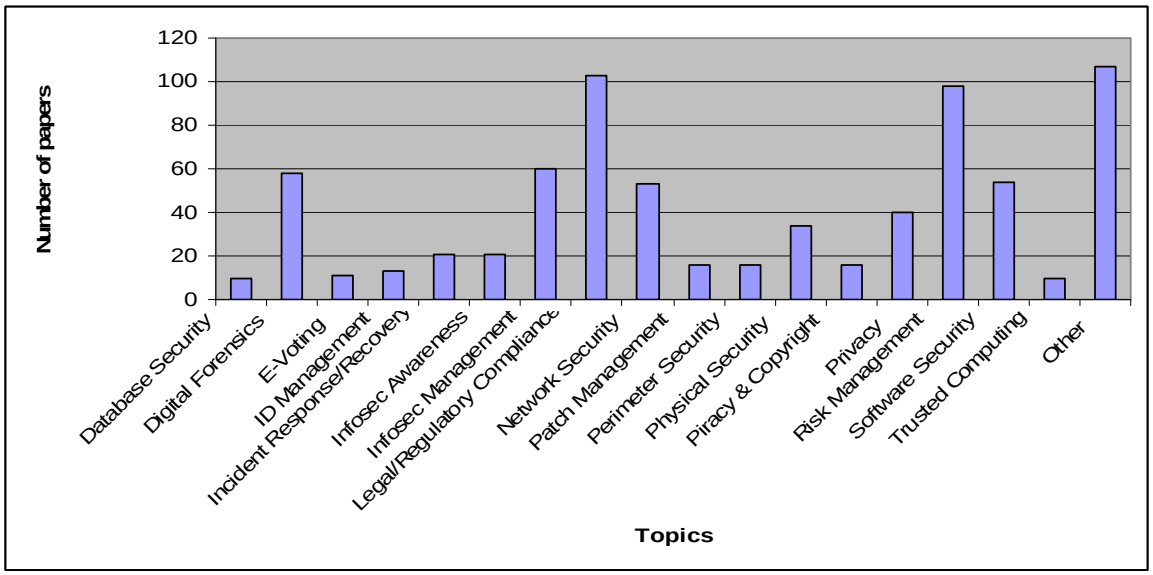


Figure 1: Importance of topics across all journals

When investigating each of the journals separately, it is interesting to note that different topics were emphasized by each journal.

Table 1 lists the top five topics in each of the journals in priority order with 1 being the most published topic for that specific journal.

Table 1: The Top Five in all the publications

	Computer Fraud & Security	**Computers & Security**	**IEEE Security & Privacy**	**Information Management & Computer Security**
Digital Forensics	3 (23)	2 (30)		
ID Management				5 (3)
Information Security Awareness			5 (9)	
Information Security Management		5 (14)	4 (23)	1 (12)
Legal & Regulatory Compliance	2 (40)	1 (56)		5 (3)
Network Security	4 (21)		4 (23)	4 (4)
Other		3 (27)	1 (41)	2 (11)
Perimeter Security				3 (5)
Physical Security	5 (20)			
Privacy			3 (28)	4 (4)
Risk Management	1 (67)	4 (22)		3 (5)
Software Security			2 (35)	3 (5)

Outstanding in the results of the Computers Fraud & Security publication is that risk management took the lead with 67 articles, followed by legal and compliance regulatory issues at 40, digital forensics at 23, network security at 21 and physical security at 20 to constitute the top five.

In the Computers & Security publication, articles on legal and regulatory compliance issues were more than all the other categories at 56, followed by digital forensics at 30, other at 27, risk management at 22 and information security management at 14 closing the top five most discussed topics.

The IEEE Security & Privacy publication focussed on amongst others on software security with 35, privacy at 28, then network security and information security management are tied at 23 and information security awareness at nine.

Lastly in the Information Management & Computer Security publication information security management took the lead at 12, with *other* at 11, followed by risk management, perimeter security and software security tied at five, then network security and privacy

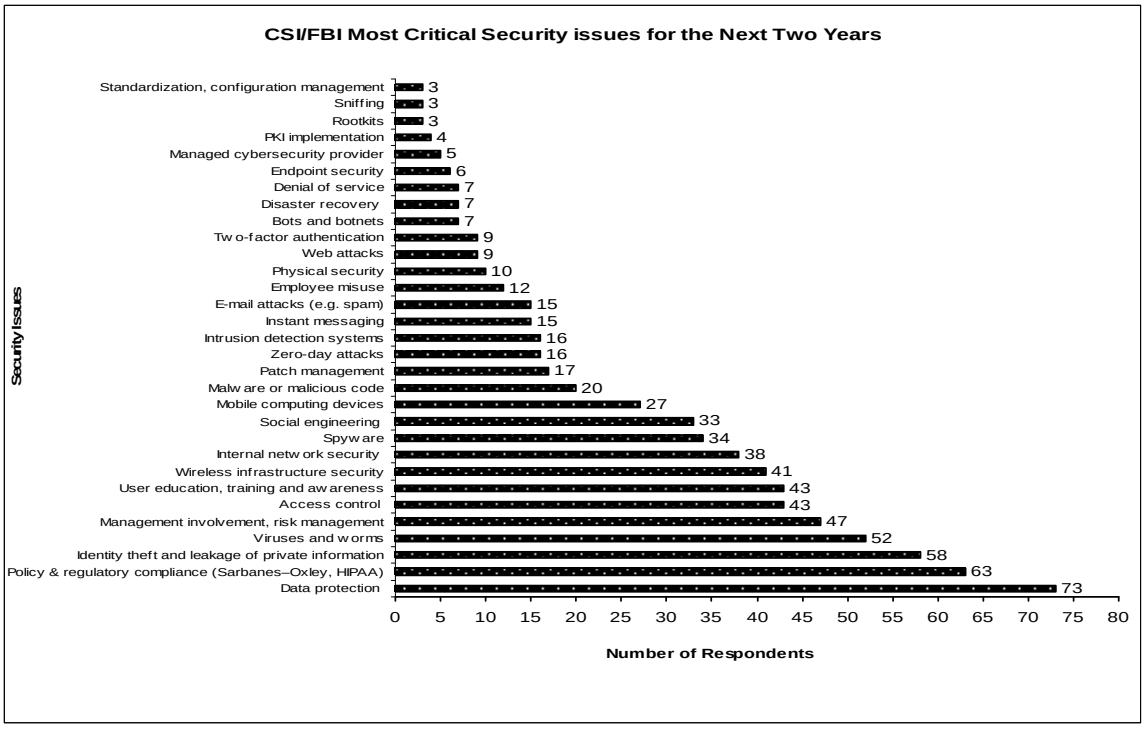
tied at four and in the 5th place legal and regulatory compliance and identity management at three.

3.1.3 Surveys of existing CSI/FBI and SANS reports (Phase 2)

In this subsection the study considers two well established surveys that had been gathering statistics and trends on information security for many years. These are the CSI/FBI computer crime and security survey and the SAN institute survey. However, the study at hand only focuses on the 2006 results.

The CSI/FBI survey has been gathering information security statistics for the past 12 years and they have developed significant experience in the field. Their results are based on the answers of survey respondents, which mainly consist of security practitioners from almost all industrial sectors in the United States. The US respondents' answers may not represent the true picture of information security worldwide, but they do provide valuable insights. The CSI/FBI (2006) data on the most critical security issues for 2007 and 2008 is used by the authors to compile a graph as shown in *Figure 2*.

Figure 2: Graph drawn from statistics/data provided by CSI/FBI (2006) (Gordon et al, 2006)



The SANS Institute (2006) report is based on twenty most respected leaders in cyber-security who developed a list of ten most important trends in predicting the future of information security. Unlike the CSI/FBI, the SAN report is a good representation of the worldwide situation of information security because it involves not only the US security

practitioners but cyber-security leaders from all over the world. The top five issues in both reports are summarised in the following table in ascending order.

Table 2: The top five issues of both security surveys

CSI/FBI computer crime survey	SANS Institute Survey
6. Data Protection	6. Laptop or mobile hardware devices encryption
7. Policy and regulatory Compliance	7. Significant growth in theft of PDA smart phones
8. Identity theft and Leakage of private information	8. More legislation governing the protection of customer information
9. Worms and viruses	9. Increase in targeted attacks
10. Management involvement and risk management	10. Increase in cell phone worms

3.2 Discussion and Analysis of Results

This section compares and discusses the results of the publications survey with the CSI/FBI and SAN 2006 reports on the future information security predictions. Notable in the findings is that most of the publications are written by security experts for the computer and information security community. Hence, one would expect to find most of the articles on database security, physical security and many other issues directly related to security technologies. However, this is not the case. Does this mean information security has changed?

No, information security has not changed per se, but it has since gained a broader and wider focus. This has caused security experts to change their focus too. From the early days of computing, information security has been put in the hands of security experts, but of late things are changing - as are clear from the results.

The results show a strong emphasis on three aspects: legal and regulatory compliance, risk management and information security management. This indicates that the security responsibility is widening to also include risk managers, forensic specialists, compliance regulators and other stakeholders. This involves a major shift from pure reactive technical measures towards a more proactive strategic approach (Volker, 2007). Also in support of the study findings are the predictions of the CSI/FBI (2006) report which points towards a strategic approach. However, the SANS institute (2006) report predicts an increase in encryption of mobile devices. The indication is that even with the move towards a strategic approach, technical measures are still as applicable as they were ten years ago.

The survey reveals that the Computers & Security publication put most emphasis on legal and regulatory compliance. In comparison to the others, legal and regulatory compliance is ranked second in the Computer Fraud & Security publication, third in the SANS institute (2006) report, second in the CSI/FBI (2006) report and fifth in Information

Management & Computer Security. Data protection, which is ranked first in the CSI/FBI report, also falls in this category. This shows that computer crime authorities around the world are working hard to find solutions for combating the rise in cyber-crime (Sophos, 2007).

Regulatory compliance goes hand in hand with legal issues as it ensures that standards are implemented and adhered to. Its main objective is to assess whether organisations have enough controls, are doing the right things, and are doing the right things the right way (Gelbestein, 2006). Regulatory compliance authorities enforce control by ensuring that organisations that do not comply with set standards face penalties and legal consequences and those that do, are awarded certificates in recognition. In as much as regulatory compliance enforces the use of appropriate security controls, its main target are the human factor of security.

The Computer Fraud & Security publication results show a main emphasis on risk management, which is ranked fourth in Computers & Security, fifth in the CSI/FBI (2006) report, third in Information Management & Computer Security and does not appear on the top five list of SANS Institute's (2006) report and the IEEE Security & Privacy publication. Information security experts are beginning to see the bigger picture. This is an indication that the debate is moving from an operational and tactical level towards a strategic level of risk management. However, this does not necessarily mean that the technical paradigm no longer has a role in information security.

Today's security threats are forcing organizations to become more adaptable and flexible with regards to the people, process and technology risks. It is through such risks that information security is a standard item on the agenda of senior management's meetings nowadays. This sets the scene and acts as the motivation for discussions on insurance in relation to securing information and its infrastructure.

The survey results further show that information security management is another focus area in the information security press. This topic is ranked first in Information Management & Computer Security, third in IEEE Security & Privacy, fifth in Computers & Security and CSI/FBI (2006). However, it is not a high priority in the other publications. This could be due to several biases that could be as a result of the audience and the focus of the publications. Information security management is a critical factor to get information security issues discussed in board rooms. Furthermore, information security management is a means to a strategic information security approach.

The survey results also show network security as another topic that has received attention in the information security press. It is ranked fourth in Computer Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security publications. This issue is just as important nowadays as it has ever been as networks are converging with their inherent risks. It is therefore very critical for the information security experts to address network security issues. Again this is an indication that technical issues are still applicable in the current and future information security landscape.

The other issue of concern in the information security press is digital forensics; a critical issue ranked third in the Computer Fraud & Security, second in the Computers & Security. However, it does not appear in the other two publications, CSI/FBI and the SAN top five. Digital forensics connects the law and information security. It ensures that evidence collected on the crime scene gets to the courts in an unhampered or uncontaminated state to facilitate the apprehension of criminals. However, such initiatives are undermined by inappropriate penalties stipulated in current laws. Hence, many computer crime perpetrators have been given inordinately light sentences for serious crimes. For example, the UK's Information Commissioner (2006) reports that between 2002 and 2006, only two out of 22 cases resulted to penalties amounting to only about £5000. A call has since been made to raise cyber crime penalties (Information Commissioner, 2006) and to increase the coordination between information security, digital forensics, government and law enforcements in order to best track and convict cyber criminals.

Ranked third in the CSI/FBI (2006) report is the issue of identity theft and the leakage of private information. Directly linked to identity theft and leakage of private information is privacy which is ranked third in IEEE Security & Privacy and Information Management & Computer Security. It is encouraging to see these issues being on the top five list of security issues being discussed. More so after Gunter Ollmann (cited in the editorial news section of Computer Fraud & Security, 2007), reported that on the black market identities are selling for much more than credit card numbers. This is another critical area that security practitioners need to look at in order to address current and future threats.

Software security is ranked second in IEEE Security & Privacy and third in Information Management & Computer Security but not covered in the other publications. Software security is a major issue that underlies insecure systems. The expectation would be to have more publications addressing software security.

The theft of laptops, smart phones, PDAs and other mobile devices is on the rise (SAN, 2006). However, what attract most thieves are not just the devices per se but the data held in them. It is therefore no coincidence that the issue of laptop or mobile hardware encryption lay at the top of the five most important security trends of the report by the SANS Institute (2006). This is an effort to ensure that even if such devices get stolen, the critical and valuable data they hold will not be compromised. Moreover, the SANS institute reported legislation governing the protection of such data or information to ensure that organisations that lose or compromise such data would face legal consequences. Data protection, which is ranked first in the CSI/FBI report, also supports the SAN institute's findings. Preserving privacy, preventing identity theft and leakage of private information is critical nowadays.

Furthermore, the SANS report predicts an increase in targeted attacks and cell phone worms. The former is concerned with purposeful attacks mainly driven by financial motives. The latter shows that the target is moving towards new environments as it spreads to exploit cellular networks. The CSI/FBI (2006) report shows that worms and viruses will continue to be a big threat to information systems in the next few years.

These threats are finding new exploits to infect and they are becoming increasingly sophisticated and thus hard to detect. Such threats cause the scope of information security to continue widening.

Physical security, information security awareness, identity management and perimeter security are also in the top five topics discussed even though not extensively. These are the issues that security experts are expected to be more concerned with. However, this is unfortunately not the case.

These research results show the current direction of information security. It is clear that information security research is moving towards a strategic approach. However, this is not a complete switch as technical measures remain applicable. The end result is that information security's focus is widening and deepening. However, several other issues remained overlooked or needs more emphasis by current research despite being critical for securing information. Such issues are discussed in the next section.

3.3 Critical Overlooked Security Issues

The survey results show that only a few articles discuss information security awareness and training, incident response and disaster recovery and the human aspect of information security (social, cultural and ethical aspects of human resources and organization policies). Organisations must understand that the best security technologies in the world cannot stop a social engineer impersonating legal users for access codes. Moreover, they cannot stop a stranger walking in an organisation empty-handed and emerging with a laptop full of sensitive data. It is for this reason that information security awareness campaigns have emerged as an important aspect of information security. A well-conducted awareness campaign can help teach and make users aware of emerging threats. This can also help to educate users on the right channels to follow in reporting security incidents. To remain effective, awareness campaigns must not be a once-off exercise, but they should be held periodically as new threats and countermeasures are introduced.

Incident response and recovery is in sixth place on the list of Computer Fraud & Security, whereas in the other publications it is nowhere near the top five. It also does not feature in the top five of either the CSI/FBI or the SANS report. After the 9/11 terrorist attacks one would have expected this topic to be among the top security issues being discussed. But this is not the case. This issue is very important in planning for the unthinkable disasters well in advance. For those vulnerabilities that can never be prevented (natural disasters), it is more beneficial to direct more resources to the recovery from loss, rather than to try and defend against them. Therefore incident response and recovery must be considered to secure information systems.

Another issue of prime concern is that of the human aspect of information security. Naturally human beings are fallible - between system designers and system users mistakes are inevitable. There is much that security design experts can learn from the designers of high reliability organisations (HROs) that embrace human fallibility ("to err

is human"). Errors or failures are inevitable and are to be expected. Security design experts should learn more from errors and failures than from successes as the designers of HROs do. Reason (2000) argues that although the fallible human condition cannot be changed, the conditions under which human beings work can. Therefore, most studies must be devoted to research on how human beings interact with IT systems and how security problems arise from such interactions (cyber deviance). This can help build secure systems that will reduce errors and restrict their effects to a minimum or acceptable level.

To summarise all the findings, the current information security landscape is moving towards a more strategic approach. The strategic approach to information security management is nowadays commonly referred to as Information Security Governance. Theoharidou et al. (2005) contend that information security has emerged as a new paradigm that requires a multidisciplinary approach.

4. Conclusion and Future Work

Information security has moved from the era of mainframe computers up to the current state of the complex Internet. With new developments and innovations, new risks came along. The survey results has shown that as we entered the twenty-first century, the scope of information security has widened and its focus is fast shifting towards a strategic governance one. Security issues now require a more coordinated and focused effort from the national and international society, governments and the private sector. It is no coincidence that the study shows a shift towards legal and regulatory compliance, risk management and digital forensic fields.

The survey's findings have also shown that most of today's security challenges are to a greater extent related to the human and organisational aspects (Anderson, 2007) of security. All indicators points to a multi-disciplinary approach in the future development of the information security discipline. However, as we move forward to address the new challenges it is also critical that we continue strengthening the technologies. New research efforts is required that minimise the gap between regulatory issues and technical implementations.

5. References

Anderson, K. (2007), Convergence: A Holistic Approach to Risk Management, Elsevier, Network Security, Vol. 2007, No. 5, pp. 4 – 7.

Anderson, R. (in press), Security Engineering: A Guide to Building Dependable Distributed Systems.

Botha, R.A. and Gaadingwe, T.G. (2006), Reflecting on 20 SEC Conferences, Computers & Security Volume 25, pp- 247–256.

Carey, L. (2008), The Evolution of Computer Virus and Anti Virus Protection, Available online at:http://www.identitytheftsecrets.com/the-evolution-of-computer-viruses-and-anti-virus-p.html, last accessed on 14 July 2008.

Computer Fraud & Security (2007), IDs Sell for Much More than Credit Card Numbers in the Underground, Editorial News, Computer Fraud & Security, Volume 2007, no.12, pp. 2

Computer Fraud & Security News (2007), UK Police Bust Fraud Gang, Elsevier Ltd, Computer Fraud & Security July 2007 Edition, Vol. 2007, Issue 6, p 2.

Conner, F.W. and Coviello, A.W. (2004), Information Security Governance: A Call to Action, Corporate Governance Task Force Report of 2004.

Conray-Murray, A. (2003), Strategies & Issues: Justifying Security Spending. Available online at http://www.itarchitect.com/articles/NMG20020930S0002.html, last accessed on 18 July 2007.

CSIA (2007), CSIA Compilation of Data Sources for Information on Cyber Security Issues. Available online at www.csialliance.org/resources, last accessed on 13 August 2007.

Cybertrust (2005), Justifying Security Spending: How to Make a Business Case for Information Security, Available online at: http://www.cybertrust.com/media/white_papers/cybertrust_wp_security_spending.pdf, last accessed on 13 August 2007.

Denning, E.D. (1999), Information Warfare and Security, ACM Press, United States of America.

Denning, P.J. (1991), Computers Under Attack: Intruders, Worms, and Viruses, Addison-Wesley Publishing Company, United States of America.

Eppel, N. (2005), Security Absurdity: The Complete, Unquestionable, and Total Failure of Information Security. Available online at http://www.securityabsurdity.com/failure.php, last accessed on 16 July 2007.

Gelbstein, E (2006), Information Security for Policy Makers: What it means- Why it matters- What to do about it? Available online at http://www.unitarny.org/mm/File/Webinars/Unitar%20eg%20presentation%2030_08.pdf, last accessed on 14 August 2007.

Gordon, L.A., Loeb M.P., Lucyshyn, W. and Richardson, R. (2006), CSI/FBI Computer Crime and Security Survey 2006 Report, Available online at www.abovesecurity.com/doc/CommuniquesPDF/FBISurvey2006.pdf, last accessed on 6 May 2007.

Information Commissioner (2006), What Price Privacy? The Unlawful Trade in Confidential Personal Information, Information Commissioner's Office, Available online at: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf, last accessed on 14 July 2008.

MacMillan, R. (2008), New Rootkit Uses Old Trick to Hide, IDG News Service, Available online at: http://www.pcworld.com/article/141300/new_rootkit_uses_old_trick_to_hide.html, last accessed on 14 July 2008.

Ormerod, P. (2003), Sunday Times Article, Available online at http://www.paulormerod.com/current.html, last accessed on 5 May 2007.

Pearson Education (2007), Computers and the Internet, Fact Monster, Available online at http://www.factmonster.com/ipka/A0872842.html, last accessed on 4 July 2007.

Petreley, N. (2004), Security Report: Windows vs. Linux, The Register, Available online at: http://www.theregister.co.uk/security/security_report_windows_vs_linux/, last accessed on 14 July 2008.

Pfleeger, C.P. and Pfleeger, S.L. (2007), Security in Computing, Fourth Edition, Prentice Hall, United States of America.

Reason, J. (2000), Human Error: Models and Management, BMJ 2000, Volume 320, pp 768-770. Available online at http://www.cs.up.ac.za/download.php/AIP780/Papers/

Reason_2000_Human_error_models_and_management_BMJ.pdf, last accessed on 29 August 2007.

Romer, H. and White, W. (2006), Security Inside Out, Oracle Security Solutions. Available online at www.oracle.com, last accessed on 19 July 2007.

Rusell, D. and Gangemi, G.T. (1991), Computer Security Basics, O'Reilly& Associates, Inc. United States of America.

SANS Institute (2006), The Ten Most Important Security Trends of the Coming Year. Available online at http://www.sans.org/resources/10_security_trends.pdf, last accessed on 4 July 2007.

Schneier, B (2003), The Speed of Security, IEEE Security and Privacy, Vol. 1, Issue 4, Jul/Aug 2003.

Schneier, B. (2007), The Psychology of Security (Draft). Available online at http://www.schneier.com/essay-155.html, last accessed on 13 March 2007.

Sophos (2007), Sophos Security Threat Report July 2007. Available online at http://www.tradepub.com/free/w_soph08, last accessed on 13 August 2007.

Stoll, C. (2000), The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, 1st Edition, Pocket, United States of America

Sural, S. (2006), Information Security: Brief History and Current Perspective. Available online at http://egovstandards.gov.in/, last accessed on 8 August 2007.

Symantec Internet Security Threat Report (2007), Trends for July – December 06, Vol. XI. Available online at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_emea_03_2007.en-us.pdf, last accessed on 13 August 2007.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2005), The Insider Threat to Information Systems and the Effectiveness of ISO 17799, Computers & Security, Vol. 24, pp 472-484.

Volker, T. (2007), Security Goes From Tactical to Strategic. Available online at http://www.mydigitallife.co.za, last accessed on 13 August 2007.

Zetter, K. (2003), Just Say No to Viruses and Worms, Available online at: http://www.wired.com/techbiz/it/news/2003/09/60391?currentPage=all, last accessed on 15 July 2008.

Appendix E: BC3I – Towards requirements specification for preparing an Information Security budget

MT Dlamini[1], MM Eloff[2], JHP Eloff[1,3], K Hone[1]

[1]Information and Computer Security Architectures Research Group
Department of Computer Science, University of Pretoria, South Africa
[2]School of Computing, UNISA, Pretoria, South Africa
[3]SAP Meraka UTD, CSIR, South Africa
{[1]mdlamini, [3]eloff}@cs.up.ac.za,
Tel.:+27129999100
[2]eloffmm@unisa.ac.za,
Tel.:+27124296336
[1]KarinH@tebabank.com
Tel.: +27115185619

ABSTRACT

The entire business landscape finds itself on the verge of a recession because of ongoing global economic turmoil. Thus, there is a heightened need to minimise and mitigate business risk and scrutinise information spending while ensuring compliance with regulatory mandates. This calls for decision makers to become vigilant in their spending and move towards an optimised information security investment. The main aim of this paper is to provide decision makers with a set of requirements to be considered when implementing a cost-effective and optimal information security budget; in a manner that preserve organisations' information security posture and compliance status. Research reported on in this paper forms part of an ongoing project known as the BC3I (Broad Control Category Cost Indicators) framework.

KEY WORDS

Information security spending, requirements, controls, economics, information security breaches, regulatory compliance.

Introduction

Information security is a continuously changing discipline that requires continuous adaptation to new and ever-changing information security threats, countermeasures and the global business landscape. The global business landscape is on the verge of facing a recession following the ongoing global economic turmoil. This came as a result of the collapse of the United States of America's sub-prime mortgage market (Kiviat, 2009). Organisations must quickly adapt to the prevailing economic climate by becoming more vigilant in their spending in general and more so on overheads such as information security expenditure (Researchandmarkets, 2007; Tipton & Krause, 2003; Timms, 2004).

Alas, despite the lingering global economic turmoil and encouraging developments in information security, a survey conducted by Symantec late last year (2008) revealed that the global *underground* economy is booming at millions of dollars in advertised goods and services (Symantec, 2008; Ko, 2008). While the whole world is in the worst economic crisis, the underground economy continues to flourish.

Despite all the years of hard work on information security technology improvements, harsh compliance regulatory penalties and more coordinated law enforcements, information security breaches are still ubiquitous and have seriously damaging consequences (Grossklags, Chuang & Christin, 2008; Fumey-Nassah, 2007; Schneier, 2002). Clearly, something is not working effectively in the information security arena.

Are the organisations putting in enough effort to protect their information assets or are they not taking any precautions? Is it too little or just enough or more? How much is really enough? This paper investigates the requirements to provide input for the preparation of a budget for information security. Research done in preparation of this paper is part of an ongoing project known as the BC3I framework (Broad Control Category Cost Indicators) (Dlamini, Eloff & Eloff, 2009).

The remainder of the paper is structured as follows: Section 2 gives a brief background on the economics of information security; Section 3 discusses related work on information security investment; Section 4 discusses the requirements to be considered when implementing a cost effective information security, and Section 5 concludes the paper.

Related Work

The field of economics of information security has become an important field of study (Tsiakis & Stephanides, 2005; Huang, Hu & Behara, 2006; Anderson & Moore, 2006; Anderson & Moore, 2007). For the past seven years, researchers have identified several topics of interest but this paper focuses only on **the economics of information security investment** (Gordon & Loeb, 2002; Camp, 2006; Anderson & Moore, 2006; Grossklags, Christin & Chuang, 2008; Hulthen, 2008).

The related literature investigated for this research project is structured as follows:

- A brief overview of the field of the economics of information security investment.

- Optimal allocation of resources to information security activities, with specific reference to the work of Gordon and Loeb (2002).

The Economics of Information Security Investment

This paper focuses on the topic of information security investment which is viewed from two opposing perspectives: either from the system defender's or the attacker's point of view.

Investing in information security is a trade-off; organisations can either choose to invest in security or not to invest (Anderson, 2001; Ioannidis, Pym & Williams, 2009). There are both direct and indirect benefits and costs involved. Directly, investing in information security reduces the risk exposure – though at an opportunity cost of other profitable investment. Not investing in information security guarantees more money – but at an opportunity cost of not having secure information assets. Indirectly investing in information security can help those who have not invested to "a free ride". Those who do invest, could easily become victims of threats that come from those who fail to invest (what economists call externality). Information security practitioners have to consider the trade-offs and related issues when they scrutinise and make information security investment decisions.

Given the current threat landscape, the consequences of not investing in information security can prove to be more costly than the consequences of investing (Fumey-Nassah, 2007). Chapman (2009) highlight that organisations are losing billions of dollars because of information security breaches. The amount of time and effort that is involved in recovering from an information security breach, besides compliance fines and penalties to be paid is also a cause of concern. Over the years, organisations have therefore been left with no option but to invest in information security.

An Optimal Allocation of Funds to Information Security

Organisations need adequate information security at a reasonable cost. For information security to make business sense; organisations must strike the right balance between the likelihood of risk and the cost to reduce such risk (Su, 2006). This has proven not an easy task to do. Goetz and Johnson (2006) point out that a majority of executives view information security as a "bottomless pit that never gets full" and some see it as "necessary evil that hinders productivity" (Conray-Murray, 2003). This is mainly due to the failure of information security managers to quantify their expenditure and the likelihood of the risk, faced by the information assets materialising. This failure has led executives to ask "how much is really enough for information security?"

In answering the fore-going question and contrary to the views of "a bottomless information security pit that never gets full"; researchers argue that there is actually an optimal point for information security spending (Anderson, 2001; Huang, Hu & Behara, 2008) which several researchers have tried to determine. It is not advisable to invest below or beyond this point.

Huang et al. (2006) use an economic model to determine optimal information security spending for organisations under multiple attacks. Modelling with variables such as system vulnerability, potential loss, budget and investment effectiveness, they demonstrate how to optimally allocate information security investments.

Wang and Song (2008) propose modelling with information security requirements, opportunity costs of the risks and budget constraints. They use a multi-objective decision-making framework to determine the optimal information security investment. Unfortunately, the modelling approaches discussed in both Huang et al. (2006) and Wang and Song (2008) do not provide a definite figure or the exact point of optimality for an information security investment. Srinidhi et al. (2008) also present a model to assist information security managers to optimally allocate financial resources to information security so as to guarantee productivity and the safety of information assets.

In 2002, Gordon and Loeb proposed an economic model (G&L model hereafter) to determine the optimal allocation of funds among different assets with different vulnerabilities to information security. Unlike the work of Huang et al. (2006) and Wang and Song (2008), their findings show that the optimal investment for protecting an information asset must at least be less than or equal to 37% of the total loss expected of the information asset. Willemson (2006) reviewed and refuted the G&L model's claim. Relaxing this model's assumptions, Willemson provided a function that suggests an investment of up to 50% and even up to 100% of the expected loss of an information asset.

Tanaka, Matsuura and Sudoh (2005) subsequently conducted an extensive empirical study using the G&L model. Their work investigates the relationship between information sharing and vulnerability levels and how it influences the decisions on information security investments. Liu et al. (2007) also conducted an empirical study on the G&L model to verify the relationship between the effects of an information security investment and the vulnerability level. Matsuura (2008) remarks that the G&L model derive it's economic benefit from threat reduction, but concludes that this is not sufficient. Therefore Matsuura extended the G&L model to include a measure of productivity.

Huang et al. (2008) have since extended the G&L model to include a risk-averse decision maker instead of a risk-neutral decision maker and adopted the expected utility theory. They have modelled the relationship between potential loss, the extent of risk aversion and the effectiveness of an information security investment. The majority of the work done seems to concentrate on how much to invest in information security. However, several important shortcomings still exist as pointed out in the next paragraph.

Recommendations drawn from the reviewed literature

The problem with the current body of knowledge is that it does not provide or recommend a set of requirements that decision makers have to consider when they develop their budgeting models. Requirements can act as a bridge in attempting to solve the problem of optimal resource allocation for information security.

Furthermore, decision makers need to provide evidence of the success of their information security spending. Due to the difficulty in establishing the monetary value of

information security benefits, requirements can also be used to act as the measure of success or failure of models for the allocation of resources.

Requirements elicitation is therefore an acceptable departure point in the attempt to find solutions to the optimal and effective allocation of funds for information security.

Requirements

The need for efficient and effective budgeting and spending on information security is driven by a number of different high-level requirements, ranging from technological to strategic issues. The elicitation of requirements for preparing an information security budget as proposed in this paper is structured as follows:

- *Requirements gleaned from existing approaches*
- *Additional requirements*

3.1 Requirements gleaned from existing approaches

The following list of requirements was identified from literature as referenced in this paper:

- Information security should be viewed as a multi-disciplinary field and therefore the budget should reflect implementation issues across the spectrum of people, process and technology.
- The budget should reflect implementation issues on the defence as well as attack side, i.e. proactive versus reactive.
- Careful consideration should be given to striking a balance between following a "standard-of-due-care" approach and following an approach based on risk assessment.
- An information security budget should address more than merely regulatory and standards compliance.

An information security budget should be based on assumptions clearly communicated to senior management, with specific reference to the % coverage of vulnerability exposure as well as the % acceptable risk levels.

Additional Requirements

The authors of the paper in hand have identified the following additional requirements to be considered when preparing a budget for information security:

- Taking cognisance of the three organisational levels
- Compiling and using a well-defined Information Security Architecture
- Other non-functional requirements

Taking cognisance of the three organisational levels

Cognisance has to be taken of the three well-known organisational levels, namely strategic, tactical and operational. These levels are to be used as a framework for organising the proposed requirements (Rolfsdotter Karlsson, 2008).

Strategic Level

On the strategic level, the budget for information security should be aligned with the vision and mission statement of the organisation, the business goals, legal obligations, overall risk appetite and policy statements. Any money spent should be in direct support of realistic and reachable business goals and priorities of the organisation. The business goals are derived from the vision, mission and values that are translated into the critical success factors of the organisation (Rolfsdotter Karlsson, 2008). This ensures that information security programmes are tightly coupled to the overall business strategy.

Legal obligations are stipulated in national and international regulatory requirements and laws. Organisations are forced to adhere to these or face prosecution if they do not.

Industry related laws and regulations must also be taken into account. Policy documents may also confirm the intent of an organisation, for example to protect the privacy of third parties. A policy describes the specific steps that an organisation will take and expects its employees to adhere to these in order to reach the organisation's business goals.

Tactical Level

The tactical level includes risk analysis for the identification of threats; standards and any compliance requirements. Thus it plays an important role in identifying threats to the security of information assets. It plays a guiding role in deciding 'how much' to spend on 'what'. Butler (2003) identifies a number of shortcomings of risk analysis, such as that exact investment decisions have to be made based on 'guesstimated' information.

Compliance with international standards also influences the spending on information security. Many countries have equivalent standards on national level that reflect ISO/IEC 27002, such as the British Standard BS ISO/IEC 27002:2005 and the AS/NZS ISO/IEC 17799:2006 standard in New Zealand and Australia.

Operational Level

On the operational level, both operational and technological requirements need to be considered. Operational requirements include aspects such as affordability of manpower, resources, optimal protection levels and feasibility. Furthermore, the operational level includes administrative requirements referring to guiding the user's actions to meet business goals and objectives as specified on the strategic level.

Technological requirements include both ICT infrastructure components such as controls on the hardware and software levels. When selecting controls, identification of an optimal mix of controls is of vital importance.

Compiling and using a well-defined Information Security Architecture

Eloff and Eloff (2005) proposed a number of requirements for the establishment of an information security architecture. These requirements – originally defined for developing information security architecture – can also be translated into requirements for information security budgets. The requirements state that information security architecture should

- **be holistic and encompassing**: The budget for information security should indeed be holistic and refer to the full spectrum of controls to be implemented. The requirement of holism involves the inclusion of all aspects when budgeting for security. the budget should not focus on isolated aspects but on all aspects.
- **make suggestions on how different controls can be synchronised and integrated to achieve maximum effect**: Very few organisations today spend enough time on the synchronisation and integration of controls, resulting in a potential over expenditure and duplication of controls. The synchronisation and integration of controls in most cases are organisation specific.
- **include a comprehensive approach to information security risk management**: The relationship between a comprehensive approach towards risk management and the information security budget is self-explanatory as the budget for information security should very clearly indicate how much risk mitigation is planned for, as well as the acceptable risk that the organisation will endure.
- **be measurable to demonstrate adherence to the requirements as set out**. Research has shown that it is somehow difficult to establish the monetary value of information security controls and of the benefits derived (Abrams et al., 1998; Conrad, 2005; Pfleeger & Pfleeger, 2007; Srinidhi et al., 2008). Despite these difficulties, the results should be expressed in monetary terms.

Other non-functional requirements

Non-functional requirements are viewed as those that impose constraints on the compilation of the budget for information security. Previous work done by the authors of this paper, as reported in Dlamini et al. (2009), suggest the following high-level non-functional requirements:

- **Flexibility**: This requirement recognises the fact that organisations are different and that they exist in different sectors. One prescribed solution regarding information security controls will not satisfy the requirements of all organisations.
- **Cost effectiveness:** Organisations must be able to identify and implement those controls that will protect their information resources in the most cost-effective way. Implementing all the controls may be a matter of "overkill", thus just "enough" should be implemented.

Lastly, the existing and current information security budget must not be ignored as a valuable input into future budget definitions. The existing budget will also shape where recurring costs must be budgeted for, e.g. licensing fees on information security tools, hardware upgrades on information security technology.

SUMMARY

In a nutshell, the UML diagram depicted in Figure 1 is used to model the requirements for preparing an information security budget as proposed in this paper.

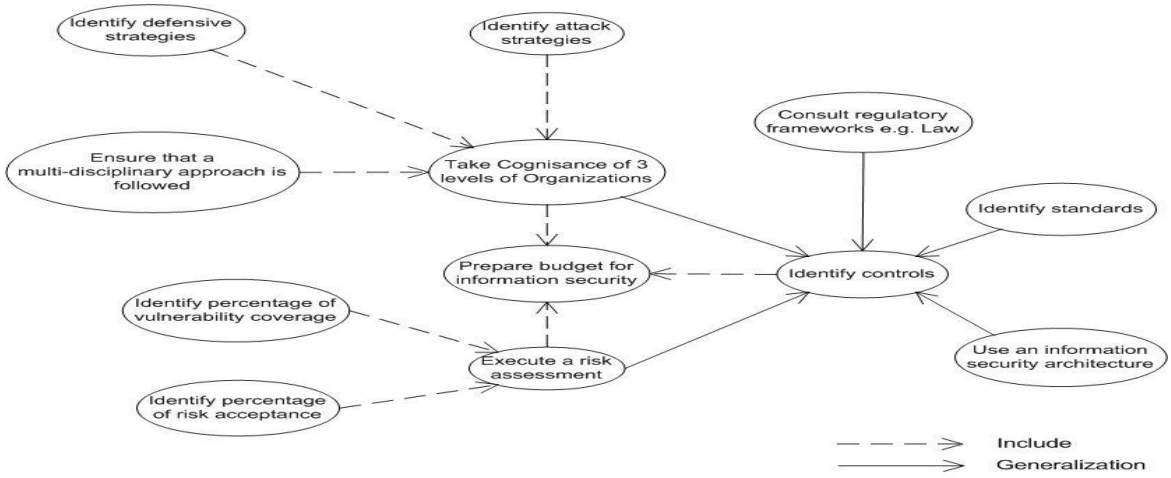


Figure 1: Use case and collaboration diagram for preparing an information security budget

Consider the above diagram. The identification of controls can be generalised as being the output of activities such as controls identified by means of regulatory investigations, standards, use of information security architecture, risk analysis, as well as cognisance of the three organisational levels. These generalisations are depicted by fixed lines whereas the broken lines show activities that should be included in the activity when preparing a budget for information security.

Conclusion

The current economic crisis is affecting organisations world-wide and all are required to spend money wisely. This also applies to spending on information security. Current models and approaches to determine *how much* to spend on *what* in order to safeguard information assets do not consider the total picture of an organisation and the

environment in which it operates? In this paper the authors approached this problem holistically and identified the requirements to be considered when preparing an information security budget. These requirements are presented in a "use case" diagram that illustrates the potential interaction between the different components.

Acknowledgments:
The support of SAP Research CEC Pretoria towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the authors and cannot necessarily be attributed to SAP Research.

References

Abrams, M.D., Johnson, C.M., Kahn, J.J. and King, S.G. (1998) Considerations for Allocating Resources for Information Security. Available online at www.c4i.org/caris.pdf, accessed on 09 February 2009.

Anderson, R. (2001) Why Information Security is Hard – An Economic Perspective, the *17th Annual Computer Security Applications Conference*, 10 - 14December 2001, New Orleans, Louisiana, USA.

Anderson, R. and Moore, T. (2006) The Economics of Information Security, *Science* 314(5799): 610-613, 27 October 2006.

Anderson, R. and Moore, T. (2007) Information Security Economics – and Beyond. Available online at: http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf, accessed on 12 January 2009.

Butler, S.A. (2003) Security Attribute Evaluation Method, PhD Thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213, USA.

Camp, L.J. (2006) The state of Economics of Information Security, *I/S: Journal of Law and Policy*, 2(2): 189-205.

Chapman, G. (2009) Cybercrime losses top $US1 trillion. Available online at: http://www.australianit.news.com.au/story/0,24897,24997483-24169,00.html, accessed on 19 February 2009.

Conrad, J.R. (2005) Analyzing Risks of Information Security Investments with Monte-Carlo Simulations, *Fourth Workshop on the Economics of Information Security*, 2-3 June 2005, Kennedy School of Government, Harvard University.

Conray-Murray, A. (2003) Strategies & issues: justifying security spending. Available online at: http://www.itarchitect.com/articles/NMG20020930S0002.html; accessed on 18.July 2007.

Dlamini, M.; Eloff, J.H.P. and Eloff, M.M. (2009) BC3I – A Model for Information Security Cost Indicators, submitted to the *Journal of Research and Practice in Information* Technology.

Eloff J.H.P. and Eloff M.M. (2005) Information Security Architecture, *Computers Fraud & Security*, 2005(11): 10-16, Nov 2005.

Fumey-Nassah, G. (2007) The Management of Economic Ramification of Information and Network Security on an Organization, *Proceedings of the Information Security Curriculum development Conference '07*, 28 – 29 September 2007, Kennesaw, Georgia, USA.

Goetz, E. and Johnson, M.E. (2006) Embedding Information Security Risk Management into the Extended Enterprise: An Executive Workshop, *MacNamee Center for Digital Strategies*, Tuck School of Business at Dartmouth University, USA. Available online at http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CIO_RiskManage/Overview.pdf, accessed on 18 February 2009.

Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investments, *ACM Transactions on Information and System Security*, (5)4: 438-457, November 2002.

Grossklags, J., Chuang, J. and Christin, N. (2008) Security Investment (failures) in Five Economic Environments: A Comparison of Homogeneous and Heterogeneous User Agents, *The Seventh Workshop on the Economics of Information Security*, 25 -28 June 2008, The Center for Digital Strategies, Tuck School of Business at Dartmouth College, Hanover, USA.

Huang, C.D., Hu, Q. and Behara, R.S. (2006) Economics of Information Security Investment in the Case of Simultaneous Attacks, *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 26-28 January 2006, Robinson College, University of Cambridge, England.

Huang, C.D., Hu, Q. and Beraha, R.S. (2008) An Economic analysis of the optimal information security investment in the case of a risk averse firm, *The International Journal of Production Economics*, 2008(114): 793 - 804

Hulthen, R. (2008) Communicating the Economic Value of Security Investment: Value at Security Risk, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Ioannidis, C., Pym, D. and Williams, J. (2009) Investments trade-offs in the Economics of Information Security, *the thirteenth Proceedings of the conference of Financial Cryptography and Data Security*, 23 – 26 February 2009, Barbados, USA.

ISO/IEC 27002:2005, July 2007 *Information technology - Security techniques - Code of practice for information security management*, renumbered in 2007.

Kiviat, B. (2009) How to Fix the Housing Market, Times Magazine. Available online at: http://www.time.com/time/magazine/article/0,9171,1879184-2,00.html, accessed on 19 February 2009.

Ko, C. (2008) Underground Economy Booming Online, Says Symantec, IDG News Service. Available online at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9123142&source=rss_ind130, accessed on10 January 2009.

Liu, W., Tanaka, H. and Matsuura, K. (2007) Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, Regular Paper, *IPSJ Digital Courier*, 3: 585 – 599.

Matsuura, K. (2008) Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, *The Seventh Workshop on the Economics of Information Security*, 25-28 June 2008, Hanover, USA.

Pfleeger, C.P. and Pfleeger, S.L. (2007) *Security in Computing*, 4th edition, Pearson Education, Inc, United States.

Researchandmarkets (2007) IT Security Market Report 2007, UK. Available at: http://www.bharatbook.com/productdetail.asp?id=11035, accessed [18 February 2009]

Rolfsdotter Karlsson, A., (2008) *Managing Performance Measurement: A study of how to select and implement performance measures on a strategic, tactical and operational level*, Master's Thesis, University of Gävle, Sweden.

Schneier, B. (2002) Computer Security: It's the Economics, Stupid, 1st Workshop on the *Economics of Information Security*, 16 -17 May 2002, University of California, Berkeley, USA.

Srinidhi, B., Yan, J. and Tayi, G.K. (2008) Firm-level Resource Allocation to Information Security in the Presence of Financial Distress, *Working paper Series 2008-17*, School of Economic Sciences, Washington State University, USA. Available online at www.ses.wsu.edu/PDFFiles/WorkingPapers/Yan/Srinidhi_Yan_GiriJune2008MISQ.pdf, accessed on 09 February 2009.

Su, X. (2006) An Overview of Economic Approaches to Information Security Management, Technical Report TR-CTIT-06-30, *Centre for Telematics and Information Technology*, University of Twente, Information Systems Group, Enschede, ISSN 1381 – 3625, Netherlands.

Symantec (2008) Symantec Report on the Underground Economy (July 2007 – June 2008), Whitepaper. Available online at: eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf accessed on 09 January 2009.

Tanaka, H., Matsuura, K. and Sudoh, O. (2005) Vulnerability and Information Security Investment: An Empirical Analysis of e-local Government in Japan, *Journal of Accounting and Public Policy*, Elsevier, 2005(24): 37-59.

Timms, S. (2004) Information Security Breaches Survey 2004: Executive Summary, PriceWaterhouseCoopers, Department of Trade and Industry, UK. Available online at: http://www.entrust.com/resources/pdf/ukdti_infosecbreachessurvey2004_execsumm.pdf, accessed on 18 February 2009.

Tipton, H.F. and Krause, M. (2003*) Information Security Management Handbook, 5th Edition*, Auerbach Publication, New York, USA.

Tsiakis, T. and Stephanides, G. (2005) The Economic Approach of Information Security, *Computers & Security*, 24(2): 105-108.

Wang, Z. and Song, H. (2008) Towards an optimal information security investment strategy, *IEEE Conference on Networking, Sensing and Control 2008*, April 6 – 8, 2008, pp. 756 – 761.

Willemson, J. (2006) On the Gordon and Loeb Model for Information Security Investment, presented at *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), University of Cambridge, UK, 26-28 June 2006. Available online at http://www.ut.ee/~jan/publ/economics.ps, accessed on27 November 2007.