INFORMATION SECURITY AWARENESS: GENERIC CONTENT, TOOLS AND TECHNIQUES

HOPE MAUWA
INFORMATION SECURITY AWARENESS: GENERIC CONTENT, TOOLS AND TECHNIQUES

By

HOPE MAUWA

Submitted in fulfilment of the requirements for the

MAGISTER TECHNOLOGIAE
DEGREE
in
INFORMATION TECHNOLOGY

in the

FACULTY OF ENGINEERING, BUILD ENVIRONMENT AND INFORMATION TECHNOLOGY

at the

NELSON MANDELA METROPOLITAN UNIVERSITY

December 2006

Supervisor: PROFESSOR R VON SOLMS
My grateful thanks go to the following people:

My promoter, Professor Rossouw von Solms. His expertise knowledge, guidance, and support played a major role in the completion of this project.

Ms Bron Kaplan, for her language direction in the writing of the thesis. You are a star.

My friends, for their support and encouragement. Guys, you were always there whenever I needed someone to talk to.
Abstract

In today’s computing environment, awareness programmes play a much more important role in organizations’ complete information security programmes. Information security awareness programmes are there to change behaviour or reinforce good security practices, and provide a baseline of security knowledge for all information users. Security awareness is a learning process, which changes individual and organizational attitudes and perceptions so that the importance of security and the adverse consequences of its failure are realized. Therefore, with proper awareness, employees become the most effective layer in an organization’s security defence.

With the important role that these awareness programmes play in organizations’ complete information security programmes, it is a must that all organizations that are serious about information security must implement it. But though awareness programmes have become increasing important, the level of awareness in most organizations is still low. It seems that the current approach of developing these programmes does not satisfy the needs of most organizations. Therefore, another approach, which tries to meet the needs of most organizations, is proposed in this project as part of the solution of raising the level of awareness programmes in organizations.
DECLARATION

I _____________________________, hereby declare that:

The work in this dissertation is my own work.

All sources used or referred to have been documented and recognized.

This dissertation has not previously been submitted in full or partial fulfillment of the requirements for an equivalent or higher qualification at any other recognized educational institution.

___________________________
## Contents

### Chapter 1  Introduction

1.1 Introduction ........................................................................................................ 1  
1.2 Background ........................................................................................................... 2  
1.3 Problem Statement ........................................................................................... 4  
1.4 Objectives ........................................................................................................... 4  
1.5 Methodology ....................................................................................................... 4  
1.6 Layout of Project ............................................................................................... 5  

### Chapter 2  Business Information Today

2.1 Introduction .......................................................................................................... 7  
2.2 Characteristics of Business Information ........................................................... 7  
2.2.1 Confidentiality of business information ....................................................... 8  
2.2.2 Integrity of business information ................................................................... 8  
2.2.3 Availability of business information ............................................................... 9  
2.3 Value of Business Information ........................................................................... 10  
2.4 Protecting Business Information ......................................................................... 12  
2.4.1 Highly networked business condition and decentralized data .................... 12  
2.4.2 Regulatory issues ......................................................................................... 14  
2.5 The Role of Employees in Protecting Business Information ............................. 17  
2.6 Conclusion ......................................................................................................... 19  

### Chapter 3  Information Security Programmes

3.1 Introduction ......................................................................................................... 21  
3.2 Information Security Objectives, Vision and Mission ....................................... 22  
3.3 Business Information Security Programmes ...................................................... 23  
3.3.1 Start at the top ............................................................................................... 23  
3.3.2 Know the business ....................................................................................... 24  
3.3.3 Funding ......................................................................................................... 24
## Contents

5.2.3 Importance of information and information security .......... 54  
5.2.4 Basic information security concepts ................................ 54  
5.2.5 Threats to and vulnerabilities of computer systems .......... 55  
5.3 Typical Company-Specific Topics ......................................... 56  
5.4 Typical Generic Topics .......................................................... 57  
5.5 Benefits of a Generic Information Security Awareness Programme ... 58  
5.6 Conclusion .............................................................................. 59  

### Chapter 6 An Information Security Awareness Programme: Generic Content, Tools and Techniques

6.1 Introduction .................................................................................. 61  
6.2 Towards a Generic Information Security Awareness Programme .... 61  
6.2.1 The ISO/IEC 13335-3 ................................................................. 62  
6.2.2 The ISO/IEC 17799 .................................................................. 64  
6.2.3 The Internet ............................................................................. 66  
6.2.4 The author’s survey .................................................................. 67  
6.3 Generic Contents of an Information Security Awareness Programme . 76  
6.4 Tools and Techniques for Offering an Information Security Awareness Programme ........................................................................ 77  
6.4.1 Information security Website ...................................................... 77  
6.4.2 Onsite instructor-led training ...................................................... 78  
6.4.3 Non-Web, computer-based training ............................................ 78  
6.4.4 Interactive video training ............................................................ 79  
6.4.5 Security newsletters ................................................................. 79  
6.4.6 Educational contests ............................................................... 79  
6.5 Delivering the Generic Programme .................................................. 80  
6.6 Conclusion ................................................................................. 81  

### Chapter 7 A Generic Information Security Awareness Programme

7.1 Introduction .................................................................................. 82  
7.2 The Contents of a Generic Information Security Awareness Programme ........................................................................ 82
Appendix C
Survey analysis ....................................................................................................................................... 171

Appendix D
Research Paper................................................................................................................................... 200
Figures and Tables

Chapter 3      Information Security Programmes
3.1      Spheres of Security .................................................................35

Chapter 5      Generic Information Security Awareness and Education
5.1      Contents of Information Security Awareness Programmes ..........52

Chapter 6      An Information Security Awareness Programme: Generic Content,
Tools and Techniques
6.1      Importance of Business Information .......................................68
6.2      Importance of ICT Infrastructure .............................................69
6.3      Effects of Confidentiality Compromise ..................................69
6.4      Effects of Integrity Compromise ............................................70
6.5      Effects of Availability Compromise .......................................70
6.6      The Importance of Awareness Programmes ............................71
6.7      Attending an Awareness Programme .....................................71
6.8      Date the Programme was attended .......................................72
6.9      Interval in Offering an Awareness Programme .......................72
6.10    Preference for Taking an Examination ....................................74
6.11    Opinion on Offering a Certificate ..........................................75
Chapter 1

Introduction

1.1 Introduction

The value of information and information technologies in today’s business environment has become increasingly important with each passing day. Information is being used to support every aspect of business, from operations to managerial decision-making and strategic competitive advantage (O'Brien, 1999), and, as is the case with all other assets, information needs to be secured.

To protect information and its related systems from danger, such tools as policy, awareness, training and education, and technology are necessary (Whitman & Mattord, 2003). In today’s computing environment, it is not enough to have only physical and technical controls to adequately secure information and information systems. The maintenance of effective security is becoming more dependent on the vigilance of the users, since it has been proven that a motivated and educated user is the best defence against any unwanted security threat (Thomson & Von Solms, 1998).

Given the importance of educated staff as a security control, awareness is, therefore, the one to do the most important parts of an organization’s information security programme. As such, organizations must create programmes aimed at raising awareness of information security concepts, requirements and controls amongst staff, managers and technologists.

The current approaches of developing these programmes recommend that they should stem directly from already existing information security policies in organizations (ISO/IEC 17799, 2005; ISO/IEC 13335-3, 2005; Du Plessis & Von Solms, 2002). As such, organizations without policies in place do not always have a basis on which to frame their information security awareness programmes.
Chapter 1: Introduction

This has resulted in low levels of awareness programmes in most organizations according to some of the recently conducted surveys (Ernst & Young, 2004; Deloitte Touche Tohmatsu, 2005). Therefore, in this research project, a different approach to the development of such programmes, which tries to give a basis to most organizations, is spelt out.

1.2 Background

Every organization is unique, and as such, has different management instructions on how it should be run. These management instructions are what are called policies (Wood, 1994), and are seen as the basis for effective information security within an organization (ISO/IEC 13335-1, 2004).

For users to behave appropriately, they first need to be made aware of the security policies and procedures in place, and also need to know and understand how to implement the procedures supporting these policies (Thomson & Von Solms, 1998). This takes the form of an information security awareness initiative designed to change behaviour or reinforce good practices in all information users. Both ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005 advocate that these programmes should be based on the objectives, strategies and policies currently in place in organizations. Since security policies or organizations are usually different, it follows that awareness programmes that stem from these policies, are also different. This could be called a company-specific approach to information security awareness (Du Plessis & Von Solms, 2002) because the contents of these awareness programmes is mostly company-specific.

Despite the important role that these programmes play, and the widespread acceptance of them in current guidelines and standards, the level of information security awareness in most organizations is still low, as is illustrated by some of recently conducted surveys (Ernst & Young, 2004; Deloitte Touche Tohmatsu, 2005).
Chapter 1: Introduction

According to the Global Information Security Survey by Ernst & Young (2004), respondents named “lack of security awareness by users” as the top obstacle to effective information security. However, only 28% listed “raising employee information security training or awareness” as being a top initiative.

The survey also showed that less than half of the respondents provided their employees with ongoing training in security and controls. In the 2005 Global Security Survey, conducted by Deloitte Touche Tohmatsu – Australia (2005), respondents pointed to a host of continuing challenges to their businesses. Most prominent among them are the increasing sophistication of threats (63%) and the lack of employee awareness and training (48%), both of which may create an environment of exploitable vulnerabilities and weak operational practices. According to the same survey, overall, security awareness and training implemented or maintained had decreased from 77% in 2004 to 65% in 2005. Though experts recommend that 40% of an organization’s security budget be spent on awareness measures (MacBrige, 2000), the report has revealed that only 15% of it is spent on employee awareness and training while 64% of it is spent on security tools.

Basing an awareness programmes on existing policies only is a limitation to organizations that do not have such policies in place. A recent survey conducted by PricewaterhouseCoopers, Information Security Breaches Survey (2004) showed the number of UK businesses with security policies continues to rise. A third of all companies and two-thirds of large businesses now have one. The reason why some organizations do not have information security policies in place is that their development is a lengthy process that requires time, money and specialized knowledge. These constraints would not make such an effort feasible for small to medium-sized companies (Du Plessis & Von Solms, 2002).

The current lack of awareness programmes in most organizations suggests that a problem exists with the traditional method of basing these programmes on the policies and procedures already in place (Du Plessis & Von Solms, 2002). Therefore, a different approach to their development has to be cultivated.
Chapter 1: Introduction

1.3 Problem Statement

There is a low level of information security awareness in most organizations, which can be attributed to the current approach of only developing information security awareness programmes from existing information security policies and procedures already in place in organizations. The fact that many organizations do not have proper information security policies and procedures in place does not only suggest that the organizations are not serious about information security, but also tends to result in a lack of information security aware staff members.

1.4 Objectives

The primary objective of this research project is to identify general topics that can be included as part of the contents of an information security awareness programme, intended to be offered to international, interdisciplinary and diverse audiences, and to specifically find out the most effective techniques for delivering such a generic content. This will be accomplished by addressing the following secondary research objectives:

- Firstly, finding out if there is a generic content component in an information security awareness programme that can be offered to international, interdisciplinary and diverse audiences
- Secondly, finding out the level of detail that should be included in each topic
- Thirdly, finding out the effective techniques for delivering such a programme.

1.5 Methodology

It is important to understand the research philosophy and research methodology of this project to appreciate the resultant solution.
Information security awareness involves people, and as soon as people are involved, the project forms part of a social phenomenon, i.e., emphasis is more on meaning of the research than on the measurement thereof. Therefore, the research is more qualitative and interpretive oriented. Consequently, the research methods chosen are, therefore, more social-scientific oriented.

The project will start with a detailed **general literature survey** to determine the current international trends. Relevant information that has been published previously will be investigated.

This will be followed by a **focused literature survey** to determine topics that are included in current programmes. Along with this, an industry **investigation** will be done to determine topics included in company programmes that are known for sound information security. Based on the above, a **questionnaire** will be drafted and forwarded to a number of South-African companies. The objective of this questionnaire will be to determine the topics to be included in a generic programme as well as the level of detail in them.

Having **analysed** the results of the questionnaire, the common content of a generic information security awareness programme will be **argued**.

### 1.6 Layout of Project

The project is documented through a set of chapters. Chapter 2 focuses on the value of business information from different perspectives, showing the role it plays in various transactions nowadays, the need to protect it, and the role that employees play to do so. Chapter 3 concentrates on concepts pertaining to these programmes and discusses, among other things, key components that must be considered when structuring the programme, as well as some of the published frameworks for information security, layers of organizational influence in information security and the importance of human involvement in protecting information. Awareness programmes, as a way and means of developing and motivating employees, are discussed in Chapter 4.
Chapter 1: Introduction

Current company-specific approaches to the development of these programmes and their limitations are also discussed. It is then suggested that a different approach from the existing one has to be developed to try to raise the existing low level of awareness. Therefore, Chapter 5 is dedicated to discussing the proposed generic approach. The chapter discusses the contents of current programmes. Typical company-specific topics are discussed and finally, topics that can be catered for in a generic awareness programme are examined. Chapter 6 focuses on discussing how the contents of the proposed approach are identified and also discusses the tools and techniques suitable for delivering generic contents. Chapter 7 continues to discuss the generic approach by describing the topics identified in Chapter 6 in detail. Chapter 8 provides a brief conclusion of the chapters. It starts with a brief introduction of the area studied and then provides an overview of the various chapters. Lastly, possible future enhancements to the programme are pointed out.

The above-mentioned chapters are supplemented by a set of appendices, which contain the details included in the focus areas identified for a typical generic information security awareness programme, the questionnaire used in the survey and the complete analysis of the survey results.

An academic paper that resulted from this project is added as an appendix at the end of the dissertation.
Chapter 2

Business Information Today

2.1 Introduction

This chapter highlights the values of business information from different perspectives, showing the role that it plays in various transactions. The values of business information comes from its characteristics (Whitman & Mattord, 2003). Therefore, these key characteristics are discussed in order to highlight the need to preserve them and extract maximum value from business information.

Safeguarding business information has always been important, but nowadays, there is an increasing emphasis on its protection (Lewis, 2003). This is because this protection has been affected by some factors in the current business environment. These factors are explored in this chapter to highlight their impact on the protection of business information. Employees of an organization have a role to play in the protection of business information because they are generally the first to be impacted by security incidents, and, as such, they can prevent incidents and mitigate damage when incidents occur (Rudolph, Warshawsky & Numkin, 2002). This chapter also highlights their role in the protection of business information to show their importance as a security control.

2.2 Characteristics of Business Information

As previously stated, the values of business information come from its characteristics. Should any of these characteristics change, its values will change, occasionally increasing, but usually decreasing (Whitman & Mattord, 2003). Thus, to ensure that business information continues to provide useful support to an organization’s operations, its key characteristics need to be preserved (Posthumus & Von Solms, 2005).
All communities of interest within the organization must make sure that the characteristics are protected. These are discussed below.

2.2.1 Confidentiality of business information

Whitman and Mattord (2003) in “Principles of Information Security” define confidentiality as the quality or state of preventing disclosure or exposure of information to unauthorised individuals or systems. In an organization, this characteristic of confidentiality is especially important as it may involve personal information about employees, customers, or patients (Whitman & Mattord, 2003). They also highlight some measures that need to be implemented to protect the confidentiality of business information:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users.

Thus, sensitive business information should not be left freely available to whoever may wish to access it. Only those parties who have been given authorisation to access this information should be allowed to do so (Posthumus & Von Solms, 2005).

2.2.2 Integrity of business information

Integrity of information is characterised as the quality, or state of being whole, complete, and uncorrupted (Whitman & Mattord, 2003). Therefore, preserving the integrity of information resources involves maintaining the correctness and comprehensiveness of that information (Humphreys, Moses & Plate, 1998). Integrity is threatened when information is exposed to corruption, damage, destruction, or any other disruption of its authentic state. The threat of corruption can occur while information is being stored, processed, or transmitted (Whitman & Mattord, 2003).
A breach of integrity could result from the intentional modification of information by authorised parties, or even its unintentional modification (Thomson & Von Solms, 1998). Whitman and Mattord (2003) highlight some forces that undermine information integrity, which include:

- Viruses and worms
- Hackers
- Noise in the transmission media
- Low power signals carrying information can cause the receiving system to record data with inaccurate values.

The integrity of business information is important because it is used in the decision-making process. If the information is not accurate or complete, it could lead to misguided decisions (Thomson & Von Solms, 1998). Information integrity is the cornerstone of information systems, because information is of no value or use if users cannot verify its integrity (Whitman & Mattord, 2003). A well-known mechanism used to preserve integrity involves attaching a simple message digest to a message before its transmission (Thomson & Von Solms, 1998). This identifier can later be used to calculate if the sent message has been modified (Posthumus & Von Solms, 2005).

2.2.3 Availability of business information

An organization must ensure that information is accessible for use by the relevant parties, at the right time, by preserving the availability of information resources (Posthumus & Von Solms, 2005). However, availability, as defined here, requires the verification of the user as the one with authorised access to such information. Availability of business information is important because having the correct information at the right time enables organizations to make well-timed business decisions that enable them to gain competitive advantage. One of the common ways in which availability is compromised is through a denial-of-service attack (Posthumus & Von Solms, 2005).
During such an attack, an information system is bombarded with a large amount of information requests, which cannot be handled by the system. Thus, the system either slows down considerably or crashes, making information unavailable (Whitman & Mattord, 2003).

Unauthorized disclosure of business information, accidental corruption or deliberate manipulation of business information, and unavailability of business information for any length of time, can all have negative impacts. Therefore, it is imperative for any business to make sure that the confidentiality, the integrity and the availability of business information are maintained to preserve the values that it possesses, and go a long way in ensuring that such information retains its values to an organization and to the organization’s relevant stakeholders (Posthumus & Von Solms, 2005). The section that follows discusses the values of business information to an organization.

2.3 Value of business information

It is important for companies to attain maximum value from the information they have concerning suppliers, customers, competitors and global markets. Prentice (2005) in the paper “Five Steps to Evolving into an Intelligent, High-Performance Enterprise” states that proprietary information about customers, strategies and sales is the underpinning of success. He further states that in the old economy, product and service attributes were sustainable competitive differentiators. Today, that advantage fades quickly as competitors join the scene. The only remaining competitive advantage is quality information, which allows organizations to respond to constant external change with ongoing renewal and innovation (Prentice, 2005).

The standard of “Good Practice” according to the Information Security Forum (2005) lists some positive financial impacts that businesses may experience if information is kept confidential, available, and accurate:

- Gain of sales, orders or contracts
- Gain of tangible assets
- Avoidance of penalties/legal liability
Chapter 2: Business Information Today

- Predictable costs of business
- Appreciated share price.

The standard also lists some positive operational impacts: -
- Management control
- Competitive advantage
- New ventures open up
- Adherence to operational standards.

There are some positive customer-related impacts too: -
- On-time deliveries to customers or clients
- Gain of customers or clients
- Gain of confidence by customers
- Good reputation is kept.

As well as some positive employee-related impacts: -
- Increase in staff morale/productivity
- Avoidance of injury or death.

Companies that routinely use information effectively outperform their competitors by a wide margin. A proactive approach to information management enables organizations to uncover the hidden strengths of their product lines, implement better ways of running their businesses, discover new ways of approaching the market and learn how to better drive competitive advantage (IBM Software Group, 2005).

IBM Corporation (2005), highlights several benefits of turning business information assets into services: -
- Lower costs through an optimized infrastructure
- Gained insights through information analysis and discovery
- Managed risks and streamlined compliance
- Leverage information for business transformation
- Gained control over master data.
Chapter 2: Business Information Today

- Management of information complexity
- Business is run on measurement rather than on estimation
- Business practices are transformed from reactive tactics to real-time operations
- Decisions are made based on up-to-date, accurate and complete information
- Organizations work efficiently and securely with suppliers, partners and customers
- Organizations reduce overall IT costs by simplifying data management administrative tasks.

There are many values that business information can provide if its confidentiality, integrity and availability are not compromised. Protecting these characteristics has always been important but there are some factors in current business circumstances that have made this protection imperative. Highly networked business conditions, decentralised data and regulatory issues are some of the factors that need to be discussed.

2.4 Protecting Business Information

Business information, and the ability to access and distribute it, is the top strategic assets in today’s competitive business environment. Therefore, one of the fundamental elements of good practice is applying safeguards to business information proportionate to its importance in the running of the business. But protection of business information poses a lot of challenges in the current environment. Some of these challenges are discussed below.

2.4.1 Highly networked business condition and decentralized data

The need to use and communicate business information effectively and work more collaboratively has driven the extensive deployment of network-based communication systems (Check Point Software Technology Limited, 2004).
Chapter 2: Business Information Today

Networks and the Internet have enabled businesses to share information and services both within the enterprise and with business partners and customers. Networks and the Internet have contributed to the recent dramatic increase in global connectivity (Check Point Software Technology Limited, 2004). They have also enabled enterprises to run applications across geographically dispersed facilities.

Although the explosion of connectivity and information exchange provides tremendous benefits, it also exposes an organization’s sensitive information and mission-critical applications to potential unauthorised access, both through connections to the Internet and from within the enterprise. In addition, the transmission of data over the Internet also exposes the data to unauthorised interception (Check Point Software Technology Limited, 2004).

Open network connectivity means that many more users could potentially gain access to important, confidential data (Thomson & Von Solms, 1998). The growth in the use of networks, the Internet, and electronic commerce has meant that threats are no longer restricted to the organization, but have expanded to anyone in the world who has a personal computer with Internet access. The above developments have resulted in the opportunity for anyone who wants to compromise the security of business information being able to have multitudes of ways of gaining access to sensitive organizational information (Thomson & Von Solms, 1998).

Historical methods for securing information resources are therefore no longer adequate to meet the security requirements of today’s global networks. In the centralised mainframe environments that dominated the information systems landscape in previous years, organizations were able to secure a limited number of access points through physical barriers and controlled access to data through log-on procedures and password protection (Check Point Software Technology Limited, 2004).
Current distributed network environments, with multiple points of access and multiple network resources, make it impractical to secure every application and network resource individually. These risks create a critical need for enterprises to protect their information and information systems from unauthorised access and use (Check Point Software Technology Limited, 2004). In the current global, high-tech, information-oriented environment, with its exploding demands for both information sharing and information security, the importance of getting a better balance between information sharing and security is becoming critical to survival (Cartney, 1999).

Not only has the protection of business information been affected by highly networked business conditions and decentralised data in the current environment, but there are also many regulatory pressures driving this protection nowadays. Some of the regulations governing the protection of business information are examined below.

2.4.2 Regulatory issues

The increasing emphasis on business information protection has many regulatory drivers. Relevant legislations and regulations have been developed in various disciplines concerning the management of information in organizations. Information security legislation is developed and implemented to prevent misuse and inappropriate exploitation of information and information technology (Hermann, 2004). Legislation may dictate a particular format or media in which information must be kept. It may also dictate specific information that must be kept and specific uses of information which may be prohibited (Hermann, 2004).
Organizations often tackle security issues as part of their efforts to comply with a variety of regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX) (Lewis, 2003), the Gramm-Leach-Bliley Act and the BASEL II regulations in Europe (Enterprise Management Associates, 2005).

The financial world is impacted by Sarbanes-Oxley, which dictates new policies and procedures for financial reporting and auditing (Lewis, 2003). It is focused on a system of checks and balances regarding finance and accounting (Hermann, 2004) and it dictates, for example, how long financial records must be kept before they can be destroyed. The Act is mostly influential in the United States of America, and applies to all disciplines.

HIPAA addresses security policies and procedures that ensure secure access, transmission and retention of Personal Health Information (PHI). Therefore, protecting medical records is a compliance issue for hospitals, insurance companies, medical practices, laboratories, life-sciences firms, pharmacies, and even other non-healthcare companies that have PHI data in human-resource departments (Lewis, 2003). This Act is also influential in the United States of America, and applies in the health sector.

The Gramm-Leach-Bliley Act of 1999 was primarily aimed at handling financial transactions. It impacts on how financial data is treated for both online and traditional transactions. It specifically limits the disclosure of personal information by financial institutions to third parties. As with HIPAA, the Gramm-Leach-Bliley Act necessitates that privacy policies must be communicated to customers (Enterprise Management Associates, 2005). This Act too, is influential in the United States of America, and applies to financial institutions such as banks, securities firms, and insurance companies.

Regulations play a similar role in IT’s concerns about compliance in other countries.
The BASEL II regulations in Europe address disclosure, as well as the need for financial institutions to better assess risk in general (Enterprise Management Associates, 2005). The regulations will be implemented in European Union countries by the end of 2006 (Tripwire, 2006), and applies to financial institutions.

It is very important to note that as technology develops, so should legislation. Compliance means that companies have to adjust their business processes to protect their data (Lewis, 2003). Information security practitioners must understand the current legal environment, stay current with new laws and regulations and watch for new issues as they emerge, because they play an important role in an organization’s approach to controlling liability for privacy and security risks (Whitman & Mattord, 2003).

Compliance is costing most companies money, time and resources but it has a silver lining. Though it takes hard work in order to meet auditor’s requirements, IT organizations can achieve several tangible benefits that bring strategic value to the organizations. Some of the benefits are discussed below.

- Improve IT Operations

By establishing effective IT controls that are tested year-round, IT organizations streamline core IT operations processes through improved change management, direct access controls and security (Active Reasoning, 2005). Most importantly, the compliance process increases accountability within the IT organization. Since compliance places the spotlight on “who did what”, everyone within the IT organization is now cognisant of how their actions and activities directly affect the overall business.
Chapter 2: Business Information Today

- **Reduce Costs**

In “Managing IT Compliance: Simplicity and Sustainability for Future Audits” it was stated that by leveraging automated compliance tools, IT organizations dramatically cut their audit and compliance costs. These costs and the individual resources associated with them can be re-allocated back to the business for more strategic initiatives (Active Reasoning, 2005).

- **Increase Overall Compliance Score**

There are host of industry-specific compliance requirements that companies must meet. Strengthening core IT controls for change management and direct access also strengthens the IT organizations’ hand in with other health, financial, and federal compliance requirements (Active Reasoning, 2005).

With these challenges in the current environment, employees have come into play in the protection of information assets. Therefore, their role in the protection of these information assets needs to be discussed.

2.5 **The Role of Employees in Protecting Business Information**

In the modern computing environment, with highly networked business conditions and decentralized data, it is near impossible to secure business information adequately with only physical and technical controls. Organizations invest in information security technologies, such as antivirus software and firewalls, to protect information assets. However, they are left with significant information security risks as a result of accidental or deliberate actions and inactions of employees. Connecting computers through networks increases risk, and network security depends heavily on the cooperation of each and every user (Rudolph, Warshawsky & Numkin, 2002). Experts say that security is only as strong as the weakest link, and authorization and identification controls are useless if even a single user does not recognise the value of information assets that are being protected.
The maintenance of effective security is becoming more dependent on the vigilance of users, since it has been proven that a motivated and educated user is the best defence against any unwanted security threats (Thomson & Von Solms, 1998). An information security programme, which properly accounts for the strengths and weaknesses of employees, is essential to securing company’s business information. Information security is best achieved when cutting-edge technology is combined with a highly trained and motivated work-force that understands the basic practices that will assist in keeping an organization’s business information secure (Kathleen, 2003).

Employees should play an important role in keeping sensitive information safe and secure. By informing employees about information security and motivating them to comply with the controls, an organization establishes a widespread, lasting and deep-rooted “security culture” that reduces information security risks (IsecT, 2003.). Employees who have not been taught how to mitigate Internet threats properly can be responsible for serious security breaches (Kathleen, 2003). This can put an organization’s business at risk and damage the company’s relationships with its partners and customers. It is, therefore, essential that organizations build a human firewall. In Human Resource magazine “Closing the security gap: data protection initiatives should include employee training” by Coe Kathleen (2003) motivates that to create an effective human firewall, three key components should be considered:

- End-user awareness
- Specialized training
- Management awareness

Information security is a rapidly evolving field that must adapt to new threats quickly. While hardware and software firewalls should be maintained frequently, regular attention to the “human firewall” is equally as important, if not more so. Recurring evaluation and maintenance of employee awareness, specialized training and management awareness are all required components of a successful security programme (Kathleen, 2003).
Although the security risks caused by people cannot be totally eliminated, increasing the awareness of information security will spread knowledge, and thus increase understanding of information security concepts and objectives. Widespread understanding will increase the extent of support and commitment of employees to the rules and motivate them to improve security. Security improvements will increase compliance and reduce risks, making security breaches less likely and/or less costly (IsecT, 2003).

Empowering employees to serve as human firewalls may be the best way to protect internal resources that have a major impact on the success of the company, its partners and customers (Kathleen, 2003). An organization’s staff is generally the first to be impacted on by security incidents. Therefore, staff that is aware of security concerns can prevent incidents and mitigate damage when incidents do occur (Rudolph, Warshawsky & Numkin, 2002).

2.6 Conclusion

Business information is being used in almost all business transactions nowadays, and as such, it has become a valuable asset. Prentice (2005) states that information is no longer a transactional by-product of business; it is its life. For organizations to extract maximum values from business information, they have to protect its characteristics because organizations risk losing a host of factors such as reputation, market shares, direct revenue, etc, if it is not protected properly (Lewis, 2003). Any compromise on confidentiality, integrity and availability of business information has financial, operational, customer-related, and employee-related impacts on an organization.

The protection of business information has been impacted by many factors, such as modern highly networked business conditions and regulations. Legislation has affected how business information and records are managed in the business world today. Therefore, it is vital for an organization to understand the scope of its legal and ethical responsibilities in order to reduce its liabilities, reduce risks from electronic and physical threats, and to reduce the losses due to legal action.
Modern highly networked business conditions and decentralization of data have made the protection of business information much more difficult. Consequently, employees have a bigger role to play nowadays in protection of business information. The previously implemented physical (mantraps, etc.) and technical (access control, etc.) security measures alone are no longer adequate in this new computing environment (Thomson & Von Solms, 1998). Therefore, employees have to be made aware of security concerns so that they can assist in mitigating incidences.

Protection of business information requires comprehensive, well-designed, and reliable information security programmes (Stoneburner, Hayden & Feringa, 2001). Structures of information security programmes will be discussed in the next chapter to show that well-structured approaches are followed when protecting business information nowadays.
Chapter 3

Information Security Programmes

3.1 Introduction

The increasing importance of business information in most businesses today has meant that it has become imperative for organizations to protect this information. Protection of business information has therefore become a major issue that needs to be managed properly, and is one of the foremost issues that demand a business solution. Since information security, i.e., the protection of information and the systems and hardware that use, store, and transmit that information (Whitman & Mattord, 2003) plays an important role in protecting vital business information assets, this chapter starts by discussing the objectives, vision and mission of information security.

Research has shown that in order to implement an effective information security programme, there are some key components that must not to be overlooked (Lewis, 2003). Therefore, some of these components that need to be considered when structuring the programme are examined. Some of the published frameworks for information security will be discussed in this chapter to highlight the point that well-structured approaches should be followed to protect business information. Layers of influence in information security are later discussed, and these involve active participation of the three general organizational levels.

It was discussed in Chapter 2 that information security is best achieved when cutting-edge technology is combined with a highly trained and motivated workforce that understands the basic principles and practices. This chapter concludes by examining the importance of human involvement in the protection of business information assets.
3.2 Information Security Objectives, Vision and Mission

It is important for managers to understand how business information and information systems support an organization’s mission. That understanding helps managers to decide the level of protection needed for each piece of business information and information system. The objective of information security is protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity (IT Governance Institute, 2005). Basically, information security provide staff with a brief overview of the “acceptable use" of any of the information assets, as well as explaining what is deemed as allowable and what is not, thus engaging them in securing the company's critical systems (Danchev, 2003). Through the selection and application of appropriate safeguards, security helps an organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets (National Institute of Standards and Technology, 1998).

Information security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures protect important information assets and thereby support the overall organizational mission (National Institute of Standards and Technology, 1998). Therefore, it is important to note that information security rules and procedures should not be too difficult to use or be too time-consuming, because users may just ignore them.

Well-structured information security programmes support the mission of the organization by protecting vital business information assets. Some of the key components of these programmes need to be examined to gain more insight into the roles that they play.
Chapter 3: Information Security Programmes

3.3 Business Information Security Programme

Structuring an information security programme requires paying attention to key components that facilitate its success. The following are some of the key components that should not be overlooked:

3.3.1 Start at the top

Developing an information security programme begins with eliciting support from the Chief Executive Officer, senior management and board of directors. Senior management support for information security ensures that there is a committed information security awareness, adequate budget, and support for the security staff. Security experts state that there is no factor more influential than senior management setting the tone that information security is important, and that individuals, including senior and middle management, will be held accountable for their actions. Although setting the tone, by itself, will not repel a single external or internal attack, the controls that can safeguard an organization are made more effective with senior management’s support. With that support, the countless activities an organization performs take on purpose and direction and add to an organization’s strength (Ernst & Young, 2004).

The Global Information Security Survey results conducted by Ernst & Young (2004) suggested strongly that when senior management has a strong belief in the value of information security, the measures taken by that organization are more effective or, at least, confidence in them is high. The survey results, on the other hand, shows that where senior management was unsupportive, all concerned tend to ignore controls or, even worse, circumvent them, in the name of expediency, to the detriment of the organization.

Not only senior management support has an impact on the success of an information protection programme, it is also important that the business is known very well.
3.3.2 **Know the business**

Understanding the nature of the business is one of the key components of an information security programme. Understanding this will help to identify which is truly mission critical information that, if lost, would seriously harm the organization; which is critical information that, if lost, would have an impact, but would not cause the organization to fail; and which is useful, but not critical, information to the organization.

To provide effective information security, organizations must have a clear focus on what they seek to protect and the corresponding threats. Understanding the nature of the business and the corresponding threats enable an organization to focus its information security preparations on the credible threats rather than taking a reactive strategy (Ernst & Young, 2004). Experience has shown that it is easier to protect against a threat that an organization understands than to counter one that is an enigma. Once it has this understanding, it can take appropriate actions that make the most effective use of its resources (Ernst & Young, 2004). Consequently, decisions and actions on countering threats should be based on investigating and understanding the unique characteristics of threats.

An organization’s survival requires that it knows enough to adapt itself to changes in the environment. Unfortunately, the Global Information Security Survey (Ernst & Young, 2004) suggests that many organizations may neither know themselves nor their ‘enemy’ as well as they should, resulting in a myopic approach to the rising number and variety of threats.

3.3.3 **Funding**

It is important to note that a business information security programme is not an information technology (IT) line item; it is the price of doing business today (Lewis, 2003).
Information security must be viewed as a business responsibility and must be regarded as an integral part of business strategy (Herold, 2003). Therefore, funding for a business information security programme should come from every department and not be an extension of the IT budget. There are several options for funding it. Some companies deem a certain percent of their information as mission critical and allocate departmental costs accordingly. Some fund their information security operations via charge backs to each department depending on the level of security needed. The decision for funding the programme partially depends on the level of financial reporting available (Lewis, 2003). It is important to point out that the costs of accounting for the programme should not outweigh the programme itself.

Experts recommend that organizations should expend more effort and resources on creating a security-conscious culture (ISO/IEC 17799, 2005; ISO/IEC 13335-3, 2005). Unfortunately, the results of a Global Information Security Survey (Ernst & Young, 2004) shows that too much money is being spent on technological tools, while too little is being directed to organizational and people issues.

These key components need to be seriously considered when designing and developing an information security programme. As seen from the discussion above, they play a vital role in the success of such a programme. Experts have published several frameworks for information security to help in the designing and development of it. Some of the published frameworks need to be examined.

3.4 Frameworks for Information Security

An information security framework is an outline of steps for designing a working plan for both securing the organization’s information assets and later implementing information security in an organization (Whitman & Mattord, 2003).
Chapter 3: Information Security Programmes

One approach organizations use is to adapt, or adopt, a published framework for information security when designing a methodology for the implementation of the necessary security controls. Numerous frameworks exist, but two of the better known will be discussed briefly because they cover aspects related to this research.

3.4.1 ISO/IEC 17799 and ISO/IEC 27001

ISO/IEC 17799:2005 addresses information security. ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization (Gamma Secure Systems Limited, 2005). The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 provides 133 information security central guidelines structured under 11 major information security management areas to enable organizations of various disciplines to identify the security controls which are appropriate to their particular area of business (Gamma Secure Systems Limited, 2005). The following major areas of information security management are covered by the standard:

- **Security policy**
- Organization of information security
- Asset management
- **Human resources security**
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance
Chapter 3: Information Security Programmes

An aspect such as **policy** of an organization above requires the employees of the organization to be properly educated in what that policy entails (Thomson & Von Solms, 1998). Therefore, an element of awareness, training and education come into play. This is evident in **Human resources security** where one of the aspects discussed under this topic is an information security awareness, education, and training for all the employees of the organization.

ISO/IEC 27001:2005 provides information on how to apply ISO/IEC 17799 and how to build, operate, maintain and improve an Information Security Management Systems (ISMS). An ISMS is the means by which senior management monitor and control their security, minimising business risks to acceptable levels and ensuring that security continues to fulfil corporate, customer and legal requirements (Gamma Secure Systems Limited, 2005).

### 3.4.2 NIST security frameworks

NIST security frameworks address computer security. The frameworks have been available for some time and have been broadly reviewed by government and industry professionals (Whitman & Mattord, 2003). Therefore, they are an effective basis for designing a security framework. The following frameworks will be examined in more detail:

- **NIST SP 800–14**: Generally Accepted Security Principles and Practices for Securing Information Technology Systems
- **NIST SP 800–18**: Guide for Developing Security Plans for Information Technology Systems
- **NIST SP 800–26**: Security Self – Assessment Guide for Information Technology Systems

**NIST SP 800–14**

This publication provides best practices and security principles that can direct the development of a security framework.
In addition to detailing best practices across a spectrum of security areas, it provides philosophical principles that should be integrated into the entire information security process (Whitman & Mattord, 2003). The security principles are given as intrinsic expectations that must be met when securing information technology (IT) systems, regardless of whether the system is small, large or owned by a government agency or a private corporation. The principles are expressed at a high level, encompassing broad areas, e.g., accountability, cost-effectiveness, and integration. The principles are to be used when developing information security programmes and when creating new systems, and practices (Swanson & Guttman, 1996). The publication describes eight principles, which are listed below:

2. Computer Security is an Integral Element of Sound Management
3. Computer Security Should Be Cost-Effective
4. Systems Owners Have Security Responsibilities Outside Their Own Organizations
5. Computer Security Responsibilities and Accountability Should Be Made Explicit
6. Computer Security Requires a Comprehensive and Integrated Approach
7. Computer Security Should Be Periodically Reassessed
8. Computer Security is Constrained by Societal Factors

These practices guide organizations on the types of controls, objectives and procedures that comprise an effective IT security programme. The practices also show what should be done to enhance or measure an existing computer security programme or to aid in the development of a new programme (Swanson & Guttman, 1996). They provide a common ground for determining the security of an organization and build confidence when conducting multi-organizational business.
Chapter 3: Information Security Programmes

The practices are provided in a checklist format to assist organizations in reviewing their current policies and procedures against the common practices presented in this publication (Swanson & Guttman, 1996). Organizations should use the practices as a starting point in order to develop additional one based on their own organizational and system requirements. The document describes 14 practices:

1. **Policy**
2. Programme Management
3. Risk Management
4. Life Cycle Planning
5. Personnel/User Issues
6. Preparing for Contingencies and Disasters
7. Computer Security Incident Handling
8. **Awareness and Training**
9. Security Considerations in Computer Support and Operations
10. Physical and Environmental Security
11. Identification and Authentication
12. Logical Access Control
13. Audit Trails
14. Cryptography

This guideline can be used by management, internal auditors, users, system developers, and security practitioners to gain an understanding of the basic security requirements most IT systems should contain.

As can be seen from above, both policy and awareness and training of employees also feature very high. Human involvement in the protection of information and computer systems is also brought out clearly. Therefore, it can be concluded that human involvement is vital to the success of these programmes.
Chapter 3: Information Security Programmes

- **NIST SP 800–18**

This publication is considered as the foundation for a comprehensive security framework, because it provides detailed methods for assessing, designing, and implementing controls and plans for IT applications of varying size (Swanson, 1998). NIST SP 800–18 is intended as a guide when creating security plans. But before the plan is developed, a determination must be made as to which type of plan is required for a system, i.e., determining the boundaries of the system and the type of system. Input for the security plan should come from various individuals with responsibilities concerning a particular IT system, including functional end users, information owners, the System Administrator, and the System Security Manager, because the system is used by all of them (Swanson, 1998).

A security plan provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. It also delineates responsibilities and expected behaviour of all individuals who access the system (Swanson, 1998). This publication provides a very good baseline for creating such security plans that contains technical information about the IT systems, their security requirements, and the controls implemented to provide protection against its risks and vulnerabilities. It is to be used by those individuals responsible for IT security at the system level and at the organization level, and it can as well be used as an auditing tool by auditors, managers, and IT security officers (Swanson, 1998).

Security plans require periodic reviews, modifications, and milestone or completion dates for planned controls to keep them current and effective. Therefore, procedures should be in place outlining who reviews the plans and follows up on planned controls.
Chapter 3: Information Security Programmes

- NIST SP 800–26

This publication provides a method to evaluate the security of unclassified IT systems or groups of systems by guiding in performing an IT security self-assessment. It aims to provide a standardized approach to assessing a system. It also provides guidance on utilizing the results of the system self-assessment to ascertain the status of an organization-wide security programme (Swanson, 2001). Self-assessments provide a method for an organization’s officials to determine the current status of their computer security programmes and, where necessary, establish a target for improvement.

The self-assessment guide utilizes an extensive questionnaire containing specific control objectives and suggested techniques against which the security of a system or group of interconnected systems can be tested and measured. The questionnaire can be used for the following purposes (Swanson, 2001):

- Agency managers who know their agency’s systems and security controls can quickly gain a general understanding of needed security improvements for a system, group of interconnected systems, or the entire agency.
- The security of an agency’s system can be thoroughly evaluated using the questionnaire as a guide. The results of such a thorough review produce a reliable measure of security effectiveness and may be used to fulfil reporting requirements, prepare for audits, and identify resources.

A self-assessment conducted on a system, or multiple self-assessments conducted for a group of interconnected systems, are methods used to measure information technology security assurance. IT security assurance is the degree of confidence one has that the managerial, technical and operational security measures work as intended to protect the system and the information it processes (Swanson, 2001). Adequate security of these assets is a fundamental management responsibility.
Adopting or adapting a framework from a published model in the design of a methodology for securing business information assets is just one option of following well-structured approaches. An information security programme that actively involves everybody in the organization, including the board of directors, is also vital. All three general organizational levels should be actively involved in protecting the business information assets. Each of the three levels has a role to play in improving the level of security in the organization, and therefore, need to be discussed.

3.5 Levels of Influence

Information security nowadays is no longer merely a technical issue which only needs attention at the technical level. It involves the active involvement from the strategic, and managerial levels as well as the technical levels of an organization in order to improve the level of security (Thomson & Von Solms, 1998). These levels of influence will be examined by discussing the roles that each level plays in assisting to secure business information assets.

3.5.1 Strategic layer

The first and top level in an organization is called the strategic level and involves the board of directors and executive management. This level is generally responsible for setting the mission, vision and objectives of the organization, and these are achieved through directing and controlling the organization and its functions. This level addresses strategic issues of information security from, at least, a business and legal perspective (Posthumus & Von Solms, 2005). It establishes the organization's information security programme and its overall programme goals, objectives, and priorities in order to support the mission of the organization through directing an organization’s information security efforts (National Institute of Standards and Technology, 1998).
Chapter 3: Information Security Programmes

It also scrutinises and reviews the effectiveness of strategies and information security policies so that these may be regulated and improved upon where necessary, based on the periodic reports from various organizational department heads through controlling an organization’s information security efforts (Posthumus & Von Solms, 2005).

The manner in which an organization is directed and controlled is called corporate governance; hence this level is sometimes called the governance level. For directing and controlling of the organization to be effective, it should be in line with the general vision and with current business strategies and objectives of the organization (Posthumus & Von Solms, 2005).

3.5.2 Tactical layer

The managerial, or tactical level is the second general organizational level. This level is more concerned about the implementation issues of information security from an infrastructure and best practice point of view (Posthumus & Von Solms, 2005). The vision set at the strategic level is implemented, normally by introducing organizational policies (National Institute of Standards and Technology, 1998). This level is also concerned with how an organization’s information security strategy is implemented and managed (Whitman & Mattord, 2003). This involves activities such as compliance with information security policies, practices and procedures (Posthumus & Von Solms, 2004).

3.5.3 Operational layer

The last, and lowest, level in the organization is called the technical, or operational, level which is responsible for the implementation of the policies, normally by means of technical and/or operational means. This level mainly includes system and network administrators (ISO/IEC 13335-3, 2005).
Chapter 3: Information Security Programmes

The administrators’ main functions are day-to-day monitoring of the network, implementing and executing organizational information security policies and procedures set out by management. They are also responsible for administrating system and network security of the organization, ensuring and maintaining the required levels of network security (ISO/IEC 13335-1, 2004). They also perform upgrading of specific security programmes such as virus tools, software patches and the administering of specific security controls, such as backups, access control lists etc (ISO/IEC 13335-3, 2005).

Involving these levels of influence in information security helps to actively involve everybody in the organization in the protection of the business information assets. Any information security initiative requires the support of an organization’s employees. Therefore, this chapter concludes by discussing the importance of human involvement in the protection of business information assets.

3.6 Importance of Human Involvement

As the ‘people’ aspect of computing cannot be completely solved by physical and technical controls (Von Solms, 2000; Du Plessis & Von Solms, 2002), it is very necessary to involve it in the information security programme. Typically, organizations depend on human involvement to prevent most security breaches. As such, there is a need to develop them into an organization’s strongest layer of defence (Ernst & Young, 2004). It is important to make security the responsibility of every individual in the organization from top management to end-user level.

Figure 3.1 on the next page was adapted from one provided by Whitman and Mattord (2003). It can be seen from the figure that people can directly access information, for example, people read hard copies of documents. They can also indirectly access information through systems, for example, electronic storage of information (Whitman & Mattord, 2003).
Chapter 3: Information Security Programmes

However, as people can directly access each ring as well as the information at the core of the model, people require unique approaches to security. In fact, the resource of people must become a layer of security, a **human firewall** that protects the information from unauthorised access and use. In order to achieve this, members of an organization must be effectively trained, implemented, and maintained, or else they, too, become a threat to the information. As such, people, not technology, are the primary defenders of information assets in an information security programme, and are uniquely responsible for their protection (Whitman & Mattord, 2003).

Many experts have recommended human involvement in the protection of vital business information. Whitman and Mattord (2003) state that information security is designed and implemented in three layers: policies, people (education, training, and awareness programmes), and technology. The information security frameworks discussed earlier on in the chapter refer to policies and procedures. These rely on human behaviour to be implemented (Thomson & Von Solms, 1998). Safeguards provide three levels of control: managerial, operational and technical (Whitman & Mattord, 2003).
But the successful implementation of operational controls for information security is reliant on the employees of the organization being properly educated in what these controls entail (Thomson & Von Solms, 1998). Therefore, it can be concluded that the reliance on human behaviour means that employees have become one of the most important factors in ensuring the security of the IT systems and the information they process (Du Plessis & Von Solms, 2002).

Employees in the entire organization need to support the security programme because, as previously stated, overall security is only as strong as its weakest link. The recklessness or simple carelessness of a single employee can undermine even the best technological countermeasures (Ernst & Young, 2004). Surveys have shown that many security breaches are simply the result of human negligence enabled by weak operational practices.

With people as important as they are for an adequate and appropriate level of security, they need to be developed and motivated so that they can counter threats appropriately, because security technology is defenceless against individuals doing the “wrong thing” (Ernst & Young, 2004). One of the ways of developing and motivating employees is through awareness. Awareness of information security spreads knowledge and thus increases understanding of information security concepts and objectives. Widespread understanding will increase the extent of support and commitment from employees to the rules and motivate them to improve security. Security improvements will both increase compliance and reduce risks, making security breaches less likely and/or less costly (NoticeBored, 2003).

3.7 Conclusion

This chapter gave a comprehensive discussion of how information security is managed in organizations. Nowadays, most organizations follow well-structured approaches to protect business information assets properly. Some of the key components of a business information security programme were discussed, and it was noted that they have a major impact on the success of the programme.
Therefore, they need to be considered when structuring an information security programme. The information security objectives, vision and mission were also discussed to highlight the vital role that information security plays in protecting business information assets.

One of the tasks in protection business information is developing an information security programme. Adopting or adapting an existing framework for information security is one approach for designing a working plan for securing an organization’s information assets. Some of the published frameworks for information security that an organization can adopt or adapt were discussed to emphasize the point that a proper methodology for implementation of the needed security controls needs to be followed to protect the information assets properly.

It was also highlighted that information security must not be viewed from a technical issue only, because the human dimension cannot be reduced by any amount of technology and is important as a security control. Everyone in the organization needs to be actively involved in securing the information assets. One approach of involving everyone in the organization that was discussed is to involve the levels of influence so that all the general organizational levels are involved in ensuring an appropriate level of security. For any information security initiative taken by an organization to be effective, it has to involve and get full support from these organizational levels. Consequently, this chapter concluded by discussing the importance of human cooperation in information security.

It has already been discussed that for the employees to be vigilant in countering threats, they need to be developed and motivated through information security awareness programmes. Therefore, the next chapter focuses on the current approaches to information security awareness programmes.
Chapter 4

Information Security Awareness

4.1 Introduction

As has been argued in the previous chapter, an organization’s overall security typically depends on human involvement to prevent most security breaches, and as such, this needs to be encouraged to counter threats appropriately. It was also shown that one of the ways of developing and motivating employees is through security awareness. This chapter aims to demonstrate the need for organizations to implement information security awareness programmes as a means of changing behaviour or reinforcing good security practices in all information resource users. A brief discussion of security awareness, training and education is given to show the differences that exist amongst these three terms. Different information security awareness programmes will be discussed to show that there are basically three types of programmes. A further discussion of information security awareness for end-users will be given to highlight the need for cultivating an information security culture amongst these information resource users. Current approaches to the development of these programmes and their limitations will be examined.

Some of the recently conducted surveys have shown that the level of security awareness in most organizations is still low despite the previously demonstrated important role it plays (Ernst & Young, 2004; Deloitte Touche Tohmatsu, 2005). One of the possible reasons for this may be the current approaches used to develop these awareness programmes. Therefore, the chapter concludes by suggesting a move away from the current approaches.
Chapter 4: Information Security Awareness

4.2 Information Security Awareness, Training and Education

The purpose of information security awareness, training and education is to enhance security (National Institute of Standards and Technology, 1998) by:

- Improving awareness of the need to protect system resources
- Developing skills and knowledge so computer users can perform their jobs more securely
- Building in-depth knowledge, as needed, to design, implement, or operate security programmes for organizations and systems.

Making information-users aware of their security responsibilities and teaching them correct practices help users change their behaviour. These also support individual accountability, which is one of the most important ways to improve information security. Without knowing the necessary security measures and how to use them, users cannot be truly accountable for their actions (National Institute of Standards and Technology, 1998).

Information security education, training, and awareness are all necessary to the successful implementation of any information security programme (Wilson & Hash, 2003). These three elements are related, but they involve distinctly different levels of learning. This sub-section explains these concepts in detail.

4.2.1 Information security awareness

Security awareness efforts are designed to change behaviour or reinforce good security practices and provide a baseline of security knowledge for all users, regardless of job duties or positions. It allows individuals to recognize information security concerns and respond accordingly. Courtney Gilbert (2003) in the paper “Developing an Integrated Security Training, Awareness, and Education Programme” described security awareness as a learning process that changes individual and organizational attitudes and perceptions to realize the importance of security and the adverse consequences of its failure.
Chapter 4: Information Security Awareness

An awareness programme mixes awareness sessions with periodic reminders and promotional materials to bring the attention of information resource users to security issues, and to increase their understanding of vulnerabilities and threats affecting the security of organizations’ information and information systems (University of Georgia, 2002).

4.2.2 Information security training

Information security training is typically considered technical training, and it focuses on improving the security skills and competencies of personnel managing by designing, developing, acquiring, and administering information resources. It is intended for information security staff, and for information technology staff in positions with security-related responsibilities, such as system administrators or network engineers (University of Georgia, 2002). It is more formal, having the goals of building knowledge and skill to augment and enhance job performance and enables people to perform more effectively (Gilbert, 2003). It is geared to understanding the security aspects of particular IT systems and applications that individuals use. For example, all users need to understand the security features of the Local Area Network (LAN) to which they are connected, as well as security issues related to connectivity to the Internet, intranet, or extranet.

The most significant difference between training and awareness is that training seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues (Wilson & Hash, 2003).

4.2.3 Information security education

Education, in general, is an advanced form of training. It leverages experience in a field of study to further enhance and develop knowledge, skills and abilities (Gilbert, 2003).
Chapter 4: Information Security Awareness

Education also integrates all the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles, and strives to produce information security specialists and professionals capable of vision and proactive response (de Zafra, Pitcher, Tressler & Ippolito, 1998). Security education, including formal courses and certification programmes, is most appropriate for an organization's designated security specialists.

As it can be seen from the definitions of the three terms, they are all important in imparting the necessary knowledge and skills needed in making information resources secure to various individual groups in the organization. The focus in this chapter is on information security awareness, and the next section discusses the different types of information security awareness that are supposed to exist in organizations.

4.3 Information Security Awareness Programmes

There are basically three types of information security awareness programmes based on major groupings of employees: - information security awareness for top management, information security awareness for IT personnel and information security awareness for end-users. These need to be examined in more detail.

4.3.1 Information security awareness for top management

This awareness programme is addressed solely at top management to give it the necessary knowledge about information security. Top management needs to be informed on all matters relating to the security of all information resources in the organization because staff looks up to it for direction and guidance on information security. Furthermore, managerial oversight is itself an important class of information security control, so managers need to be aware of their governance responsibilities including monitoring and supporting their subordinates (NoticeBored, 2003).
Thomson and Von Solms (1998) state that the knowledge that they acquire in this programme: -

- Makes them aware of the importance of information security
- Enables them to make informed decisions regarding information security issues that have been put in place in the organization
- Makes them openly demonstrate their commitment and support for the implemented security controls.

Management need to be educated about an organization’s corporate information security policy in order for it to play an active, participative role in drawing up an effective security policy. Therefore, the good time for this awareness programme should be shortly before the development of the corporate information security strategy. Since top management of an organization is generally fairly stable, this part of the programme should be run as a one-off one. It will be necessary to conduct a refresher or add-on course if the top management structure changes in any way, or if the legislation governing the protection of information resources, which may have an effect on the functioning of the organization changes, or as a result of international developments, e.g., if an international security certification scheme is introduced (Thomson & Von Solms, 1998).

### 4.3.2 Information security awareness for IT personnel

This category includes IT network and system managers, application developers, information security administrators, computer auditors and end-users that develop and share spreadsheet and database applications, etc. Technologists are largely ignored by traditional information security awareness activities, yet they are expected to understand, implement and operate most of the technical security controls.
Technical details relating to design and operation of information security controls are most relevant to these people. Improved understanding of information security will help persuade technologists to incorporate appropriate technical controls in systems they build and operate, and make use of controls in systems they use (NoticeBored, 2003). Therefore, the objectives of this component are to give IT staff the necessary knowledge about information security risks, and the techniques that can be applied to minimise these threats in order to provide effective information security management for the organization (Thomson & Von Solms, 1998). These techniques must ensure appropriate levels of confidentiality, integrity and availability of business information.

It is envisaged that the detailed course for this awareness programme must be a once-off event, but it is recommended that refresher courses should be offered whenever needed. This could be as a result of changes in hardware/software, which may have an effect on the functioning of the security safeguards in place, which would then require re-structuring. From time to time, it is also necessary to offer courses on new developments in this area, and staff turnover could also necessitate the need for a course (Thomson & Von Solms, 1998).

4.3.3 Information security awareness for end-users

Prime targets for this awareness programme are the employees who use information systems, handle corporate information or control IT assets. In practice, this means practically anyone within the organization, including top management and IT personnel, and perhaps some others such as contractors and consultants. Managing information may or may not be a central part of every individual’s daily working life, but every employee has a part to play in information security culture. This type of programme helps to reduce the chance that anyone can reasonably claim to be ignorant of his or her information security responsibilities and/or rules.
Therefore, the objectives of this component are to give employees the necessary knowledge to maintain information security by ensuring the following three properties (Thomson & Von Solms, 1998):

- Confidentiality
- Availability
- Integrity.

It is important to motivate employees to use the knowledge they get through this awareness programme to the benefit of the organization. This section of the programme provides the end-users with the knowledge and motivation to ensure that information security is maintained. The required end result of this phase of the programme is that the end-user’s behaviour is modified to such an extent that the security related aspects of their daily operations are carried out automatically (Thomson & Von Solms, 1998).

The first session of this phase of the programme should be relatively comprehensive and will serve as an introduction to information security. Following on this first session should be a number of short sessions, designed to introduce the user to the different security aspects that need to be addressed in their daily routines (Thomson & Von Solms, 1998). It is also necessary to include this type of awareness programme in new employee induction processes.

This phase of awareness programme is highly required as it is responsible for introducing an information security culture in all employees in the organization as end-users of information resources. An information security culture amongst employees is vital in securing an organization’s information resources and needs to be examined.
4.4 Need for an Information Security Awareness for End-Users

Information security awareness for end-users focuses on developing an organization culture that is both aware and capable of responding to security related risks. It aims at changing the way employees behave towards an organization’s vital information and cultivating an information security culture right through the organization. Their every action in dealing with information assets should incorporate security considerations and in time, security considerations will become part of the culture of the organization. The way in which people work with information assets in their daily job functions will eventually become the way things are done in the organization, and this will eventually become part of the culture of the organization (Du Plessis & Von Solms, 2002).

Achieving this level of understanding represents a major challenge because no amount of technology can reduce the overriding impact of human complexities, inconsistencies, and peculiarities. Ernst & Young (2004) report that any strategy that overlooks this realization is inherently flawed. With proper awareness and training, employees can become the most effective layer in an organization’s security defence. Therefore, an organization could increase its level of protection significantly with effective awareness and training initiatives (Ernst & Young, 2004).

Information security awareness for end-users is very important in instilling a culture of security awareness in employees in the organization. As such, current approaches to implementing security awareness programmes need to be investigated.

4.5 Current Approach to Security Awareness

As pointed out in the last sub-section, information security awareness programmes play an important role in a complete information security programme. As such, organizations are striving hard to instil a security awareness culture amongst its employees through these programmes.
The current approach to implementing information security awareness programmes in these organizations is discussed below.

**Guidelines and standards**

The development of information security awareness programmes in organizations is based on the security policies and procedures currently in place therein, because every organization is unique, and as such, different organizations have different management instructions on how these organizations should be run (Du Plessis & Von Solms, 2002). The management instructions, i.e., policies, are seen as the basis for effective information security within the organization (ISO/IEC 13335-1, 2004). Basing information security awareness programmes on the existing security policies and procedures in the organizations is advocated prominently in current information security guidelines and standards.

Two such standards are ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005. They advocate that the information security awareness training programme of employees should be based on the objectives, strategies and policies of the organization (Du Plessis & Von Solms, 2002).

It is important to note at this stage that these programmes differ in organizations because each has its own security policies and its own goals. This could be called a company-specific approach to information security awareness since it is based on elements that are very specific to a particular organization (Du Plessis & Von Solms, 2002).

Though it has been demonstrated in the previous discussion that information security awareness programmes play a vital role in information security, the level of awareness in most organizations is still low according to some of the recently conducted surveys (Ernst & Young, 2004; Deloitte Touche Tohmatsu, 2005). The discussion that follows examines possible reasons for this.
4.6 Limitations of Current Approach to Security Awareness

Despite the illustrated importance of information security awareness and the widespread acceptance of this fact in current guidelines and standards, the level in most organizations is still low. According to the Global Information Security Survey 2004 by Ernst & Young (2004), respondents named “lack of security awareness by users” as the top obstacle to effective information security, however, only 28% listed “raising employee information security training or awareness” as being a top initiative in 2004. The survey also showed that less than half of the respondents provided their employees with ongoing training in security and controls. In the 2005 Global Security Survey, conducted by Deloitte Touche Tohmatsu – Australia (2005), respondents pointed to a host of continuing challenges to their businesses. Most prominent among them were the increasing sophistication of threats (63%) and the lack of employee awareness and training (48%), both of which could create an environment of exploitable vulnerabilities and weak operational practices. According to the same survey, overall, security awareness and training implemented, or maintained, decreased from 77% in 2004 to 65% in 2005. Though experts recommend that 40% of an organization’s security budget be spent on awareness measures (MacBrige, 2000), the report has also revealed that only 15% of information security budget is spent on employee awareness and training, while 64% of it is spent on security tools.

Thus, the recent surveys have clearly shown that the level of security awareness in most organizations is still low despite the vital role it plays. A possible reason for such a lack of awareness programmes in organizations could be the approach used to implement such programmes (Du Plessis & Von Solms, 2002). As pointed out in the last sub-section, both ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005 stress the need for implementing these programmes based on the information security policies and procedures already in place in the organizations. But not all organizations have these policies in place.
A recent survey conducted by PricewaterhouseCoopers LLP (2004), Information Security Breaches Survey 2004, reveals that a third of all companies in the United Kingdom, and two-thirds of large businesses also in the United Kingdom, now have information security policies in place. Now, if these policies were the only basis for awareness programmes, it would mean that only those organizations with policies in place would have something on which to base their information security awareness programmes. The reasons why some organizations do not still have information security policies in place are that the development of such policies and procedures is a lengthy process that requires time, money and specialized knowledge. These constraints would not make such an effort feasible for small- to medium-sized companies (Du Plessis & Von Solms, 2002).

The current lack of awareness programmes in most organizations suggest that a problem exists with the traditional method of basing awareness programmes on the policies and procedures already in place in the organization (Du Plessis & Von Solms, 2002). Therefore, a different approach to the development of information security awareness programmes has to be developed that would try to increase the current low levels of awareness in most organizations.

4.7 Moving Away from a Company-Specific Approach to Security Awareness

It has already been shown that there is an information security awareness gap left by the current approach to the development of awareness programmes in organizations that needs to be fulfilled. A different approach to the development of these programmes has to be developed to complement the existing approach. This approach should not base its content on the security policies and procedures already in place in an organization. Moving away from such a company-specific approach would effectively make an awareness programme independent of the security policies that prove to be lacking in most organizations. Such an approach to implementing a programme into an organization can be called a generic approach to information security awareness (Du Plessis & Von Solms, 2002).
Chapter 4: Information Security Awareness

An investigation of complete awareness programmes has to be carried out to find out the contents covered in them. From the contents, general and common aspects that affects most organizations and do not entirely depend on the company-specific policies need to be identified. This would form the contents of the generic approach to awareness programmes.

Moving away from company-specific information would allow for the creation of an awareness programme that would be suitable for most organizations. Therefore, the proposed approach is expected to improve matters because the shortfall in the current approach will be avoided.

4.8 Conclusion

One of the main components of any information security programme is implementing an information security awareness programme that makes employees aware of their security responsibilities. Making employees aware of these responsibilities contributes to the success of an information security programme; they behave accordingly since they realize the importance of security and the adverse consequences of its failure. Different information awareness programmes, based on major groupings of employees have been discussed, and it has been shown that each of the awareness programmes is important and needs to be implemented in organizations. Information security awareness for end-users was further discussed to highlight the complementary role it plays in instilling an information security culture amongst employees, regardless of their job duties or position.

Information security awareness is so important to the overall information security of an organization that awareness programmes feature very prominently in current information security guidelines and standards (Du Plessis & Von Solms, 2002). Therefore, the current approach to the development of these awareness programmes has been examined by referring to what is contained in ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005. These standards stress the need to base the awareness programmes on the existing security policies in the organizations.
This has been discussed as a limitation to the development of awareness programmes, because not all the organizations have information security policies in place. Some of the recently conducted surveys confirm that there is an information security awareness gap in many organizations.

Therefore, it was suggested that in order to raise the low level of security awareness in organizations, a different approach to developing awareness programmes has to be developed to complement the existing company-specific approach to these programmes. The next chapter examines the proposed generic approach, to the development of awareness programmes that attempts to move away from the basing the contents of them entirely on the existing security policies and procedures already in organizations. Contents for complete awareness programmes will be discussed, and from these, typical company-specific topics and topics that can be catered for in a generic programme will be identified.
Chapter 5

Generic Information Security Awareness and Education

5.1 Introduction

It was highlighted in the previous chapter that there is a low level of information security awareness in most organizations despite the demonstrated important role it plays and the wide acceptance of it in the current information security standards and guidelines. It was also motivated that the approach used to implement the awareness programmes could be responsible for such a low level of awareness programmes. It was then suggested that a different approach from the existing one has to be developed to try to raise this low level of awareness. Therefore, this chapter discusses the proposed approach.

The focus is on the contents, and as such, this chapter begins by discussing the contents for information security awareness programmes. Typical company-specific topics will be discussed, and topics that can be catered for in a generic awareness programme will be examined. This chapter concludes by discussing the anticipated benefits of the proposed approach.

5.2 The Contents of Information Security Awareness Programmes

The contents of an awareness programme refer to topics and areas of knowledge that are addressed through the awareness programme (Du Plessis & Von Solms, 2002). It is important to remember that the programme discussed in this research is for the end-users, and includes every employee that works with information in an organization despite their different roles and responsibilities.
Chapter 5: Generic Information Security Awareness and Education

Note has also to be taken that users to be reached by an awareness programme largely determine the content of the awareness programme, since it is important that users are only given materials applicable to them (Du Plessis & Von Solms, 2002). Therefore, the material or the topics of the awareness programme discussed here focus at this end-user level. Figure 5.1 was adapted from Lindie du Plessis mini thesis, Information Security Awareness: Baseline Education and Certification. The figure illustrates the different areas of security knowledge that can be covered in an information security awareness programme. These knowledge areas are examined in more detail to determine the topics covered under each.

![Figure 5.1: Contents of Information Security Awareness Programmes](image-url)

Figure 5.1: Contents of Information Security Awareness Programmes
5.2.1 The security policy of an organization

One of the most important aspects of an awareness programme is to teach employees of the existence of an organization’s information security policy. Such a programme should make employees aware of the existence of such policies and provide insight into why a policy is needed. The security policy of the organization sets the security direction for the organization (Du Plessis & Von Solms, 2002), and as such, knowledge of this policy will help the employees understand what the organization is striving for in information security. Knowledge of the policy will also serve to impress on employees the importance that top management attaches to information security and the awareness programme (Thomson & Von Solms, 1998). Some of the aspects included in a security policy that should be taught to the employees include definitions of terminology, the CEO’s support signature, different employee roles and responsibilities, compliance to policy and incident handling (Du Plessis & Von Solms, 2002).

5.2.2 Procedures and how to implement them

Employees must be made aware of procedures they have to follow in their everyday tasks (ISO/IEC 13335-1, 2004). Security policies of the organization are broad, and as such, procedures translate the policy into specific steps that employees must follow in order to support the goals of the policy and so create a secure information technology environment. Some of the procedures beneficial to most employees of most organizations (Du Plessis & Von Solms, 2002) are listed below: -

- Password creation and usage
- Virus protection
- Hackers and crackers
- Social engineering
- Backing up
- Internet usage
Most of these procedures are related to the controls in place in the organization. For example, if an organization makes use of passwords, then procedures related to the creation and use of these would need to be in place. It is these procedures that employees must be made aware of and motivated to follow.

5.2.3 Importance of information and information security

The importance of information and information security has to be taught to employees. They have to know how important the business information they are protecting is to an organization, and that will serve as a motivation to do their part in securing information (Hansche, 2001; Du Plessis & Von Solms, 2002). Therefore, the material in this knowledge area is focused on explaining how businesses rely on information, and also the consequences to the business if the information is compromised (Human Firewall Organization, 2001; Du Plessis & Von Solms, 2002). Some of the elements or topics that are supposed to be included here include:

- Real-life examples
- Legislations about the protection of information
- Information security standards

5.2.4 Basic information security concepts

It is imperative that all employees who use computer technology or its output product, regardless of their specific job responsibilities, must know IT security basics and be able to apply them (de Zafra, Pitcher, Tressler & Ippolito, 1998).
Chapter 5: Generic Information Security Awareness and Education

Helping employees understand what information security is, and how it seeks to protect information, gives them a better understanding of other aspects of security awareness, such as threats and vulnerabilities (Du Plessis & Von Solms, 2002). The main idea behind this knowledge area is to equip employees in doing their every day tasks in a secure manner. Helping employees understand how their actions are protecting information assets will empower them, instead of just making them follow orders (Du Plessis & Von Solms, 2002). Some of the material that fall under basic information security concepts (de Zafra, Pitcher, Tressler & Ippolito, 1998) include:

- Goals of information security
- Risk management
- Physical, technical and operational controls
- Existence of a security policy
- Other definitions such as backup, ethics, individual accountability, firewalls, hackers and crackers etc.

5.2.5 Threats to and vulnerabilities of computer systems

To understand why employees need to protect information, they need to be made aware of the threats to and vulnerabilities of information assets (Du Plessis & Von Solms, 2002). They should also be made aware of how real the problems of security threats are. Therefore, real life examples and use of statistics could underline the need for information security awareness (Hansche, 2001; Du Plessis & Von Solms, 2002). The materials that fall under this knowledge include:

- Real-life examples
- Viruses
- Hackers and crackers
- Social engineering
- Vulnerabilities of connected systems
- Internet vulnerabilities
Chapter 5: Generic Information Security Awareness and Education

- E-mail vulnerabilities
- Physical vulnerabilities
- Legal issues, such as inappropriate use of network facilities, copyright, software licensing and piracy, privacy issues, etc.

If employees do not know how their actions are actually endangering information assets, chances of information-asset compromise are high. Therefore, understanding the vulnerabilities of the information they work with should eliminate problems caused by ignorance. Knowledge of threats and vulnerabilities also helps employees recognize a possible situation of concern and allows them to act before consequences spread (Du Plessis & Von Solms, 2002).

The knowledge areas discussed above are covered in a company-specific approach to information security awareness programmes. But some knowledge areas are very specific to a particular organization, while others are general to most organizations. Therefore, typical company-specific contents need to be examined.

5.3 Typical Company-Specific Topics

The contents addressed by a typical company-specific approach relate to a particular organization. Referring back to Figure 5.1, these include an organization’s information security policy contents and specific procedures.

Since the goals and directions are different for different organizations, so also will be the policy documents. As such, employees of different organizations are therefore educated by different awareness material concerning the policies of their organizations. Therefore, security policies form the basis of a typical company-specific approach to implementing awareness programmes (ISO/IEC 13335-1, 2004).
Procedures are based on the broad guidance provided by policies, and as such, they are much more specific for every organization, and they also form part of the contents for a typical company-specific approach to awareness. It is through policies and these procedures that employees within a specific organization are guided in their role of securing the organization’s information technology environment (Du Plessis & Von Solms, 2002).

As shown in Figure 5.1, there are two types of procedures: procedures that are specific to an organization, and procedures that are general to most organizations. Previously, it was also pointed out that procedures are related to the controls in place in the organizations. In many cases, most organizations have the same type of controls in place (Du Plessis & Von Solms, 2002), which directly follows that they have near similar procedures. For example, most organizations use passwords, and as such, procedures for the creation and use need to be taught to employees. Some procedures are therefore common and general to most organizations while others are very specific to a particular one. It is these specific procedures that form part of the contents of the company-specific approach. For example, procedures, such as who to contact in case of security breaches, are definitely company-specific (Du Plessis & Von Solms, 2002).

Having examined the typical company-specific aspects, it is also very necessary to examine aspects that can form the contents for a generic programme.

5.4 Typical Generic Topics

A generic awareness programme has to be independent of any information that would be specific to a particular organization or to a particular group of employees (Du Plessis & Von Solms, 2002). Referring back to Figure 5.1, the knowledge areas that would fall under this category are generic procedures, importance of information and information security, basic information concepts and threats to and vulnerabilities of computer systems.
The focus in today’s information technology environment is not only on educating employees on the policies of the organization, but also on changing the behaviour and cultivating an information security culture right through the organization (Von Solms, 2000: Du Plessis & Von Solms, 2002). To achieve this, an information security programme would include aspects other than only the policies of the organization. Such aspects include general procedures, basic information technology concepts, threats to and vulnerabilities of computer systems and the importance of protecting information in today’s business environment (Du Plessis & Von Solms, 2002), which tend to be general and common aspects that affect most organizations. Generally, these aspects are part of a company-specific contents but could be catered for in a non-company specific way or generic awareness programme.

Areas such as the contents of company policies and the company-specific procedures of the organization will not form part of the content for the generic approach. This does not imply that these aspects are not important, or that employees do not need education in this field (Du Plessis & Von Solms, 2002). The most a generic awareness programme can do is to introduce to the employees the existence and importance of such company-specific information. The objective is to merely give them an idea as to why they need to be aware of it (Thomson & Von Solms, 1998).

It can be seen from the discussion above that most of the aspects covered in a company-specific approach to information security awareness are general and common to most organizations. Therefore, the next section examines the would-be benefits of the generic approach to show that the limitations of a company-specific approach are eliminated.

5.5 Benefits of a Generic Information Security Awareness Programme

The proposed generic approach to information security awareness is expected to overcome the limitations of a company-specific approach. This section will attempt to provide an idea as to its usefulness or benefits.
As stated previously, a generic programme necessarily omits any information that would be specific to a particular organization and any information that is specific to a particular employee’s roles and responsibilities. Its contents are concentrated on the general and common aspects that tie most organizations together. Therefore, a generic approach gives most organizations a foundation on which to base their awareness programmes, as compared to the typical company-specific approach, which is limited to organizations with information security policies in place. As such, it is expected to raise the level of security awareness in most organizations, because organizations, with or without security policies in place, would be able to implement it. It can also be adopted or adapted by many organizations since the contents covered by the generic approach are general and common to most organizations. This means that information security awareness programmes need not to be developed from scratch for every organization. It also means that different awareness programmes need not be developed for different employees in different organizations. The consequence of this is that organizations, especially small to medium-sized organizations, would be relieved of developing the awareness programmes from scratch, which is a very daunting task. It has to be noted that the development of information security policies is a lengthy process that requires time, money and specialised knowledge (Du Plessis & Von Solms, 2002).

Focusing the material of the awareness programme at the end-user level would also make a generic awareness programme applicable to individuals that work with information technology in their personal capacity. Hence, home users or one-man businesses could draw similar benefits from such an awareness programme as the employees of an organization (Du Plessis & Von Solms, 2002).

5.6 Conclusion

This chapter gave a comprehensive discussion of the proposed approach to information security awareness programmes, i.e., the generic approach, by examining different contents for the awareness programmes.
Different needs that could be catered for in an information security awareness programme were discussed to highlight the general and common aspects that tie different organizations together. Then, typical company-specific aspects were identified and discussed from the different aspects covered in such a programme. It was discovered that most of the aspects covered in company-specific programme are general and common to most organizations. These aspects were then discussed as the contents that would form typical generic programmes, because they do not depend on specifics. This chapter concluded by examining the would-be benefits of a generic approach to awareness programmes to show that the limitations of a company-specific approach are overcome by this approach.

Several sources were used in identifying the generic contents and are discussed in detail in the next chapter. From these sources, contents of the generic programme will be identified.
Chapter 6

An Information Security Awareness Programme: Generic Content, Tools and Techniques

7.1 Introduction

In the last chapter, possible contents for different types of awareness programmes were examined, and it was realised that most of the aspects covered in them are common and general to most organizations. It was also discussed that these aspects do not depend on the specifics of a particular organization, and as such, they could form the contents of a generic information security awareness programme.

Several sources were used in formulating the actual contents of this programme to make sure that the foundation on which it is based is as broad as possible. Therefore, this chapter discusses what these sources recommend. It was also thought that collaborating with South African industries to identify the programme’s generic contents would be beneficial. Therefore, this chapter also discusses the survey that was conducted with several South African organizations to identify such contents. Based on the recommendations from the sources and the survey, the content for a generic programme will be proposed. This chapter concludes by discussing the tools and the techniques suitable for delivering it.

6.2 Towards a Generic Information Security Awareness Programme

Several internationally recognised sources were used to identify the contents of a generic information security awareness programme and to ensure the pros and cons are argued on a broad basis.
Chapter 6: An Information Security Awareness Programme: Generic Content, Tools & Techniques

This was done to make sure that a broader base is used in arguing the contents, and that most of the important security areas would be included in the programme. These sources will be discussed in detail: -

- The ISO/IEC 13335-3
- The ISO/IEC 17799
- The Internet
- The Author’s Survey.

6.2.1 The ISO/IEC 13335-3

The standard recommends that information security awareness programmes should include a corporate IT security policy, and should cover all objectives of an IT security plan. It goes on to say that the programme should ensure that the IT staff and the end-users have enough knowledge of the hardware and software systems, that they understand why safeguards are necessary, and they know how to use them correctly. The areas covered in the programme should achieve the objectives above, and to achieve these, the standard recommended the following topics: -

- An explanation of the importance of security to both the organization and the individual within it
- The security needs of and objectives for the IT systems in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability
- The implication of security incidents for both the organization and the individual
- The correct use of the IT systems, including hardware and software
- The objectives behind, and an explanation of, the corporate information security policy, any guidelines and directives, and risk management strategy, leading to an understanding of risks and safeguards
The necessary protection for and risks to IT systems

Restricted access to IT areas (authorised personnel, door locks, badges, entrance logs) and to information (logical access controls, read/update rights), and why these are necessary

The need to report breaches of or attempts to breach security

Procedures, responsibilities and job descriptions

Procedures prohibited to IT staff and end-users because of security factors

The consequences if staff are responsible for security breaches

The IT system security plans to implement and check safeguards

Why these safeguards are necessary, and how to use them correctly

Procedures related to security compliance checking

Change and configuration management.

It also recommends both interactive and promotional techniques as effective mechanisms for the delivering the contents of such programmes. It reports that interactive techniques (staff meetings, training courses, etc.) provide two-way communication that allows participants and security personnel to validate concepts and requirements. Promotional techniques (video, e-mail, security banners, posters, publications, etc.) are single, directional communication’s methods, which allow management to broadcast concepts, information, and attitude in an inexpensive manner (ISO/IEC 13335-3, 2005).

One of most fundamental concepts mentioned is that it is necessary to implement the programme at all levels of an organization, because it is the responsibility of every individual to review and be intimately familiar with the security policies and procedures of their work environment.
6.2.2 The ISO/IEC 17799

This standard also highlights the need to develop an information security awareness programme that ensures employees are familiar with information security policies, standards and procedures. It also encourages extending the programme to contractors and third-party users to ensure that they are familiar with these policies, standards and procedures. It stresses that these programmes should be based on an organization’s policies and procedures.

The standard, in general, is composed of 11 main security areas, and within those 11 areas, there are 39 main security categories. The security areas covered include (University of Miami School of Medicine, 2006; ISO/IEC 17799, 2005): -

- Security policy: the objective of this area is to provide management direction and support for information security in accordance with business requirements and all relevant laws, regulations and private certificatory requirements
- Organization of information security: the objective of this area is to manage information security within an organization's overall administrative structure
- Asset management: the objective of this area is to achieve and maintain appropriate protection of organizational assets
- Human resources security: the objective of this area is to ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles for which they are considered, in order to reduce the risk of theft, fraud or misuse of facilities (Information security awareness is addressed per sé in this area)
Physical and environmental security: the objective of this area is to prevent unauthorized physical access, damage or interference to an organization's premises and infrastructure, using controls appropriate to the identified risks and the value of the assets protected

Communications and operations management: the objective of this area is to ensure the correct and secure operation of information processing facilities

Access control: the objective of this area is to control access to information, information processing facilities, and business processes

Information systems acquisition, development and maintenance: the objective of this area is to ensure that security is an integral part of the organization’s information systems, and of the business processes associated with those systems

Information security incident management: this area aims to ensure information security events and weaknesses associated with the organization's information and information system assets are communicated in a manner to allow appropriate corrective actions to be taken

Business continuity management: the area's objective is to ensure timely resumption from, and, if possible, prevention of interruptions to business activities and processes caused by failures of information systems

Compliance: the objective of this area is to ensure compliance with all statutory, regulatory, certificatory or contractual obligations.
As can be seen from the above, the standard focuses on a broad overview of various areas of information security, because it is intended to provide a common basis for developing organizational security standards and effective security management practices, such as information security awareness programmes. The high, broad level and the conceptual approach allow this standard to be applied across multiple types of enterprises and applications. The security areas covered are essential in building effective information security in any organization.

Although the ISO/IEC 17799 standard covers a very wide spectrum of information security areas, the main security category of Information Security Awareness, that forms part of the Human Resources Security area, is of specific importance to this study.

6.2.3 The Internet

Some awareness programmes offered on the Internet were studied thoroughly to gain more insight into the topics covered in them. A well-known one is the SANS Security Awareness Programme. This covers general security areas affecting most organizations, and each area is composed of one or more elements (SANS Institute, 2005): -

- Passwords (weak/strong/password management/unique account passwords)
- Computer viruses (anti-virus software/definition updates)
- Malicious codes (personal firewalls/detecting malware)
- Personal use and gain (personal business)
- Data backup and storage (regular backup schedules/restore procedures test/offsite backup)
- Incident response (incident response plan)
- Environmental (clean power/smoke damage)
- Inventory control (media sanitization/asset theft)
Chapter 6: An Information Security Awareness Programme: Generic Content, Tools & Techniques

- Physical security (access to spaces/identification badges)
- Social engineering (account harvesting/financial data gathering).

It also covers true-life stories that have happened to people and organizations to reinforce the concepts covered. Each one demonstrates the consequences of simple mistakes or lapses in information and computer security.

Having studied what is covered in these sources, a questionnaire was drafted and sent out to some well-known South African organizations which follow sound information security principles. The following sub-section discusses the survey in detail.

6.2.4 The author’s survey

The main aim of the survey was to solicit ideas on what organizations think should be included in a generic programme. It is important to point out that the organizations that participated operate in different industrial sectors. This was done in order make sure that the identified content is suitable for interdisciplinary organizations. Consequently, industries from mining, manufacturing, food and beverage, education, communications and IT sectors, participated in the survey.

The questionnaire used in the survey is included as Appendix A.

- Analysis of the survey results

The complete analysis of the survey results is set out in Appendix B.

50 questionnaires were sent out to industries and only 13 of them were returned. The survey method might have contributed to number of responses received. Though the number of responses was small, important conclusions were drawn from the survey results and need some discussion.
Conclusions drawn from the survey

The following important points were noted from the survey results:

- It was encouraging that all the organizations that participated in the survey realise the importance of information and the ICT infrastructure to their daily operations. Over 60% of the organizations rated their business information and the ICT infrastructure as very important (see Figure 6.1 and Figure 6.2 below).

**Figure 6.1: Importance of Business Information**
All the organizations agreed that they are directly impacted upon in their daily operations if the confidentiality, integrity and availability of information and the ICT infrastructure are compromised in any way. The extent of this impact is shown in the tables of Figures 6.3, 6.4, and 6.5 below.

**EFFECTS OF CONFIDENTIALITY COMPROMISE**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not affected</td>
<td>0</td>
</tr>
<tr>
<td>Lightly affected</td>
<td>0</td>
</tr>
<tr>
<td>Moderately affected</td>
<td>6</td>
</tr>
<tr>
<td>Seriously affected</td>
<td>7</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

Table 6.3: Effects of Confidentiality Compromise
Chapter 6: An Information Security Awareness Programme: Generic Content, Tools & Techniques

<table>
<thead>
<tr>
<th>EFFECTS OF INTEGRITY COMPROMISE</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not affected</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Lightly affected</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Lightly affected</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Seriously affected</td>
<td>12</td>
<td>92.3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Table 6.4: Effects of Integrity Compromise

<table>
<thead>
<tr>
<th>EFFECTS OF AVAILABILITY COMPROMISE</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not affected</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Lightly affected</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Moderately affected</td>
<td>4</td>
<td>30.8</td>
</tr>
<tr>
<td>Seriously affected</td>
<td>9</td>
<td>69.2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Table 6.5: Effects of Availability Compromise

Over 75% of the respondents indicated that they have organizational information security policies, procedures and guidelines. This percentage indicates that most of them realise the important role that these play in protecting information assets. It is very important for organizations to have them and to make their employees aware of their existence. Moreover, any information security initiative starts with these policies. But there are still some organizations where employees are unaware of their existence. This is confirmed by the survey: about 20% of the respondents indicated that they did not know whether their organizations have policies or not (see Figure C.1 and C.2 in Appendix C).

- It is an encouraging development that all the respondents realise the important role that awareness programmes play (see Figure 6.6 on the next page).
Unfortunately, about 60% of the respondents indicated that they have never attended any such programme (see Figure 6.7 below). Another discouraging fact is that out of those that attended awareness programmes, most of them attended them more than a year ago, (23%) (see Figure 6.8 on the next page).
Figure 6.8: Date the Programme was attended

+ Awareness programmes are supposed to be ongoing exercises to make sure that the security of information assets is kept uppermost in employees’ minds. Therefore, respondents were asked how often they should be offered. Most proposed that they should be offered once a year (see Figure 6.9 below).

Figure 6.9: Interval in Offering an Awareness Programme
The respondents recommended the following topics to be addressed and included in a programme: -

- Data backup and storage
- Social engineering
- Remote/mobile worker security
- Malicious code security
- Password security
- Internet/web browser security
- E-mail security
- Wireless security
- Physical and environmental security
- Computer ethics
- Privacy and confidentiality
- Photocopy security
- Paper-copy document security
- Accountability and responsibility
- Copyright, piracy and intellectual property
- Anti-virus software and firewalls
- Information security policies, standards and procedures
- Information risk management.

The respondents also recommended the following topics should be part of the elective contents and be taught to employees holding managerial positions: -

- Contingency planning
- Incident management
- IT laws, regulations and standards
- Computer auditing
- Information asset management
- IT Governance
- Change management.
The respondents were asked if they would prefer to take an examination after attending a programme. 54% of them indicated that they would like to take a test or examination after completing such a programme (see Figure 6.10 below).

![Preference for Taking an Examination](image)

Figure 6.10: Preference for Taking an Examination

It was also necessary to find out if an awareness certificate needs to be offered after attending a programme and/or after successfully passing an examination. Over 50% of the respondents did not like that idea (see Figure 6.11 on the next page).
The mechanism used for delivering the programme is of critical importance to the success of the awareness campaign (Hansche, 2001), and as such, respondents were asked to propose effective mechanisms to do it. They recommended the following:

- Newsletters
- Awareness posters and screen savers
- Computer-based training
- In-person instructor-led training.

The guidance and recommendations provided by the above sources and survey are sufficiently broad to base the contents of a generic programme on them. Therefore, a single content of such programme will be identified, based on these.
6.3 Generic Contents of an Information Security Awareness Programme

It is important to bear in mind that general and common aspects affecting most organizations’ employees would need to be included when identifying the topics for a generic programme. Any company-specific information, such as information security policies, guidelines and procedures, would only be introduced to the employees to make them aware of their existence, and encourage them to find out more from their respective organizations. Based on the guidance and recommendations from the sources studied and the survey, the following are identified as part of the contents of a generic information security awareness programme: -

- Data backup and storage
- Social engineering
- Remote/mobile worker security
- Malicious code security
- Password security
- E-mail security
- Physical and environmental security
- Computer ethics
- Privacy and confidentiality
- Paper-copy document security
- Accountability and responsibility
- Anti-virus software and firewalls
- Information security policies, standards and procedures.
- Information risk management
- Contingency planning
- Incident management
- IT laws, regulations and standards
- Computer auditing
- Change management.
Chapter 6: An Information Security Awareness Programme: Generic Content, Tools & Techniques

As pointed out previously, the mechanism used to deliver an awareness programme is critical to the success of it. This is discussed next.

6.4 Tools and Techniques for Offering an Information Security Awareness Programme

It can now be concluded that information security can only be improved upon through the proper awareness of staff. However, the level of success can always be improved upon by the method of awareness. Therefore, common tools and mechanisms employed by organizations will be examined before identifying suitable ones for delivering the generic programme.

6.4.1 Information security Website

This technique is most suitable for distributed environments. The Website can be implemented as a completely separate, independent site or as a sub-set or as an addition to an existing company intranet. In some cases, this approach can be implemented by creating two separate sites: an internal site for staff, accessible from the company network only, and an external site, accessible to everyone around the world (Danchev, 2003). It has the advantage that attendees of a Web-based session can study independently and learn at their own pace.

Web-based awareness courses are useful when an organization has many people who distributed in several locations, and who need to take the refresher or course at a time that is convenient for them. This technique is especially well suited for use by individuals who have diverse backgrounds and experiences in technology (Rudolph, Warshawsky & Numkin, 2002).
6.4.2 **Onsite instructor-led training**

This is one of the oldest, but one of the most popular, techniques for delivering training material to an audience. Speaking face-to-face with an audience is one of the most effective ways of stimulating security awareness. The approach is generally more effective when some form of visual aid is used to help emphasise key points. If presentations are used, experts recommend that they should not be more than 30 minutes long to allow the attendees to absorb the concepts presented (Thomson & Von Solms, 1998). The biggest advantage of the technique is the interactive nature of the instruction.

However, it has several potential disadvantages. For example, in a large organization, there may be a difficulty in scheduling sufficient classes so that all of the target audience can attend. In an organization that has a widely distributed workforce, there may be significant travel costs for instructors and students. Although there are these challenges for distributed environments, some learners prefer this traditional method to other methods (Wilson & Hash, 2003).

6.4.3 **Non-Web, computer-based training**

This technique continues to be popular, even with Web availability. It can be an effective method for the distribution of awareness material, especially if access to Web-based material is not feasible. Like Web-based training, this technique does not allow for interaction between the instructor and students or among students (Wilson & Hash, 2003). Tools, such as screen savers, which display security messages, login scripts, which are security messages displayed whenever a user logs on to a system, could be used.

*In many cases this approach can be used in conjunction with other approaches.*
6.4.4 Interactive video training

This is one of several distance-learning techniques available for delivering the awareness material. This technology supports two-way, interactive audio and video instruction. The interactive feature makes the technique more effective than non-interactive techniques (Wilson & Hash, 2003). Its advantages include (Thomson & Von Solms, 1998): -

- Adding extra life to a presentation
- Providing a multi-media dimension
- Reducing travel expenses

Though it has the above advantages, a few organizations can afford to implement it because of its expensive nature.

6.4.5 Security newsletters

Another way to reach and educate staff is by way of a security newsletter, usually sent via e-mail. It helps to enhance the visibility of a security awareness programme. Giving staff an additional option of having the newsletter sent to their private (home) e-mail address as well, helps in that they have the opportunity to read it at home, if they do not have time to do so at work. The main idea behind the creation of a security newsletter is to provide users with an interesting and engaging way of understanding the points outlined in the security policy (Danchev, 2003).

6.4.6 Educational contests

This is one of the tools that are used to convey the awareness material to staff. Conducting various security related contests from time to time not only helps measuring the security awareness level of staff, but also varies and innovates the educational process.
Password cracking contests are a good example. Contestants are faced with the challenge of cracking a file that has been protected by a password chosen by a fellow contestant, with the idea of finding/eradicating weak passwords. Upon conclusion of the contest a discussion is started on how the password was cracked, what made it a weak password (if that was the case), etc. Most staff are usually interested in such activities, and most of them will do their best to use hard-to-crack passwords following the recommendations on the process of creating strong passwords from the security awareness course (Danchev, 2003).

The discussion of the various tools and mechanisms for delivering the awareness material above will help to identify suitable and relevant tools and mechanisms for delivering the generic information security awareness programme. The eventual goal of the organization plays an important role in choosing the most appropriate tools and mechanisms. It must be stressed that the approached above can broadly be categorized in two groups, namely, those that can be used for initial information security awareness or training and those that are used to remind employees of information security aspects. This dissertation focuses primarily on the former group.

6.5 Delivering the Generic Programme

Not all the mechanisms discussed above would be suitable and effective for delivering a generic information security awareness programme. The goals of the generic approach would affect the suitability and the effectiveness of a mechanism, and the primary goal of such a programme is that it should be suitable for as many employees of as many organizations as possible (Du Plessis & Von Solms, 2002). To stay in line with this goal, the method of delivering the programme should be able to reach all these identified employees.

After considering this primary goal, a Web-based approach to delivering an awareness programme would be most suitable and effective.
Chapter 6: An Information Security Awareness Programme: Generic Content, Tools & Techniques

It could be implemented in two ways: through the Internet, or alternatively, an organization could host the Website on its intranet.

6.6 Conclusion

This chapter discussed how the topics of a generic programme were identified. Internationally recognised sources that comprehensively cover awareness programmes were studied with the aim of checking the areas recommended by them for inclusion. Several sources were studied so that the basis on which a generic programme rests is broad and valid. It was also necessary to identify the contents of such a programme by more practical means. Therefore, the chapter also gave the results of a survey conducted with some South African organizations known to follow sound information security principles. Based on the studied sources and the survey, the contents of a generic programme were identified. To achieve its goals, a Web-based mechanism for delivering awareness material was also recommended.

The next chapter discusses in detail the recommended topics of a generic information security awareness program.


Chapter 7

A Generic Information Security Awareness Programme

7.1 Introduction

In the last chapter, topics that could form part of the contents for the generic information security awareness programme were identified, using several internationally recognised sources that comprehensively cover awareness programmes. To make the foundation on which the programme is based as broad as possible, some awareness programmes offered on the Internet were also studied. The identification of the contents was also collaborated with some South African industries.

The focus in this chapter is to discuss the identified contents in detail. Two broad focus groupings exist for the identified contents and will be discussed in detail. For the sake of clarity and ease of understanding, within each of the focus groups, the contents will be grouped into logical categories. One of the most important aspects in awareness programmes is delivering material that is relevant and suitable to a particular focus group. Therefore, this chapter will also discuss aspects related to the level of detail to be included in the focus areas. Having clarified the level of detail to be expected in each focus area, the chapter will conclude by discussing the objectives behind each focus area.

7.2 The Contents of a Generic Information Security Awareness Programme

In Chapter 6, the following broad topics were identified, from which to form part of the contents of a generic information security awareness programme:

- Password security
- Paper document security
- Malicious code security
Chapter 7: A Generic Information Security Awareness Programme

- Data backup and storage
- Physical and environmental security
- Social engineering
- Web service (Internet and e-mail) security
- Mobile worker security
- Wireless security
- Computer ethics
- Information security policies, standards and best practices
- Accountability and responsibility
- Information asset management
- Incident management
- Information risk management
- Contingency planning
- Legal, regulatory and contractual requirements issues
- Change management
- Computer auditing

These topics are so broad and cover so many different processes that if they are offered in the way in which they are listed above, understanding and learning from them may be difficult. Therefore, they need to be logically categorised to assist in understanding them and facilitate offering of independent programme modules.

7.3 Broad Focus Groupings

Before the topics are categorised, it important to point out that two broad focus groupings exist; the first is for every information user, and the second only for the relevant IT management.

The focus group, ‘every information user’, comprises all employees who use either microcomputers or workstations as part of their daily activities.
Chapter 7: A Generic Information Security Awareness Programme

This group needs the necessary information security knowledge to ensure that information security is not compromised in any way. Therefore, to ensure that they have the relevant knowledge, they need to be made aware of the following areas: -

- Password security
- Paper document security
- Malicious code security
- Data backup and storage
- Physical and environmental security
- Social engineering
- Web service (Internet and e-mail) security
- Mobile worker security
- Wireless security
- Computer ethics

The focus group, ‘relevant IT management’, comprises top management of an organization, including managers of the various business departments, who are responsible for setting the information security policies, which must be followed by the whole organization (Thomson & Von Solms, 1998). This group needs to have the necessary security knowledge in order to make informed decisions regarding information security. Therefore, in order to achieve this, they need to be aware of the following: -

- Information security policies, standards and best practices
- Accountability and responsibility
- Information asset management
- Incident management
- Information risk management
- Contingency planning
- Legal, regulatory and contractual requirements issues
- Change management
- Computer auditing
Chapter 7: A Generic Information Security Awareness Programme

It has to be mentioned that, in most cases, IT management is also a normal information user group and must therefore, learn the topics in the first category.

Having classified the topics according to these two broad focus groupings, it is now necessary to categorise the topics in each of the focus group.

7.4 Categories of a Generic Information Security Awareness Programme

Several possible categorisations exist. One of the possible categorisations is grouping the topics according to areas of security knowledge, such as importance of information and information security, basic information security concepts, threats to and vulnerabilities of computer systems, procedures and how to implement them, etc. For example, the material on the importance of information and information security focuses on explaining how businesses rely on information, and also the consequences to them should their information be compromised (Human Firewall Organization, 2001; Du Plessis & Von Solms, 2002). Elements covered in this knowledge area include (Du Plessis & Von Solms, 2002):

- Legislation
- Standards
- Real-life examples

Another possible categorisation is grouping the topics based on the direct effect they have on the key characteristics of information: confidentiality, integrity and availability (NoticeBored, 2005). There are other topics that do not directly affect the key characteristics of information, such as information security policies, standards and best practices, and these are addressed solely to relevant IT management. This, therefore, defines another category. Then, there are other topics that neither directly affects the key characteristics of information nor are they addressed to relevant IT management. These, too, define another category.
This categorisation of topics, based on their effect on the key characteristics of information above, fits very well with the two broad focus groupings discussed in the previous section. All the topics in the ‘every information user’ focus group fall under the first four categories: confidentiality, integrity, availability and other information security topics categories and most of the topics in the ‘relevant IT management’ focus group fall under the security management category. Only two of the topics in this focus group fall under the availability topics’ category. Therefore, it will be adopted in this research.

7.4.1 Confidentiality topics

The topics in this category directly affect the confidentiality of information, both corporate and personal, in one way or another. The topics that fall under this category include (NoticeBored, 2005): -

- Password security
- Paper document security

7.4.2 Integrity topics

Topics in this category directly affect the integrity of information, both corporate and personal, in one way or another. There is only one topic discussed under this category: -

- Malicious code security

7.4.3 Availability topics

Topics in this category directly affect the availability of information, corporate or personal, in one way or another. Topics addressed in this category include: -

- Data backup and storage
- Physical and environmental security
- Incident management
- Contingency planning
Note that incident management and contingency planning are for relevant IT management. Therefore, they will be discussed under ‘relevant IT management’ programme.

7.4.4 Other information security topics

Topics in this category discuss other aspects of information security, e.g., e-mail security, Internet security, social engineering, etc.; therefore, the topics in this category include:

- Social engineering
- Web service (Internet and e-mail) security
- Mobile worker security
- Wireless security
- Computer ethics

7.4.5 Security management topics

Topics in this category concern the management of information security in an organization by management. Topics in this category are solely addressed to relevant IT management. Topics in this category include:

- Information security policies, standards and best practices
- Information risk management
- Information asset management
- Accountability and responsibility
- Legal, regulatory and contractual requirements issues
- Change management
- Computer auditing

The categorisation above will facilitate in offering independent programme modules under each category. It will also aid in easing understanding of concepts being presented. Before the two focus areas are discussed in detail, it is important to discuss the level of details to be included in the focus areas.
Chapter 7: A Generic Information Security Awareness Programme

7.5 Level of Detail in Each Focus Area

The users to be reached by an awareness programme largely determine the level of detail included in a programme, since it is important that users are only given materials that is applicable to them. There are basically two extremes of levels of detail; too much technical detail and too little.

7.5.1 Too much technical detail

Including a lot of technical detail in a programme is appropriate to employees with relatively high levels of knowledge with regard to information security matters. This would not be appropriate, for example, to end-users of information in a multi-disciplinary environment. End-users with minimal computer experience would be intimidated by, and would not respond well, to jargon (Rudolph, Warshawsky & Numkin, 2002). As a result, they would not develop an interest in the programme, and eventually they would not understand the concepts presented.

7.5.2 Too little technical detail

Including too little technical detail in a programme may result in misrepresentation of the concepts. As a result, the information delivered may not be sufficiently relevant to the audience. Therefore, including too little technical detail is not appropriate in any way, because understanding how processes work is essential; however, people with a little understanding of the processes might become even more confused if the information they are presented with is misrepresented.

The challenge is to find the balance between too much and too little technical detail. This introduces the third level, which can be called ‘the correct balance of technical detail’.
7.5.3 Correct balance of technical detail

This level explains some of the concepts in everyday/layman’s terminology. Awareness material should be presented in such a way that employees find it easy to learn and remember. This helps employees who, more than likely, have very little, if any, knowledge of information security, to understand the concepts being presented. This is very appropriate and suitable in a multi-disciplinary environment because the audiences have similar levels of computer knowledge and experience, and similar needs (Rudolph, Warshawsky & Numkin, 2002).

It is important that awareness material for the generic programme is presented in a simple and straightforward manner. It needs not be very technical in nature. The discussion of the level of detail above will help in deciding the details to include when discussing the focus areas. The focus areas will be described in brief. The detailed discussion of the focus areas is done in Appendix A.

7.6 Description of the Focus Areas

For the sake of clarity, the focus areas of the generic programme will be discussed under the two focus groupings discussed above; one for every information user and the other for relevant IT management. As previously stated, IT managers are also information users, and as such, they need to know aspects under every information user group before undergoing through the aspects intended for them only in relevant IT management group.

7.6.1 Programme 1: For every information user

This subsection only discusses topics identified for all the end-users of information in a generic environment.
Confidentiality topics

♦ Password Security

Description

These days, almost everyone who uses a computer is familiar with the concept of ‘logging on’. In technical jargon, this is known as identification and authentication. The combination of a username and password when logging on is how the computer knows that you are who you claim to be. Passwords are considered the first line of defence against attackers, who may sit down at a computer and attempt to log in to a valid account. Passwords are also considered the last line of defence against attacks across the network. When technical controls fail, or are configured incorrectly (as is often the case), a secure password is the only thing that keeps hackers and worms out (SANS Institute, 2005).

♦ Paper document security

Description

Employees should know that security of paper documents is as necessary as that of electronic documents. All these documents contain vital business information that if compromised, impacts on an organization in various ways. Documents containing confidential information must be placed out of sight, preferably in locked cabinets when not in use. Paper records containing personal information must be disposed of securely. Documents containing confidential information that does not require archiving should also be disposed of securely, e.g., shredding them. It is necessary to develop routine and appropriate methods for handling documents containing confidential information, such as a written retention policy.
Chapter 7: A Generic Information Security Awareness Programme

- **Integrity topics**

  - **Malicious code security**

  **Description**

  Viruses, worms, and Trojans are all examples of attack software that is known collectively as malicious code or malware. These can hide behind an infected Web page or disguise themselves as, amongst others, a downloadable game, screen saver or e-mail attachment.

  Viruses are programs that are designed to spread by first infecting executable files or system areas of hard and floppy disks and then spread or self-replicate. Viruses usually operate without the knowledge or desire of the computer user (SANS Institute, 2005). They usually require interaction from someone to be activated. The virus may arrive in an e-mail message as an attachment or be activated by simply opening a message or visiting a malicious Website. Some viruses consume storage space or simply cause unusual screen displays. Others destroy information (New York State, 2005). If a virus infects a computer, all the information on a hard drive may be lost and/or compromised. It has to be known that viruses may also spread to other machines that share the information accessed by the infected machines.

  Worms are similar to viruses, but they self-replicate, they are self-propagating. This means that they spread themselves; users do not even have to open or run an attachment (New York State, 2005). Worms look for systems that are vulnerable to a particular type of attack, and then exploit that weakness. Once the weakness has been exploited on a computer, the worm copies itself to that computer and starts looking for other vulnerable computers.
Trojans (also known as backdoors) are malicious code hidden in a legitimate program that, when executed, performs some unauthorized activity or function. Trojans install themselves on a computer once vulnerability has been exploited. This can be done manually by a hacker, or automatically by a worm or a virus. The common element is that the user never has any idea that this has occurred (SANS Institute, 2005).

There are more than 75,000 different examples of malicious codes that exist, so the threat is real, and it causes real monetary damage to companies. Viruses can exhibit many different symptoms, because there are many examples (SANS Institute, 2005), and if a machine behaves erratically, it is advisable to contact an organization’s computer support representative.

- **Availability topics**

  - **Data backup and storage**

  **Description**

  Backup of data or processes is a critical safeguard in any IT security environment (Du Plessis & Von Solms, 2002). But the major function that backups serve is insurance. If an organization follows a simple set of best practices with respect to backups, it has the protection against mishaps that range from the smallest (accidentally deleted files) to the largest (network operation centre catastrophe).

  Data backup and storage plays a major role in disaster recovery, but it can also play a crucial part in effective incident response (SANS Institute, 2005). For example, if an intruder manages to compromise a server, it is a much simpler task to reinstall the system from the last known ‘clean’ backup. On the other hand, it would be difficult to recover from the compromise if there was no backup in place.
Chapter 7: A Generic Information Security Awareness Programme

♦ **Physical and environmental security**

*Description*

There is basically a wide array of threats that could exploit unrecognized or inadequately addressed vulnerabilities of the physical environment. These threats include natural disaster threats, e.g., earthquakes, floods, hurricanes, tornadoes, landslides, etc., and unintentional or intentional physical threats, e.g., power outages, equipment failures, fires, proximity of potentially toxic or explosive industrial facilities, local crime, etc. Physical and environmental security plays a vital role in protecting all the resources of an organization, including its people. Failure to recognize and effectively address local threats and associated vulnerabilities, both internal and external, can result in a potentially disastrous disruption of information technology functionality (Information Systems Security Association, 2004).

- **Other information security topics**

♦ **Social engineering**

*Description*

Social engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to gain access to office spaces, accounts, computer systems, networks, or obtain proprietary information without the realization that a security breach is occurring (New York State, 2005). The methods used include lying, fake e-mails, phone calls, and setting up phony Websites (SANS Institute, 2005). Some e-mails entice the recipient into opening an attachment that activates a virus.
Chapter 7: A Generic Information Security Awareness Programme

Something to keep in mind is never to give out personal information, such as passwords, credit card numbers, social security numbers, or other confidential information, if the person asking for the information is not very well known to you. It is also important to investigate any request for information with an authorized representative from the organization, before providing the information, if there is doubt about the authenticity of a request. Finally, if you suspect social engineering is being attempted, contact your network administrator or Help Desk to ensure a timely and appropriate response.

♦ Web service (Internet and e-mail) security

Description

One of the greatest security risks in the company is the Internet connectivity, and its misuse through uneducated employees. It is a fact that some employees will surf to sites that are strictly prohibited, and most probably will somehow end up downloading malicious files and/or hostile code from hacker sites (Danchev, 2003). Therefore, it is always a good idea to explain, in detail, the possible dangers of surfing the Internet.

It has to be known that no one on the Internet is immune. Those affected include banks, financial and insurance companies, brokerage houses, consultants, government contractors and agencies, hospitals and medical laboratories, network service providers, utility companies, the textile business, universities, and wholesale and retail trades. The consequences of a break-in cover a broad range of possibilities: a minor loss of time in recovering from the problem, a decrease in productivity, a significant loss of money or staff-hours, a devastating loss of credibility or market opportunity, a business no longer able to compete, legal liability, and the loss of life (Software Engineering Institute, 1997).
Chapter 7: A Generic Information Security Awareness Programme

Generally, e-mail systems are a high-risk area due to their constant availability to the outside world. The use of e-mail to conduct business, contact clients, and its integration in many other business-related processes exposes an organization’s mail addresses and mail systems to potential attackers. On the other hand, this is also the number-one entry point from which most of the malicious programs enter an organization.

Therefore, a well-known and proven malicious code-protection program is a must-have, as it will detect, block and/or filter out most of the known dangerous files and hostile scripts trying to enter an organization’s networks (Danchev, 2003).

♦ **Mobile worker security**

*Description*

Computers, nowadays, are accessible via a variety of mobile equipment, such as laptops, PDAs and even cell phones. A person can even download information from the Internet to a cell phone. While convenient and fun to use, some good practices help protect the information contained in this equipment. These devices carry vital information that must be protected. They are more easily stolen or misplaced because of their size. It is always important to remember that if a laptop, a PDA or a cell phone is gone, the information is as well.

♦ **Wireless security**

*Description*

Wireless networks are very popular for their ease of use and portability. The Internet can be reached via radio waves without having to plug a machine into a network.
It is with the same ease of connecting that malicious individuals connect to unprotected networks. Attackers conduct drive-by eavesdropping, called “war driving” to listen in on unsecured devices in homes and businesses (New York State, 2005). Therefore, extra measures need to taken to ensure that the wireless equipment is secure from these malicious individuals.

♦ **Computer ethics**

*Description*

The use of information technology in an organization can be regulated with the introduction of many rules and regulations. The use to which IT can be put is very widespread, and the correct usage of this very powerful resource will, in many cases, rest on the good judgement and ethics of that particular user (Thomson & Von Solms, 1998). Computer ethics form a basis for deciding what is right and wrong when making decisions (Du Plessis & Von Solms, 2002). Therefore, all employees need to observe these ethics so that they are not held reliable for some unethical behaviour.

The awareness programme for the end-users of information includes everybody in an organization. Therefore, it is recommended that relevant IT management have to go through the above programme before doing the ‘elective’ modules described below, which are only applicable to them.

### 7.6.2 Programme 2: For relevant IT Management

This subsection discusses the ‘elective’ modules identified for relevant IT management in a generic environment.
Chapter 7: A Generic Information Security Awareness Programme

- Availability topics

  ♦ Incident management

Description

A computer security incident can be defined as anomalous activity on a computer. Viral infections, evidence of intrusion, odd network activity, unauthorized physical access, or misuse of resources, are basically some of security problems that can constitute an incident.

Management should know that incident response is a critical part of overall corporate security. When an incident occurs, every individual responsible should be involved: the user, the administrator, management, the response team, and sometimes, law enforcement (SANS Institute, 2005). Some of the key factors that help to make incident response effective are rapid reaction, clear communication, and knowing what to do before an incident occurs.

♦ Contingency planning

Description

Organizational entities depend on their IT resource infrastructure now, more than at any previous time in history, to deliver mission-critical information in a timely fashion. The operational importance of information assets, whether based on cost or time factors, is such that organizations can ill afford to endure the consequences of significantly disruptive events impacting on supporting information technology resources or the information assets directly (Information Systems Security Association, 2004). Therefore, the key role for managers is strategic planning to ensure the continuous information systems’ availability when a successful attack and/or a natural disaster occur.
Management should plan for and operate information technology in such a way as to preserve the continuity of organizational operations. The most effective way of doing this is through a business continuity plan (BCP). A BCP is a guiding document which allows an organization to continue operations when disasters occur (Thomson & Von Solms, 1998), such as floods, earthquakes, power outages, computer viruses, etc.

Management should identify sensitive and critical systems that are crucial to the daily operations of an organization. All designated sensitive and critical systems should have a written backup procedure and disaster recovery plan. This helps to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters (NHS Information Authority, 2004).

**Security management topics**

- **Information security policies, standards and best practices**

*Description*

In a broad sense, information security policies are management directives that establish the business goals, security framework, responsibilities, and governance (Hunter, 2000). As building a good security policy provides the foundations for the successful implementation of security-related projects in the future, this is, without a doubt, the first measure that must be taken to reduce the risk of unacceptable use of any of the company's information resources. The first step towards enhancing a company's security is the introduction of a precise, yet enforceable, security policy, informing staff on the various aspects of their responsibilities, general use of company resources and explaining how sensitive information must be handled. The policy will also describe in detail the meaning of acceptable use, as well as listing prohibited activities (Danchev, 2003).
The development and the proper implementation of a security policy is highly beneficial as it will not only turn all staff into participants in the company's effort to secure its communications, but also help reduce the risk of potential security breaches through “human-factor” mistakes. These are usually issues, such as revealing information to unknown or unauthorized sources, the insecure or improper use of the Internet and many other dangerous activities. Additionally, the building process of a security policy will also help define a company's critical assets, the ways they must be protected and will also serve as a centralized document, as far as protecting information assets is concerned (Danchev, 2003). Therefore, management must ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security (Information Systems Security Association, 2004). Management must also make sure that all staff are educated and trained in these policies.

Standards and best practices are the most direct and efficient means of achieving a standard of due care (Hunter, 2000). In general, they advocate good security principles in information security. As such, management must make an effort to familiarise itself with standards and best practices acceptable at national or international level. This will help in following security standards and best practices that are acceptable nationally or internationally. Two such standards accepted on an international level are ISO/IEC 17799 and ISO/IEC 13335. ISO/IEC 17799 is used as a reference for implementing and maintaining information security within an organization, since it provides a set of security controls which has been compiled using the best security practices internationally (Thomson & Von Solms, 1998). ISO/IEC 13335 lays down internationally accepted guidelines in the field of information technology security management.
♦ **Information risk management**

*Description*

Management needs to manage threats to information in the same way as one would manage risk to personal belongings. Management should ensure that information security measures are appropriate to the value of the assets and the threats to which they are vulnerable. In order to choose effective and efficient measures, management must identify the assets to be protected, the threats to the assets, and the vulnerability of the assets or their environment to the threats (Information Systems Security Association, 2004).

Management must make sure that well-informed owners, managers, custodians, or other responsible parties must assure the security of information assets, with regard to the value of their confidentiality, integrity, and availability requirements. Such an approach, performed strategically, on an on-going basis, or as changes dictate, must enable well-informed decisions regarding whether to accept, mitigate, or transfer the risks associated with the information assets and supporting IT resources. These decisions should be based on the monetary value of the assets, probability and consequences of direct or indirect harm or loss, related threats, effectiveness of existing safeguards and controls, and whether additional safeguards or controls could be expected to provide cost-effective incremental risk mitigation (Information Systems Security Association, 2004).

♦ **Information asset management**

*Description*

Management should routinely catalogue and value information assets, and assign levels of sensitivity and criticality. Information, as an asset, must be uniquely identified and responsibility for it assigned.
In order to manage information assets efficiently, management must know what to protect. In order to be effectively managed, it is essential to identify and enumerate the core attributes of information as assets. These information asset attributes include (Information Systems Security Association, 2004): -

- Identity
- Ownership
- Custody
- Content
- Value (ideally expressed in monetary terms) of the confidentiality, availability, and integrity of the information assets
- Sensitivity (which relates directly to confidentiality)
- Criticality (which relates directly to availability and integrity).

An organizational ownership of information assets must be established. The person or custodian legitimately established as the owner of an information asset has the authority and responsibility to make or delegate decisions regarding the security of it. It is, typically, the organization that will ultimately suffer liability, loss, or other harm, if the confidentiality, availability, or integrity of the information asset is compromised (Information Systems Security Association, 2004).

The identity and content of an information asset must be clearly established for the owner to make informed decisions regarding its security. Knowing the value of the information asset, as related to its confidentiality, availability, and integrity, enables the owner to understand the financial risks and associated threats that must be mitigated when establishing security requirements for it (Information Systems Security Association, 2004). It is important to keep in mind that most information attributes change value over time, in some cases increasing and in others, decreasing, and as such, these attributes should be reviewed regularly.
Chapter 7: A Generic Information Security Awareness Programme

♦ Accountability and responsibility

Description

Accountability characterizes the ability to audit the actions of all parties and processes that interact with information. Therefore, management must make sure that information security accountability and responsibility are clearly defined and acknowledged. This helps to clearly define, identify, and authorize roles and responsibilities at a level commensurate with the sensitivity and criticality of information. The relationship between all parties, processes, and information must also be clearly defined, documented, and acknowledged by all parties. All parties must have responsibilities for which they are held accountable (Information Systems Security Association, 2004).

♦ Legal, regulatory and contractual requirements issues

Description

Information security, which is regulated by some laws and regulations, and understanding this legal environment are ways of controlling an organization’s liability for privacy and security risks. Management should take steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets.

In order for an organization to diligently comply with all legal, regulatory, and contractual requirements associated with its operations, it is necessary to ensure that no requirement exists for which compliance measures have not been put in place. As part of this effort, plans should also be in place to address potential actions against the organization should their policy, processes, or actions be called into question (Information Systems Security Association, 2004).
Chapter 7: A Generic Information Security Awareness Programme

♦ Change management

Description

This focuses on IT operational change management, beginning when upgrades or updates to IT assets, i.e., infrastructure or applications, are identified for movement to production and ending when such assets are retired from the production environment. This includes application maintenance and emergency change controls (Taylor, Allen, Hyatt & Kim, 2005).

Change management is sometimes difficult for organizations to master, because so many stakeholders are involved (e.g., business managers, application system developers, IT operations staff, auditors). However, this is not a reason for organizations to be complacent about low performance. Stable and managed production environments require that implementation of changes be predictable and repeatable, following a controlled process that is defined, monitored, and enforced (Taylor, Allen, Hyatt & Kim, 2005).

♦ Computer auditing

Description

Computer auditing is a branch of general auditing, i.e., control of information and communications technologies. It concerns primarily the study of computer systems and networks from the point of view of examining the effectiveness of their technical and procedural controls to minimize risks (IsecT Ltd, 2006).

All audits are performed in relation to certain risks identified by the auditor, which he/she believes are important. Analysis of the risks leads to the definition of control objectives. For example, the auditor might be concerned that a finance system could be modified by unauthorized persons, so would determine that there is a control objective to prevent this.
Chapter 7: A Generic Information Security Awareness Programme

The specific controls that are actually embedded in, or associated with, IT systems and processes are then assessed to determine whether they adequately address the risks, meaning that they satisfy the control objectives (IsecT Ltd, 2006). It is advisable to implement best practice controls.

In conclusion, it is important to point out that a generic awareness programme makes sacrifices in the scope of the material that it presents. The scope needs to be sacrificed in order to satisfy the primary goals of keeping the programme generic. In so doing, company-specific needs are not fulfilled by such a programme. Instead, it tries to provide a baseline of awareness by educating the employees on the essentials of information security. Having such a baseline in place can provide organizations with the assurance that some basic level of awareness exists among employees.

7.7 Conclusion

This chapter gave a comprehensive discussion of the topics identified for a generic information security awareness programme. Two broad focus groupings were identified and then the focus areas (the topics) were logically divided between the two focus groupings. Within each focus group, the topics were logically categorized for the sake of clarification and understanding. It was vital to discuss the level of detail to be included in this kind of awareness programme since it is very necessary to offer material that is only relevant to employees. Therefore, a section was dedicated to discussing aspects related to level of detail before the focus areas were described.

It is important to points out that aspects thought to be vital and necessary under each topic will be discussed in more detail in Appendix A to bring out the elements that information users should be aware of. Possible scenarios will also be given, where necessary, to make employees aware of the reality of threats to information assets in current business conditions.

The next chapter discusses a summative conclusion of the project.
Chapter 8

Conclusion

8.1 Introduction

The objective of this project was to identify general topics that can be included as part of the contents of an information security awareness programme intended to be offered to international, interdisciplinary and diverse audiences, and to specifically find out the most effective techniques for delivering such a generic content. This was accomplished by addressing the following research objectives:

- Firstly, identifying the **generic content component** of such a programme
- Secondly, finding out the **level of detail** that should be included in each topic
- Thirdly, finding out the effective **techniques** for delivering such programme.

Current approaches stress the need to develop programmes from existing information security policies and procedures already in place. But not all organizations have these because their development is a lengthy process that requires time, money, and specialized knowledge. Organizations without these policies and procedures do not have a basis on which to support their programmes. This has contributed to the current low level of information security awareness in most organizations. But most of these programmes do have a generic component that is company-independent. Therefore, to address the first objective, contents for information security awareness programmes were examined in order to identify topics that are general to most organizations.
This was complemented by studying what information security standards recommend, what is covered in some of the awareness programmes offered on the Internet, and the survey conducted with some South African organizations known to follow sound information security principles. Based on the guidance from these sources and the survey, the generic content component was identified. Therefore, it can be concluded that the first secondary objective has been met satisfactorily.

One of the most important aspects in awareness programmes is delivering material that is relevant and suitable to a particular focus group. The users to be reached by an awareness programme largely determine the level of detail included in a programme, since it is important that users are only given materials that are applicable to them. Therefore, to determine the level of detail to be included in the focus areas, aspects related to the level of detail were discussed. It was concluded that the correct balance of technical detail needs to included in topics because the audiences to be reached by the generic programme, more than likely, have very little, if any, knowledge of information security. Therefore, presenting the awareness material in a simple, straightforward manner will help the audiences to understand the concepts being presented. Based on the arguments in this paragraph, it can be claimed that the second secondary objective has also been met.

Information security can only be improved upon through the proper awareness of staff. However, the level of success can always be improved upon by the methods of awareness. Therefore, common tools and mechanisms employed by organizations were examined before identifying suitable ones for delivering the generic programme. The primary goal of a generic programme is that it should be suitable for as many employees of as many organizations as possible. To stay in line with this goal, the method of delivering the programme should be to be able to reach all these identified employees. After considering this primary goal, the Web-based method was identified as a suitable and effective method for delivering the generic programme. As the most effective techniques of delivering awareness programmes have been described and concluded, also, the third secondary objective has been met.
Therefore, having successfully met all the three secondary objectives, it can be concluded that the primary objective of this project, “to identify general topics that can be included as part of the contents of an information security awareness programme, intended to be offered to international, interdisciplinary and diverse audiences, and to specifically find out the most effective techniques for delivering such a generic content” has successfully been met.

8.2 Summary of the Chapters

The first part of the project was devoted to discussing the value of information in various business transactions nowadays. Information has become a valuable business asset, and as such, organizations have a responsibility to protect it because they risk losing a host of factors, such as reputation, market shares and direct revenue, if it is compromised in any way.

Some of the factors that have impacted the protection of business information were explained. Previously implemented physical (mantraps, etc.) and technical (access control, etc.) security measures alone are no longer adequate. Consequently, employees have a more critical role to play nowadays.

Thereafter, a comprehensive discussion on how information security is managed in organizations was given, and how these follow well-structured approaches to properly protect business information assets. Some of the key components of an information security programme, which could have a very large impact on the success of the programme, were discussed, and it was emphasized that they need to be considered when structuring such a programme. Some of the published frameworks for information security that an organization can adopt or adapt were discussed to emphasize the point that a proper methodology for implementation needs to be followed.
Chapter 8: Conclusion

One point that was strongly emphasized was that information security must not be viewed only from a technical viewpoint, because the human dimension cannot be reduced by any amount of technology. In addition, it was noted that everyone in the organization should be actively involved in securing information assets, and their cooperation is of utmost importance.

The need to involve people highlighted the need to discuss information security awareness programmes that make employees aware of their own responsibilities. It was found that different awareness programmes, based on major employee groupings exist, and these are important and need to be implemented. Information security awareness for end-users was further discussed to highlight the complementary role it plays in instilling an information security culture amongst employees.

The next section was devoted to discussing the current approach to the development of these programmes by referring to the recommendations of ISO/IEC 17799:2005 and ISO/IEC 13335-1:2004. These standards stress the need to base the awareness programmes on existing security policies in organizations. This was pointed out as a limitation because not all organizations have such policies in place. Some of the recently conducted surveys confirmed that there is an information security awareness gap in many organizations. Therefore, it was suggested that in order to raise this level, a different approach to developing programmes has to be taken to complement the existing company-specific approach.

Then, a comprehensive discussion of the proposed generic approach to a security awareness programme was provided by comparing the contents of many programmes and finding common aspects covered by them. These commonalities could form the basis of a non-company specific generic information security program.

Thereafter, how the contents of the proposed approach were identified was discussed, detailing the sources used. Tools and techniques effective for delivering these were also discussed.
Finally, the recommended generic awareness programme was discussed in detail by identifying the programme’s topics and discussing them in detail.

### 8.3 Possible Further Enhancements

It is important to realize that an information security awareness programme has to deliver information that is current in the information security discipline, e.g., legislations, which have an effect on the functioning of organizations, threats to organizations, etc. Therefore, the programme needs to be updated frequently, whenever it is needed to reflect these current concerns in information security so that employees are not taught out-of-date information.

### 8.4 Conclusion

Information is playing an ever-increasing role in the running of most businesses nowadays. Management, technical and operational controls are used to ensure that it is properly protected. One of the operational controls used is an information security awareness programme, which basically fits into a wider information security programme. Current approaches to the development of programmes prohibit some organizations, without information security policies in place, from implementing them. This project has attempted to develop a generic approach that does not depend entirely on the existing information security policies in organizations. The generic approach would allow most organizations, even those without policies in place, to be able to develop the programme.


Kathleen, C. (2003). Closing the security gap: data protection initiatives should include employee training - HR Technology. HR Magazine.


Bibliography


Appendix A

Detailed Discussion of Generic Contents
Appendix A: Detailed Discussion of Generic Contents

Detailed Discussion of Generic Contents

1. Introduction

In Chapter 7, two broad focus groups were identified for the generic programme. Therefore, the identified contents will be discussed under these two groups. Also, within each focus group, the contents were grouped into logical categories for the sake of clarity and ease of understanding them. These categories will be maintained in the detailed discussion of the focus areas that follows.

It was also pointed out that it is important to deliver material, which is relevant and suitable to a particular focus group, for the programme to succeed, and this is largely determined by the type of users to be reached by the programme. Since employees to be reached by the generic programme have, more than likely, very little, if any, knowledge of information security, it is important that awareness material for the generic programme is presented in a simple and straightforward manner. Explaining some of the concepts in everyday/layman’s terminology will be vital to the success of the programme in a multi-disciplinary environment.

Each focus group was described in Chapter 7. The objective of this Appendix is to give some aspects that employees have to know under each focus area. Where possible, a possible scenario will be given to reinforce the concepts covered and to make the picture as real as possible.

In order for employees to obtain a better understanding of the aspects being discussed, it is important to define some terminology that is going to be used when discussing the topics. Understanding these terms will help the employees obtain the most benefit from this programme.
Also, where possible, a possible scenario will be given under a topic to make the picture as real as possible to the employee.

2. Terminology

The following terminology will be encountered during the security awareness course. Therefore, it is encouraged that course members understand it before starting to study the course material.

Accountability The property that someone is held responsible for a specific task. This ensures that any incident can be traced uniquely to an individual.

Asset Anything that belongs to an organization and is of value to it.

Availability The property of information being available or accessible on demand by an authorized user or resource.

Confidentiality The property that information is only made available or disclosed to authorized individuals or processes.

Cracker An individual who uses an advanced knowledge of networks or the Internet to compromise network security.

Controls Measures that are taken protect against the risks that threaten information and information technology assets of an organization.

Hacker An individual who attempts to compromise the security of an IT system with the intention to cause disruption or obtain unauthorized access to information.

Impact The consequence that an organization suffers after a threat has successfully managed to exploit a vulnerability of an asset.

Integrity A property that ensures that information and processing methods are complete and accurate.
Appendix A: Detailed Discussion of Generic Contents

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT security</td>
<td>All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.</td>
</tr>
<tr>
<td>Reliability</td>
<td>The property of consistent behaviour and results.</td>
</tr>
<tr>
<td>Residual risk</td>
<td>A risk that still remains after safeguards have been implemented. It has to be known that risks are usually partly mitigated by the safeguards.</td>
</tr>
<tr>
<td>Risk</td>
<td>The potential that an existing specific threat will exploit a vulnerability of an asset and cause loss or damage to that asset.</td>
</tr>
<tr>
<td>Safeguard</td>
<td>A mechanism or procedure, which is used to reduce a risk to an asset.</td>
</tr>
<tr>
<td>Threat</td>
<td>A potential violation of security.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>A weakness or a set of weaknesses of an asset that could allow a threat to cause damage to it.</td>
</tr>
</tbody>
</table>

This terminology is given to assist in understanding the concepts discussed in the topics below. The next sections are dedicated to discussing the material or the topics of the awareness programme.

3. **Focus Areas**

For the sake of clarity, the focus areas of the generic programme will be discussed under the two focus groupings discussed above: one for every information user and the other for relevant IT management.

3.1 **Programme 1: For every information user**

This sub-section only discusses topics identified for all the end-users of information in a generic environment.
3.1.1 **Confidentiality topics**

The topics in this category directly affect the confidentiality of information, both corporate and personal, in one way or another. Users need to be aware of the following aspects in this category:

♦ **Password security**

Passwords are an extremely important system protection mechanism, and as such, there are some special precautions that should be taken in choosing, using, and protecting them. Some of those precautions will be discussed.

▪ **Weak passwords**

Passwords are one of the primary components of a good security system. Computer accounts, databases, and even some Websites use them to limit access to authorized users only. Unfortunately, users do not take this access control device seriously enough, and unknowingly create a significant vulnerability that ill-intentioned people take advantage of. The major password mistake made by users is the choice of a “weak” password. The following lists some weak password characteristics ([SANS Institute, 2005; Thomson & Von Solms, 1998](#)): -

- Contains less than eight characters
- Is a word found in a dictionary (English or foreign)
- Is a common usage word, such as the name of family member, pet, friend, character, computer term and name, birthday or other personal information, etc.
- Any of the above spelled backward.
Appendix A: Detailed Discussion of Generic Contents

- **Strong passwords**

Creating a password that is completely secure can be a difficult task. The key to a strong password lies in how long the password is, combined with the use of as many character types as possible (SANS Institute, 2005). It is important to note that there is software that specializes in guessing passwords, and is easily obtained, and simple to use. So, the goal is to choose a password that will take a very long time for these programs to guess. Some of the recommendations for creating strong passwords are listed below (Centre for Information Technology, 2001; SANS Institute, 2005):

- Meet minimum length requirement set by corporate policy
- Use upper and lower case letters
- Use numbers
- Use special symbols, like punctuation
- Employ mnemonics like song titles or catch-phrases and strengthen by following bullets above
- Use a password that is easy to remember so that you do not have to write it down
- Use a password that can be typed quickly. This makes it harder for someone to steal your password by watching over your shoulder
- Do not use login name or real name in any form, whether it be reversed, capitalized, doubled, etc
- Do not use any information that is easily obtainable. This includes spouse’s or child’s name, license plate numbers, telephone numbers, ID numbers, brand of automobile, name of the street, etc
- Do not use a password of all digits, or all letters. This significantly decreases the search time for a cracker
- Do not use a word contained in a any English or foreign language dictionary, spelling lists, or other lists of words
Appendix A: Detailed Discussion of Generic Contents

Users need to be fully aware of their responsibility to keep their usernames and passwords as secret as possible. Users need to know that it is completely forbidden to share this information with anyone, ranging from the representatives of the Information Security Office (ISO), their family members, etc (Danchev, 2003).

- **Password management**

Choosing a strong password is a very important part of operating a computer securely. As you move to stronger passwords and the requirement to change them more frequently, good password management techniques become more important. The following are some recommendations for secure password management (SANS Institute, 2005; Dark, 2000):

- Never write down a password
- If you need to, write down obscure password “hints”
- Approved password storage software may be an acceptable alternative
- Passwords should be changed periodically
- Do not reuse previous passwords
- Never tell or share a password with anyone
- When your computer prompts you to save your password, click on “No”
- If you think your password has been compromised, change it immediately. Employees should notify the information security officer or manager at their organization.

- **Unique account passwords**

Most users have accounts on multiple systems, including e-mail accounts and Website accounts.
They have more than a single account, and managing all those passwords can be tough. Many employees make the mistake of using one password for all of their accounts. The problem with this approach is that if hackers are somehow able to compromise the password associated with one account, they can effectively walk across all of the systems and accounts accessed by the password (SANS Institute, 2005). Separate passwords for separate accounts help keep an intruder contained in one place, if he or she is lucky enough to crack one. Some of the recommendations to follow for multiple account passwords are (SANS Institute, 2005): -

- Choose completely unique passwords for every account, including system, e-mail, Web page, database accounts
- Do not use categories like cities, teams, or beers
- Do not use keyboard patterns.

Possible scenario

The following example demonstrates the need to keep passwords unique and completely different for different accounts. An employee had similar password for different workstations allowing him access to multiple computers, not knowing that this was a vulnerability to more than one workstation. An intruder managed to figure out and crack the password. He was able to “hop” from one workstation to the next because he had access to all of them.

♦ Paper document security

It should know that security of paper documents is as necessary as that of electronic documents. All these documents contain vital business information that if compromised, impacts on an organization in various ways. Some of the aspects to be known about the security of paper document are discussed below.
Photocopy machines are located in almost every office in the world. They are often located in public areas to make access to them simple for every employee. This makes spotting fraudulent use all the more difficult. Some of the information security issues about photocopying that users should know include (RU Secure, 2005): -

- Unauthorized copies can be made releasing confidential information
- Authorized copies may be mislaid, disclosing confidential information to unauthorized parties
- Unauthorized persons can, nevertheless, sometimes gain access to sensitive material and use copying facilities for personal or other reasons
- Unauthorized people may see and remove copies during the copy process
- Unauthorized people may see the contents of the document during copying
- Confidentiality can be breached by original sheets being left in machine
- Sheets of partially copied material can become jammed in the machine, which can disclose sensitive information to unauthorized persons, e.g., the person removing the blockage.

Some of the key actions to take to ensure safety of document photocopying include (RU Secure, 2005): -

- Documents, which are classified as confidential, should not to be copied without formal authority
- Ensure that you keep all copies in your control whilst copying
- With sensitive information, only make the required number of copies, never any ‘spares’
- All original sheets must be accounted for at the end of copying
Appendix A: Detailed Discussion of Generic Contents

- An organization’s access control system should safeguard against access to unauthorized material
- Challenge, and report to those responsible for security, any person observed copying documents seemingly beyond the scope of their job
- Challenge, and report to those responsible for security, any visitor copying your organization’s documents
- Never leave the copier or documents unattended
- Gather each set of copies as they are completed
- Ensure that unauthorized people cannot read any documents whilst passing the machine
- When doing confidential copying, ensure other persons are not waiting to use the photocopy machine
- All unwanted sheets must be disposed of securely, e.g., the shredder
- Clear the damaged sheets personally, or closely supervise the clearance of the sheets.

3.1.2 Integrity Topics

Topics in this category directly affect the integrity of information, corporate or personal, in one way or another. There is only one topic discussed under this category: -

- **Malicious code security**

Viruses, worms, and Trojans are all examples of attack software that is known collectively as malicious code or malware. These can hide behind an infected Web page or disguise themselves as a downloadable game, screen saver or e-mail attachment.
Appendix A: Detailed Discussion of Generic Contents

There are more than 75,000 different examples of malicious codes that exist, so the threat is real, and it causes real monetary damage to companies. Viruses can exhibit many different symptoms, because there are many examples (SANS Institute, 2005), and if a machine behaves erratically, it is advisable to contact an organization’s computer support representative. If working at home, disconnect the computer from the Internet and run a full virus scan.

- Preventing malware

Good anti-virus software will detect and clean malware, including Trojan programs. Therefore, all computers must have anti-virus software installed, and it is the responsibility of all staff to scan their computers regularly. All software and incoming files should be scanned, and staff are advised to scan new information files and software before they are opened or executed.

Some of the tips for preventing malware include (Danchev, 2003; SANS Institute, 2005; New York State, 2005):

- Before implementing or using software from any source, check it for viruses with a current virus scanner
- Store removable media as CDs/thumb drives/diskettes as “write protected” whenever possible to prevent infection by viruses
- Do not load free software on a computer from an untrusted source
- Do not open files with extensions such as .bat, .cmd, .com, .exe, .pif, .scr, or .zip if you do not know the source
- Be careful about downloading games, screensavers and other files. Download only from trusted Internet sources
- Be careful about file and music-sharing services, because you can inadvertently share files you did not intend to share. Downloaded files can contain viruses and other malicious code.
Appendix A: Detailed Discussion of Generic Contents

- **Anti-virus software**

SANS Institute (2005) reports that viruses cause more damage to computers and information each year than any other type of attack. They can destroy the operating system, delete or corrupt files, or choose sensitive files from a hard drive to mail to people in address book. As a result, anti-virus software is the most critical component of computer protection. It should be the first element that is installed on any Microsoft Windows-based system. Even if an organization has centralized anti-virus protection on its e-mail servers, it is important for every corporate computer to be individually protected, because viruses can spread by methods other than e-mail (SANS Institute, 2005).

- **Definition updates**

Anti-virus software relies heavily on a component known as a “definition file”. Definition files contain the signatures or “electronic fingerprints” that the anti-virus software uses to identify viruses. Each virus has a unique signature, and without a definition file that contains that signature, the virus cannot be identified.

Since new viruses are released daily, the anti-virus vendors must release new definition files that contain these new signatures just as often. As a user, it is important to update the definition files for anti-virus software daily in order to keep it protected from today's viruses. One good solution is to configure anti-virus software to update its definition files automatically over the Internet. This will poll the vendor's Website and download the latest definition files if they are more recent than what is installed (SANS Institute, 2005).
3.1.3 Availability Topics

Topics in this category directly affect the availability of information, corporate or personal, in one way or another. The following is a detailed discussion of the topics in this category:

♦ **Data backup and storage**

Backup of data or processes is a critical safeguard in any IT security environment ([Du Plessis & Von Solms, 2002](#)), but the major function that backups serve is insurance. If an organization follows a simple set of best practices with respect to backups, it has the protection against mishaps that range from the smallest (accidentally deleted files) to the largest (network operation centre catastrophe).

The following is a discussion of some of the simple actions that can be done with backups:

- **Regular backup schedule**

Creating a schedule of regular backups saves the trouble of rebuilding a system from scratch after it has crashed. Hackers, power surges, hardware failures, and even software upgrades are some of the known things that cause systems to quit functioning. Therefore, backup copies allow an organization to recover from these ‘accidents’.

There are usually two different types of backups. The first is a **full system backup**, in which a backup of the entire disk is created. The second type is an **incremental backup**, in which only the files that have changed or been added since the last backup are archived. A good rule of thumb on an active system is to perform a full backup on Sunday, and then incremental backups each day of the week.
Appendix A: Detailed Discussion of Generic Contents

Laptop or desktop users might perform a full system backup once a month and then perform incremental backups once per week (SANS Institute, 2005). It is important to point out that how often backup of information is performed depends on how much information is created, and how much one is willing to lose if the system crashes.

- **Restore procedures test**

  It is important to test backup procedures occasionally and make sure that the information can actually be restored from the backed up copies. Testing backup procedures also helps to validate that the backups are actually being created. It also familiarizes an individual with how to use the software for recovering a system. Knowing and testing the recovery procedures and software, and validating the backup media help to respond to a crisis rapidly (SANS Institute, 2005).

- **Offsite backup**

  Disasters come in all shapes and sizes. Fires, floods, tornadoes, and even terrorists can destroy computers and the buildings they reside in. It is important to physically separate the backups from the computers, so that they are not damaged together with the computers. Natural disasters can cover wide areas, so it is a good idea to measure the distance of separation in terms of kilometers (SANS Institute, 2005). It is also important to avoid vulnerable storage locations like flood plains, coastal areas, and fault lines. The building itself has to have adequate fire protection and physical security.

  **Possible scenario**

  This example demonstrates why a regular backup schedule can be so important. In this example, two Web-hosting servers were not backed up. A software upgrade resulted in many of the Websites breaking.
Repairing the servers required an excessive amount of effort and time, because there were no backups. If the backups were there, repairing the servers would not have taken so much effort and time. Although the example discusses server class machines, desktop systems are just as important for the timely completion of duties.

**Physical and environmental security**

There is basically a wide array of threats that could exploit unrecognized or inadequately addressed vulnerabilities of the physical environment. These threats include natural disaster threats, e.g., earthquakes, floods, hurricanes, tornadoes, landslides, etc., and unintentional or intentional physical threats, e.g., power outages, equipment failures, fires, proximity of potentially toxic or explosive industrial facilities, local crime, etc. Physical and environmental security plays a vital role in protecting all the resources of an organization, including its people ([Information Systems Security Association, 2004](#)).

**Physical and environmental security fundamentals**

There are a number of factors in the physical environment affecting information security. These factors depend entirely on the diligence of employees to ensure that they do not become a significant impact to security.

The following are some tips to help create a physical work environment that is secure and protects information assets ([Dark, 2000; Thomson & Von Solms, 1998](#)): -

- Be sure to lock the door of the office at the end of the day and when leaving the office for a long time
- Do not leave resources unattended during the workday
- Do not grant unauthorised people access to equipment
- If you are working in an open area, request a security cable for your equipment
Appendix A: Detailed Discussion of Generic Contents

- If you use a laptop, keep it close by at all times
- Do not let others sneak over your shoulders when processing sensitive information or typing passwords
- Do not let outsiders use your computer, unless sure of their identity and authorisation
- Ensure that the computer screen is not positioned in such a way that it is easily readable by someone entering the office or someone outside the window
- Always sign off when leaving the office for a long time. A computer that has not been signed off may have open communications lines, or it may be running a program that requires a password. Signing off stops all such processes, and can also prevent damage from electrical break downs or surges
- Do not put sensitive or confidential printouts in a waste-paper basket. Sensitive and confidential paper documents must be destroyed by putting them through a shredder.

Access to space

Corporate space should be designed with physical security and access control in mind. Processes, like identification badges, should also be put into place in order to help employees recognize who does and does not belong in certain areas. Some of items to be implemented in an organization to aid in controlling access to space include (SANS Institute, 2005): -

- Segment visitor areas from working areas that contain sensitive documents or computers
- Clearly mark areas that are restricted to authorized employees
- Have a corporate identification policy stating employees must wear IDs in plain sight
- Always politely challenge people who do not seem to belong in an area.
**Possible scenario**

This example demonstrates the need for staff to take access control seriously. A medical organization expanded and re-modelled its office space. In the process, temporary and permanent staff was allowed unrestricted access to spaces. To make matters more confusing, the mandatory display of corporate identification was not being followed. This created physical security lapses. An intruder came in one day and sat at one of the computer terminals, apparently trying to solve some sort of system problem. He had access to sensitive medical and billing information of patients. But security personnel caught him later on. This incident could have been avoided if the staff had taken access control seriously. Too often, we make assumptions about strangers who walk into our places of work.

3.1.4 **Other information security topics**

Topics in this category discuss other aspects of information security, e.g., e-mail security, Internet security, social engineering, etc.; therefore, the topics in this category include:

- **Social engineering**

Social engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to gain access to office spaces, accounts, computer systems, networks, or obtain proprietary information without the realization that a security breach is occurring (New York State, 2005). The methods used include lying, fake e-mails, phone calls, and setting up phony Websites (SANS Institute, 2005). Some e-mails entice the recipient into opening an attachment that activates a virus.
Something to keep in mind is never to give out personal information, such as passwords, credit card numbers, social security numbers, or other confidential information, if the person asking for the information is not very well known to you. It is also important to investigate any request for information with an authorized representative from the organization, before providing the information, if there is doubt about the authenticity of a request.

- **Warnings and precautionary measures**

  Some of the common social engineering warning signs include (SANS Institute, 2005): -

  - It is an emergency, and something needs to be changed now
  - Requests for account changes outside of normal work hours
  - “I’m a senior executive, you don’t need to follow policy”
  - We need your password to accomplish “something”
  - “I forgot the system password, what is it?”

  The following are some of the measures to take in order to limit the chances of being a victim of social engineering (New York State, 2005): -

  - No one should ever request your password via e-mail or telephone
  - Before providing information to a telephone caller, check if the individual is authorized to receive that information
  - Employees should report any suspicious calls to the appropriate individual in an organization
  - Before opening an e-mail attachment or clicking on a link, verify it is from someone known, ensure that anti-virus software is current and that the message in the e-mail makes sense. If all the parts do not add up, the attachment may contain a virus; delete it
If you encounter one of the warning signs, do not be afraid to say “No” until you are able to positively identify the requester.

Possible scenario

In the following scenario, an employee received a professional and convincing looking e-mail from his Internet service provider. This e-mail requested information that he was not comfortable providing, and it caused him to take a second look at what turned out to be a social engineering attempt aimed at collecting his bank account information.

♦ Web service (Internet and e-mail) security

One of the greatest security risks in the company is the Internet connectivity and its misuse through uneducated employees. Therefore, it is always a good idea to explain, in detail, the possible dangers of surfing the Internet. It has to be known that no one on the Internet is immune. Those affected include banks, financial and insurance companies, brokerage houses, consultants, government contractors and agencies, hospitals and medical laboratories, network service providers, utility companies, the textile business, universities, and wholesale and retail trades.

The consequences of a break-in cover a broad range of possibilities: a minor loss of time in recovering from the problem, a decrease in productivity, a significant loss of money or staff-hours, a devastating loss of credibility or market opportunity, a business no longer able to compete, legal liability, and the loss of life (Software Engineering Institute, 1997).

♦ Internet security best practices

Some of the well-known best practices for Internet use include (Danchev, 2003; SANS Institute, 2005): -
Appendix A: Detailed Discussion of Generic Contents

- Do not visit inappropriate Websites with objectionable content; pornography, gambling, pirated software, hacker/hacking sites, as well as those generally considered as prohibited by an organization’s security policy
- Downloading software, files or anything else is prohibited. If you need any applications for your day-to-day business, contact either the IT department, or the Help Desk. If you do get clearance to download a piece of software, remember never to execute it before scanning it with the corporate anti-virus/anti-Trojan software
- All Internet activity should continuously be monitored, and users should be aware that they could be held liable for visiting prohibited Websites, downloading illegal files and content, as well as facing the penalty of having their access to the Internet limited (until they can prove that they are fully aware of the risks created by their actions).

**E-mail security best practices**

The following are some of the well-known best practices for e-mail use (Danchev, 2003; SANS Institute, 2005): -

- If e-mail attachments are allowed, the attachment(s) must be scanned before opening as well as confirming with the sender (i.e., via phone) that indeed an attachment has been sent. This will also reduce the risk of running a program that has been e-mailed out automatically (unknown to the originator), via some kind of malicious application, that has made use of the mail account(s) and/or mailing system of the sender. If attachments are forbidden, follow the policy and do not download/run any file(s) received as attachments
Appendix A: Detailed Discussion of Generic Contents

- Do not use an organization’s e-mail accounts for registration purposes of any kind, and do not use it while posting messages in Web forums or newsgroups. You may want to create one, special (possibly aliased) account for this purpose only.

- Do not use an organization’s e-mail system for running your own business, excessive personal mailing, sending large attachments, thus wasting valuable bandwidth.

- Do not respond to chain letters, or any other sort of spam using an organization’s e-mail systems; if in doubt, contact the ISO office.

- Never forward any organization information to external e-mail accounts (i.e., send a work document to your home e-mail account, so to work on it further from home that evening), without first checking with your manager.

- The proper use of the e-mail system should continuously be monitored, and the users should be aware that they could be held liable for illegal activities, such as spamming, sending and receiving illegal content, etc.

- E-mail is not private. Only communicate in e-mail what you would be comfortable communicating to a crowd of people. Use encryption to secure messages that need to be private.

Possible scenario

This example demonstrates the need to be careful with unsolicited e-mail. One of the employee’s friends conducted a small experiment. She got unsolicited e-mail with the usual message “If you don’t want to receive future e-mail from us, use the REPLY button and place the word CANCEL in the subject header.” Her friend created a new e-mail account, and used it to reply to the unsolicited commercial e-mail.
That e-mail was almost immediately flooded with a large number of unsolicited commercial e-mails, not just from the first offender, but from others as well. So it appears that this REPLY was just another scam to collect addresses with which to clog the Net (Dark, 2000).

♦  Mobile worker security

Computers, nowadays, are accessible via a variety of mobile equipment, such as laptops, PDAs and even cell phones. A person can even download information from the Internet to a cell phone. While convenient and fun to use, some good practices help protect the information contained in this equipment. These devices carry vital information that must be protected. These equipments are more easily stolen or misplaced because of their size.

♦  Precautionary measures

If a laptop is used, remember the following (New York State, 2005):

- Secure it with a cable lock or store it in a locked area or locked drawer
- Backup information
- Keep it with you during air and vehicle travel, until it can be locked up safely. Do not forget to retrieve it after passing through airport security.

Treat all portable devices in the same careful manner as a laptop and keep an eye on them.

Possible scenario

This example demonstrates the need to take precautionary measures with portable equipment when working remotely. The personal portable computer of a CEO of a certain organization disappeared from a hotel conference room moments after addressing a national business journalists’ meeting.
The laptop contained proprietary information that could be valuable to foreign governments. The CEO left the computer unattended on a podium for about 15 to 20 minutes, when he stepped down to talk to a small group of business editors and writers less than 30 feet away (Dark, 2000).

♦ **Wireless security**

Wireless networks and laptops are very popular for their ease of use and portability. The Internet can be reached via radio waves without having to plug a machine into a network. It is with the same ease of connecting that malicious individuals connect to unprotected networks. Therefore, extra measures are needed to ensure the safety of the wireless equipment. It helps if an organization has a policy regarding use of wireless devices (New York State, 2005). It is also very important to consult the equipment’s manual for specific details.

♦ **Remote access**

Remote access allows users to access data from outside locations using dial-up equipment and public telephone lines or cellular/wireless phones on the Internet. Because this form of access is designed for off-site use that may extend after normal business hours, extra measures are required to prevent unauthorized access (New York State, 2005):

- Keep dial-up numbers confidential
- Do not check the “Save Password” box. Instead, type the password each time you log on. Laptop theft is common. Checking that box gives the thief not only the laptop but also access to an organization’s computer systems. Even if they do not do any damage to an organization’s computer system, they can use it to hack into other organizations and make it look like one of the employees in your organization did it.
Computer ethics

The use of information technology in an organization can be regulated with the introduction of many rules and regulations. The use to which IT can be put is very widespread, and the correct usage of this very powerful resource will, in many cases, rest on the good judgement and ethics of that particular user (Thomson & Von Solms, 1998). Computer ethics form a basis for deciding what is right and wrong when making decisions (Du Plessis & Von Solms, 2002).

Appropriate use of IT corporate resources

The following are examples of some appropriate uses of IT ethics in an organization (University of Toronto, 1995; Thomson & Von Solms, 1998):

- Respect for the rights of others
- Respect for the property of others
- Consideration of other persons using shared systems, equipment, and facilities
- Confidentiality in use of passwords and personal identification numbers
- A presumption of the right to privacy
- Use of tools for the purpose for which they were intended
- Adherence to etiquette and culture as defined in systems that are used
- Using tools for the intended purpose
- Adherence to company-defined etiquette
- Respect to the organization’s rights and property.
Inappropriate use of IT corporate resources

Inappropriate use of information technology includes (University of Toronto, 1995; Thomson & Von Solms, 1998): -

- Unauthorized access, alteration, destruction, removal and/or disclosure of data, information, equipment, software, or systems
- Deliberate over-extension of the resources of a system, or interference with the processing of a system
- Disclosure of confidential information, e.g., passwords, personal identification numbers, etc
- Propagation of pornographic materials
- Use of organization’s facilities and resources for personal gain
- Propagation of hate literature and harassment
- Unauthorised copying of software
- Harassment, including sexual harassment
- Theft of resources

Possible scenario

The scenario demonstrates the need to observe the privacy of others. Organization XYZ hired somebody to implement and manage its logical access control policy. He found that many usernames and passwords belonging to terminated employees were still active, though their owners were gone, some for several years. He also found that one of these username/password combinations had been used subsequent to the owner’s departure. Files accessed included confidential personnel and payroll records of a key executive. Though no one had noticed, the executive’s files had been altered to imply that a medical condition had become a significant risk. This fabricated medical problem could have affected the executive’s career upon his next review, given the high stress nature of his job.
Assuming that the departed party had violated the company’s privacy policy, he wrote a letter to the executive accusing the former employee of a breach of privacy. An investigation ensued, the police were consulted, and the individual accused was interrogated aggressively.

3.2 Programme 2: For relevant IT management

This sub-section discusses the elective modules identified for relevant IT management in a generic environment as well.

3.2.1 Availability topics

As stated previously, topics in this category directly affect the availability of information, corporate or personal, in one way or another. These topics, this time, are only intended for relevant IT management.

♦ Incident management

A computer security incident can be defined as anomalous activity on a computer. Viral infections, evidence of intrusion, odd network activity, unauthorized physical access, or misuse of resources, are basically some of security problems that can constitute an incident. Management should know that incident response is a critical part of overall corporate security. When an incident occurs, every individual responsible should be involved: the user, the administrator, management, the response team, and sometimes, law enforcement (SANS Institute, 2005).

▪ Incident response plans

Management must ensure that an organization’s incident response plans should be included in its policy. Corporate incident response plans outline what should be done in times of incidents.
As such, they help to minimize and limit damage, because employees know what to do. The plans should define explicitly (SANS Institute 2005): -

- What must be done in various situations
- Who to call immediately if there is an accident
- Who is responsible for handling problems
- What to do or not do if you find an intruder on a computer.

The following are some points to keep in mind in preparing for the unexpected: -

- Post an incident call list in an obvious place
- No attempt has to be made by employees to handle the incidents by themselves. Reporting the incidents using the call list is a good procedure
- If you suspect that a computer has been hacked, do not touch the keyboard or turn off the computer.

**Possible scenario**

This example demonstrates the need for an organization to have an incident response plan. A customer's computer at a managed security provider was hacked. It had to be taken offline to fix, but there was no incident response plan in place. As a result, the decision about what to do about it was a very difficult one, resulting in a delay in recovery. When time is of the essence, it is important to have all the “tough calls” already made and approved by management (SANS Institute, 2005).

♦ **Contingency planning**

Organizational entities depend on their IT resource infrastructure now, more than at any previous time in history, to deliver mission-critical information in a timely fashion.
The operational importance of information assets, whether based on cost or time factors, is such that organizations can ill afford to endure the consequences of significantly disruptive events impacting on supporting information technology resources or the information assets directly (Information Systems Security Association, 2004). Therefore, the key role for managers is strategic planning to ensure the continuous information systems’ availability when a successful attack occurs.

Management should plan for and operate information technology in such a way as to preserve the continuity of organizational operations. The most effective way of doing this is through a business continuity plan (BCP). A BCP is a guiding document which allows an organization to continue operations when disasters occur (Thomson & Von Solms, 1998), such as floods, earthquakes, power outages, computer viruses, etc.

- **Contingency planning process**

Because of the integrated natures of incident responses, disaster recovery and business continuity plans, management should realize that an overall contingency planning process addresses areas within each. There are six steps in the consolidated contingency planning process (Whitman & Mattord, 2003):

1. **Identifying the mission or business-critical function**: Each organization must identify those areas of operation that must continue in a disaster to enable an organization to operate. Those must be prioritized, from most critical to least critical, to allow optimal allocation of resources, e.g., time, money, and personnel, in the event of a disaster.

2. **Identifying the resources that support the critical functions**: For each function, an organization must identify the resources required by that function to be successful.
These resources can include people, computing capability, applications, information, services, physical infrastructure, and documentation

3. **Anticipating potential contingencies or disasters:** Organizations brainstorm potential disasters and determine what functions they would affect.

4. **Selecting contingency planning strategies:** Organizations identify methods of dealing with each anticipated scenario and outline a plan to prepare for and react to the disaster. Armed with this information, the actual consolidated plan begins to take shape. For each incident scenario, three sets of procedures are created:
   - The group develops and documents the procedures that must be performed during the incident. These procedures are grouped and assigned to individuals. The planning committee begins to draft a set of these function-specific procedures.
   - Once the procedures for handling an incident have been drafted, the second set of procedures is developed, which are those that must be performed immediately after the incident has ceased. Again, separate functional areas may be assigned different procedures.
   - The group drafts a third set of procedures, which are those tasks that must be performed to prepare for the incident. These are the details of the information backup schedule, the disaster recovery preparation, training schedules, testing plans, copies of service agreements, and business continuity plans if any.

5. **Implementing the contingency strategies:** At this stage, an organization signs contracts, acquires services, and implements backup programs that integrate the new strategy into an organization’s routine operations.
6. Testing and revising the strategies.

Possible scenario

A risk assessment performed at XYZ organization showed that the ground floor Central Computing Services Complex (CCSC) was well isolated from most major disruptive agents, except for flooding. The systems security officer mentioned that weather statistics showed that each year the tropical storm count increased, as had the attendant rainfall amounts, with the result that larger amount of water pooled for longer periods in places where they had not 15 years earlier. It was generally recognized that a flood would damage, or destroy, the IT facilities on the first floor. Historically, flood cleanup had required four to six weeks in this area. Also, a service outage of greater than 14 days would render XYZ organization financially insolvent. Therefore, the officer recommended that XYZ's flood insurance must be reviewed to ensure that it was commensurate with asset values and corporate requirements as they currently stood. He further recommended that management consider relocating the CCSC to a higher floor in the building, or away from the current building, where the threat of flooding could be reduced or eliminated. When questioned concerning the cost of these and other measures, the officer stated that the most costly recommendation was more than 2000 times less than the estimated cost to clean up the facility and replace all damaged equipment in the event of total loss. He further stated that an appropriate increase in flood insurance would add less than 0.5% to the insurance expense line of the corporate operational budget (Information Systems Security Association, 2004).

3.2.2 Security management topics

Topics in this category concern the management of information security by management of an organization. Topics discussed in this category are solely addressed to management only. The topics include:
Information security policies, standards and best practices

In a broad sense, information security policies are management directives that establish the business goals, security framework, responsibilities, and governance (Hunter, 2000). As building a good security policy provides the foundations for the successful implementation of security-related projects in the future, this is, without a doubt, the first measure that must be taken to reduce the risk of unacceptable use of any of the company's information resources. The policy will describe in detail the meaning of acceptable use, as well as listing prohibited activities (Danchev, 2003). Therefore, management must ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security (Information Systems Security Association, 2004). Management must also make sure that all staff are educated and trained in these policies.

Policy development

There is considerable information available to assist in the development of security policy. As a minimum, the policy should (Hunter, 2000): -

- Emphasize the value and dependence on information, and the importance of information security to the organization
- Identify the goals and principles of effective information security
- Identify minimum security regulations and compliance requirements. This includes elements, such as risk management policy, classification and labelling of information, personnel and physical security, legal and contractual requirements, system development and operation, business continuity planning, incident reporting and response requirements, violation enforcement, and security awareness and education
- Define roles, responsibilities, and accountabilities
Appendix A: Detailed Discussion of Generic Contents

- Contain any critical information system or issue-specific requirements
- Have a statement of management’s intention
- Have an explanation of the process for reporting security incidents.

**Policy management**

Whitman and Mattord (2003) state that policies are living documents that must be managed and nurtured, as they constantly change and grow. To remain viable, these policies must have (Whitman & Mattord, 2003):

- An individual responsible for the creation, revision, distribution and storage of the policy
- A schedule of review
- Review procedures and practices
- Date of origin, along with the date(s), if any, of revisions.

**Standards and best practices**

Standards and best practices are the most direct and efficient means of achieving a standard of due care (Hunter, 2000). In general, they advocate good security principles in information security. As such, management must make an effort to familiarise itself with standards and best practices acceptable at national or international level. This will help in following security standards and best practices that are acceptable nationally or internationally. Two such standards accepted on an international level are ISO/IEC 17799 and ISO/IEC 13335. ISO/IEC 17799 is used as a reference for implementing and maintaining information security within an organization, since it provides a set of security controls, which has been compiled using the best security practices in the United Kingdom and internationally (Thomson & Von Solms, 1998). ISO/IEC 13335 lays down internationally accepted guidelines in the field of information security management.
**Possible scenario**

This example demonstrates the need for organization to have an information security policy in place. During routine system maintenance, an employee, who was unhappy with his manager and XYZ organization, realized there was no prohibition on Trojan Horses or other similarly malicious activity. Thus, he built a Trojan Horse into a modification of the accounts receivable application system that he routinely maintained. He then submitted his resignation and left the company. Six months later, the Trojan Horse, a logic bomb, began to systematically corrupt files on the birthday of his former manager. Within a few weeks, the file was severely contaminated, as were all backup files. The result was a sustained inability to generate invoices and receive related accounts. XYZ’s ability to prosecute him was thwarted by the complete lack of policy articulating management and ownership perception of the value of the information assets. He was, thus, successful in his vengeful attack at great cost and embarrassment to XYZ organization (Information Systems Security Association, 2004).

♦ **Information risk management**

Management needs to manage threats to information in the same way as one would manage risk to personal belongings. Management should ensure that information security measures are appropriate to the value of the assets and the threats to which they are vulnerable. In order to choose effective and efficient measures, management must identify the assets to be protected, the threats to the assets, and the vulnerability of the assets or their environment to the threats (Information Systems Security Association, 2004).

▪ **Risk management process**

The risk management process includes three components of risk equation: asset, threat, and vulnerability.
The goal is to reduce risk by reducing some component of the risk equation. For example, controls that eliminate system vulnerability or prevent a threat will reduce the level of risk.

Risk assessment is a process of choosing controls based on probabilities of loss and the impact of the loss. The following questions form the foundation for determining the level of risk associated with potential threats (Hunter, 2000): -

- Threat Events-What could go wrong?
- Frequency-How often could it happen?
- Impact-What are the consequences?
- Confidence/Uncertainty-How certain are the answers to the first three questions?

Once this is complete, answers to the following questions will help make informed decisions about whether to accept, avoid, or transfer risks: -

- What can be done about unacceptable risks?
- How much will it cost?
- Are selected safeguards effective?
- What is the residual risk?

**General risk management cycle**

Security management should follow a risk management cycle, such as the one below. This model is based on common risk management principles applied by leading organizations. These five principles described by the model are (Hunter, 2000): -

- Determine needs based on an assessment of information security risks in terms of the impact on business operations
- Establish a central management focal point to ensure that weaknesses in one organizational unit do not place the entire organization’s information assets at risk
- Implement appropriate policies and related controls
Appendix A: Detailed Discussion of Generic Contents

- Promote awareness to continually educate both users and managers on risks and related policies
- Monitor and evaluate the effectiveness of policies and controls.

General Risk Management Model

Information asset management

Management should routinely catalogue and value information assets, and assign levels of sensitivity and criticality. Information, as an asset, must be uniquely identified and responsibility for it assigned. In order to manage information assets efficiently, management must know what to protect. In order to be effectively managed, it is essential to identify and enumerate the core attributes of information as assets. These information asset attributes include (Information Systems Security Association, 2004):

- Identity
- Ownership
- Custody
- Content
Value (ideally expressed in monetary terms) of the confidentiality, availability, and integrity of the information assets.

Appendix A: Detailed Discussion of Generic Contents

- **Sensitivity** (which relates directly to confidentiality)
- **Criticality** (which relates directly to availability and integrity).

It is important to keep in mind that most information attributes change value over time, in some cases increasing and in others, decreasing, and as such, these attributes should be reviewed regularly.

Some of the security issues that surround inventory and asset control will be discussed.

- **Disposal of media**

Most organizations only concern themselves with keeping track of what is on the various computing devices that are allocated and in use. Few organizations pay attention to information that may be left on equipment when that equipment has been replaced. It is necessary to purge all sensitive information from information storage devices before disposal. These include removable computer media, such as tapes and disks and printed reports.

A note has to be taken that simply deleting files does not actually erase information from a disk; it is always there and can be retrieved quite easily. Therefore, the sanitization of electronic media on all computing devices should be one of the last steps of asset control and management (SANS Institute, 2005). The following are some of the tips to bear in mind during media sanitization:

- Deleting files or formatting disks does not actually erase the data, it can still be retrieved
- Before disposing of equipment it should be securely “wiped”
- Workstations, laptops, PDAs, and cell phones should be wiped
Asset control should include the sanitization of all media associated with old electronic equipment.

Appendix A: Detailed Discussion of Generic Contents

- **Asset theft**

  The proper management of corporate assets helps to keep honest people honest. Organizations that track information asset resources are in a much better position when it comes to being able to identify losses due to theft. Some of the information asset controls to prevent theft include (SANS Institute, 2005):

  - Implement random bag checks of personnel entering or leaving the building
  - Ensure proper asset controls are in place in areas like the repair department.

  **Possible scenario**

  The following example demonstrates the need for a proper asset control in an organization. A dishonest employee, working without proper supervision, took advantage that there was no proper asset control and began stealing computer equipment. He began bragging to another employee about the incredible perks of working in the computer-repair department. Without the proper asset controls in place, the colleague was able to steal a network, one piece at a time (SANS Institute, 2005).

- **Accountability and responsibility**

  Accountability characterizes the ability to audit the actions of all parties and processes that interact with information. Therefore, management must make sure that information security accountability and responsibility are clearly defined and acknowledged. This helps to clearly define, identify, and authorize roles and responsibilities at a level commensurate with the sensitivity and
criticality of information. All parties must have responsibilities for which they are held accountable (Information Systems Security Association, 2004).

Appendix A: Detailed Discussion of Generic Contents

- **Holding employees accountable**

Management should hold all parties accountable for their access to and use of information, e.g., additions, modifications, copying and deletions, and supporting IT resources. One way of doing it is to affix the date, time, and responsibility, to the level of an individual for all significant events.

In order to assure that employees behave as expected, it is necessary to know who did what, and when it was done. Therefore, it is essential that organizations establish and maintain a basis of control for information assets. Such a control framework requires individual and organizational accountability at all levels. Holding all parties accountable is intended to assure that any use made of, or actions taken on, information assets and supporting IT resources should be for authorized business/mission purposes only, and that such use or action can be reliably traced to the responsible party or parties, who will be held accountable (Information Systems Security Association, 2004).

**Possible scenario**

When reviewing the daily access audit report, the Information Security Officer (ISO) of organization XYZ, found several invalid payroll file access attempts by an employee who works in the graphics arts department. When the ISO spoke with the employee and his manager, it was determined that the employee was planning to ask for a raise, and his invalid accesses resulted from his attempting to learn what others in his department were being paid. The employee stated that, armed with such information, he would have an idea of what an acceptable pay increase might be. He would, thus, have an
advantage in the raise negotiations. The ISO turned the matter over to the employee’s manager for disciplinary action.

Appendix A: Detailed Discussion of Generic Contents

The ISO managed to trace the employee’s attempts because information assets were controlled and monitored with an accompanying audit log to report any modification, addition, or deletion to the information assets (SANS Institute, 2005).

♦ Legal, regulatory and contractual requirements issues

Information security is regulated by some laws and regulations, and understanding this legal environment are ways of controlling an organization’s liability for privacy and security risks. Management should take steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets (Information Systems Security Association, 2004).

▪ Copyright

Copyright laws are different for different countries, but most countries have laws that prevent original works from being reproduced, hired or adapted (Du Plessis & Von Solms, 2002). Although there are no “international copyrights” to protect information, most countries are members of the Berne Convention and the Universal Copyright Convention (UCC), which allow for the international protection of copyrighted material (Whatiscopyright.org, 1998; Du Plessis & Von Solms, 2002).

Top management needs to know the consequences of making an illegal copy of a software package. If illegal software is found on an organization’s computer equipment, it is the chief executive officer of the organization who is held responsible (Thomson & Von Solms, 1998). The organization, therefore,
could be held liable for expensive legal fees, fines, and negative publicity, all of which could be detrimental to the organization.

Appendix A: Detailed Discussion of Generic Contents

- **Software licensing and piracy**

Management should know all types of piracy to be able to handle the software licensing and piracy issues properly. The following are the various types of piracy (Microsoft Corporation, 2005):

- **End-User Piracy**: Users copy software without appropriate licensing for each copy. This includes both casual copying and distribution between individuals, and organizations that do not strictly monitor the number of software licenses they install and do not acquire enough licenses to cover their software installations.

- **Pre-Installed Software**: A computer manufacturer takes one copy of software and illegally installs it on more than one computer. Consumers should be on the lookout for proper license documentation, when purchasing a new computer, to ensure they are getting what they paid for.

- **Internet Piracy**: Unauthorized copies are downloaded over the Internet. If downloads are made available on the Internet, make sure that the publisher has authorized this distribution.

- **Counterfeiting**: Illegal copies of software are made and distributed in packaging that reproduces the manufacturer's packaging. Counterfeit registration cards with unauthorized serial numbers are often included in these packages.

- **Online Auction Piracy**: This takes several forms, such as software resold in violation of the original terms of sale, NFR (Not For Resale), or software that has not been authorized for resale by a third party, online distributors offering special deals with the software publisher, liquidated inventories, or...
acquisition through bankruptcy sales. These types of phrases are used to fool consumers into believing that they are getting genuine products that would not otherwise be discounted.

Appendix A: Detailed Discussion of Generic Contents

Some of the risks associated with using pirated software are (Microsoft Corporation, 2005): -

- **Quality** - It often lacks key elements and documentation, and comes with no warranty protection or upgrade options
- **Viruses** - Untested, counterfeit discs may be infected with viruses that will damage hard drive or cripple network, without the benefit of technical support
- **At Work** - copying or using illegally copied software at work puts an entire organization at risk for copyright infringement. Pirated software that is either dysfunctional or that contains viruses wastes company resources and drives up IT costs.

---

**Privacy issues**

Many countries have privacy laws that protect the privacy of individuals or organizations. Management should be aware that being in possession of information does not mean that that information can be used in an unlimited fashion. Information can often only be used for the specific purposes for which it was obtained. Using information for any other purposes could be violating the individual or organization’s privacy (Du Plessis & Von Solms, 2002) and can evoke legal action.

The US Government Privacy Act is an example of a law that protects the privacy of information. This Act requires the US government to safeguard personal data processed by federal agency computer systems. It also requires it to provide ways for individuals to find out what personal information is being recorded and to correct inaccurate factual information (National Institute of Standards Technology, 1998).
Change management

This focuses on IT operational change management, beginning when upgrades or updates to information assets, i.e., infrastructure or applications, are identified for movement to production and ending when such assets are retired from the production environment. This includes application maintenance and emergency change controls (Taylor, Allen, Hyatt & Kim, 2005).

Change management is sometimes difficult for organizations to master, because so many stakeholders are involved (e.g., business managers, application system developers, IT operations staff, and auditors). Stable and managed production environments require that implementation of changes be predictable and repeatable, following a controlled process that is defined, monitored, and enforced (Taylor, Allen, Hyatt & Kim, 2005).

Change management process

Management has to know and be familiar with the change management process to increase chances of change success. It typically includes the following activities (Taylor, Allen, Hyatt & Kim, 2005): -

- Identify the need for the change
- Prepare for the change
  - Document in detail the change request
  - Document the change test plan
  - Document a change rollback plan, in case of change failure
  - Write a step-by-step procedure that incorporates the change, the test plan, and the rollback plan
Submit the change procedure in the form of a change request

Develop the business justification and obtain approvals

Appendix A: Detailed Discussion of Generic Contents

Assess the impact, cost, and benefits associated with the change request

Review and assess the risks and impacts of the change request, including regulatory impacts

Authorize the change request

Authorize, reject, or request additional information on the change request

Prioritize the change request with respect to others that are pending

Schedule, coordinate, and implement the change

Schedule and assign a change implementer

Schedule and assign a change tester

Test the change in a pre-production environment

Communicate the change to stakeholders likely to be affected

Approve the change for implementation

Implement the change as requested

Verify and review the implemented change (a critical step that is most often overlooked)

Was the change successful?

Was the change process followed?

What was the variance between the planned and implemented change?

Were internal control, operations, and regulatory compliance requirements maintained?

What were the lessons learned that can be use to improve the process?
Close the change request and communicate with the affected parties
Make agreed-to changes to the change management process

Appendix A: Detailed Discussion of Generic Contents

Introduction of, or changes to, outsourcing, in sourcing, and other supplier and partner relationships
Maturity of department’s processes, particularly the introduction of quality management and structured development or operations processes
New or different security threats, vulnerability or impacts.

♦ Computer auditing

Computer auditing is a branch of general auditing concerned with governance, i.e., control of information and communications technologies. It concerns primarily the study of computer systems and networks from the point of view of examining the effectiveness of their technical and procedural controls to minimize risks (IsecT Ltd, 2006). All audits are performed in relation to certain risks identified by the auditor, which he/she believes are important.

 Conducting audit

It has to be known that computer auditing is done in different ways, and individual auditors have their own favourite ways of working. But, it is important to understand the main stages of a typical computer audit assignment, which includes the following (IsecT Ltd, 2006):

1. Scoping and pre-audit survey - auditors determine the main areas of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment. Information sources at this stage include background reading
and Web browsing, previous audit reports and, sometimes, subjective impressions that deserve further investigation.

Appendix A: Detailed Discussion of Generic Contents

2. **Planning and preparation** - during which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control matrix.

3. **Fieldwork** - gathering evidence by interviewing staff and managers, reviewing documents, printouts and information, observing processes, etc.

4. **Analysis** - this step involves sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques may come in handy.

5. **Reporting** – it involves reviewing the analysis and trying to make sense out of it, and then writing a report up, circulating or presenting it to clients and client managers to have their say, and finally issuing it.

6. **Closure** - closure involves preparing notes for future audits and chasing-up management to complete the actions they promised months earlier.

4. **Conclusion**

Different aspects thought to be vital and necessary under each topic were discussed to bring out the elements that information users should be aware of. Throughout the discussion, many sacrifices in the scope of the material covered have had to be made. In every aspect, an effort was made to present the awareness material in a simple and straightforward manner. This was so because the audiences to be reached by the
generic programme have, more than likely, very little, if any, knowledge of information security, because they come from different disciplines. As such, they are not information security experts who can understand very technical information.

Appendix A: Detailed Discussion of Generic Contents

What the entire generic programme tries to do is to provide a baseline of awareness by educating the employees on the essentials of information security. Having such a baseline in place can provide organizations with the assurance that some basic level of awareness exists among employees. Such a baseline effort could be compared to the ISO/IEC 17799 best practices for information security management (Du Plessis & Von Solms, 2002). This standard suggests choosing controls from a set that was identified to work for most organizations through experience, instead of going through a company-specific approach to identifying what exactly each company requires (Von Solms, 2000; Du Plessis & Von Solms, 2002).
Appendix B

Questionnaire

This questionnaire was administered to some South African companies known to follow sound information security principles with the aim of soliciting topics as part of the contents for generic information security awareness programme.
Research Title: Information Security Awareness: Generic Content, Tools and Techniques

Researcher: Hope Mauwa, MTech student in Information Technology, Nelson Mandela Metropolitan University (NMMU)

Supervisor: Prof. Rossouw Von Solms, Information Technology, Head of Department at NMMU North Campus

To Whom It May Concern

This study is based on research to identify what general topics can be included as part of the contents for an information security awareness programme intended to be offered to internationally, interdisciplinary, distributed audiences, and to specifically find out the most effective techniques for delivering such a generic content.

The questionnaire is designed to solicit topics from you, which you think should be included as the contents for the generic information security awareness programme.

The objectives of information security awareness programmes, based on literature researched reads as follows:
Security awareness efforts are designed to change behaviour or reinforce good security practices of all information users. They provide a baseline of security knowledge for all users, regardless of job duties or positions. Security awareness is a learning process that changes individual and organizational attitudes and perceptions to realize the importance of security and the adverse consequences of its failure.

Appendix B: Questionnaire

If you have any questions during the completion of the questionnaire, please contact me on the following email address, hoprab@yahoo.com

Date completed: ............................................... (To be completed by participant)

<table>
<thead>
<tr>
<th>SECTION A: USE OF BUSINESS INFORMATION IN YOUR ORGANIZATION</th>
</tr>
</thead>
</table>

Definition: Business Information

A.1 How important is the **business information** of your organization for the daily operations of the organization? (1 = not important, 5 = very important)

A.2 How important is the information and communication technology **infrastructure** of your organization to the daily business operation of the organization? (1 = not important, 5 = very important)

A.3 To what extent are you affected in your work when the business information and ICT systems are not accessible for the whole day, i.e., **availability of business information is compromised**?

   1 Seriously affected
   2 Moderately affected
   3 Lightly affected
   4 Not affected
   5 Don’t know

A.4 If the business information of your organization is exposed to unauthorised individuals or systems, i.e., **confidentiality of business information is compromised**, to what extent is the organization affected?
Appendix B: Questionnaire

A.5 To what extent is your organization affected when the integrity of business information is compromised, e.g., when business information is changed?

1. Seriously affected
2. Moderately affected
3. Lightly affected
4. Not affected
5. Don’t know

SECTION B: INFORMATION SECURITY AWARENESS: CONTENT, TOOLS AND TECHNIQUES

Please mark an “X” in the appropriate box or, where indicated, provide a written response.

B.1 Does your organization have a Corporate/Organization Information Security Policy?

1. Yes
2. No
3. Don’t know

B.2 Are there security procedures or guidelines in your organization, e.g., guidelines for creating a ‘good’ password, available to all employees using organizational information resources?

1. Yes
2. No
3. Don’t know

B.3 Do you think information security awareness programmes intended to train employees in (Formating gone nuts) good security practices are important?

1. Yes
2. No
3. Don’t know

B.4 Have you ever attended any information security awareness training programme?

1. Yes
2. No

B.5 If your response to B.4 is yes, how long ago was that?

1. 1 – 3 months ago
2. 4 – 6 months ago
3. 7 – 9 months ago
4. 10 – 12 months ago
5. More than 12 months ago
B.6 What is your recommendation regarding the frequency at which the information security awareness training should be offered to the employees? Choose only one option.

1. More than 3 years
2. Once every 3 years
3. Once every 2 years
4. Once in a year
5. Twice in a year

Appendix B: Questionnaire

B.7 Which of the following topics would you recommend to be part of the contents of the security awareness programme to be taught to everybody in the organization regardless of job position? (Mark with an ‘X’ in the appropriate box)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Recommend</th>
<th>Not recommend</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data backup and Storage (Saving files on diskettes/CD/ remote computer on the network)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Engineering (Using social skills to convince people to reveal valuable information)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile/Remote Worker Security (Security issues when working out of the traditional office environment)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious Code (Viruses, worms, Trojans, key loggers, adware/spyware etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Security (Guidelines for password creation, use, and management)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet/Web Browser Security (Information security issues linked with browsing the Web)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Security (Security relating to the receipt and sending of electronic mail)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Security (Security of telephone network systems from such things as hacking)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Security (Security issues relating to use of wireless technology, such as Bluetooth)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical and Environmental Security (Protecting the facilities against unauthorized access, fires, floods, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Ethics (Accepted behaviours in information security)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacking/IT-Related Fraud (Gain access to computer systems and information illegally by bypassing controls)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topic</td>
<td>Recommend</td>
<td>Not recommend</td>
<td>Don't know</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td>Privacy and Confidentiality (Keeping sensitive corporate and personal information secret)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photocopy Security (Security of company documents in relation to photocopying)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper-copy Document Security () something missing??</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountability and Responsibility (Issues relating to holding employees accountable and responsible for their actions)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copyright, Piracy and intellectual property (Issues relating to software licensing and protection of intellectual property)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-virus Software and Firewalls (Anti-virus software helps to prevent computers from being infected with viruses. Firewalls, combination of hardware and software that limits crackers from computer and network systems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security Policies, Standards and Procedures (Written plan of action that influences and determines decisions in an organization. Standards, procedures and guidelines explain how employees comply with policy)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If there are other topics that have not been listed above, but you wish that they should be included, please list them below: -

1. ........................................................................................................................................
2. ........................................................................................................................................
3. ........................................................................................................................................
4. ........................................................................................................................................
5. ........................................................................................................................................

B.8 Would you recommend the awareness of technical details of some of the topics recommended in B.7 above to every employee in the organizations, e.g., configuration of and updating of anti-virus software?

1. Yes [ ]
2. No [ ]
3. Not sure [ ]

If you are not holding a managerial position or a technical position, do not answer B.9 below.

B.9 Which of the following topics would you recommend to be part of the elective contents of the security awareness program to be taught to only employees holding managerial and technical positions? (Mark with an ‘X’ in the appropriate box)
<table>
<thead>
<tr>
<th>Topic</th>
<th>Recommend</th>
<th>Not recommend</th>
<th>Don't know</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Information Security Risk Management (Cyclical process for analyzing and managing risks)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Contingency Planning (Planning for success by preparing to cope with the worst)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Incident Management (Reacting to, containing, resolving and learning from information security incidents)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 IT laws, Regulations and Standards (These define obligations and best practice for IT and information security e.g. ISO 17799)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Computer Auditing (Assessing IT business controls against risks, compliance and assurance)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Information Asset Management (Accountability and responsibility for information assets)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 IT Governance (Structural and procedural controls relating to the management and control of IT, including supervision and oversight)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 Change Management (Security aspects of IT-related changes, e.g., patching, testing and configuration management, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If there are **other topics** that have not been listed above, but you wish that they should be included, please list them below:

1. ........................................................................................................................................
2. ........................................................................................................................................
3. ........................................................................................................................................
4. ........................................................................................................................................
5. ........................................................................................................................................

B.10 Would you prefer to take an examination after completing studying the topic-materials?

1. Yes
2. No
3. Don’t know

B.11 What is your opinion on offering of the Information Security Awareness Certificate?

1. Should be offered after completing studying the topics-materials and successfully passing the examination
2. Should be offered after completing studying the topics-materials
Appendix B: Questionnaire

B.12 If you recommended that a **certificate should be offered** in B.11 above, how long should the certificate be valid?

1. For 3 years
2. For 2 years
3. For 1 year
4. For 6 months
5. For 4 months

B.13 Which of the following would you regard as effective mechanisms for delivering the security awareness topics chosen in B.7 and B.9 to employees? Please mark with an “X” in the appropriate box. You can select more than one option.

1. Newsletters
2. Posters
3. Handouts/leaflets/pamphlets
4. Screen savers
5. Computer-based training
6. In-person instructor-led training

Thank you for completing the questionnaire
Survey Analysis

This is the analysis of the survey conducted with some South African Companies known to follow sound information security principles with the aim of soliciting topics for the generic information security awareness programme.
**Survey Analysis**

**IMPORTANCE OF BUSINESS INFORMATION**

<table>
<thead>
<tr>
<th>Importance</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unimportant</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Slightly unimportant</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Neutral</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Important</td>
<td>5</td>
<td>38.5</td>
</tr>
<tr>
<td>Extremely important</td>
<td>8</td>
<td>61.5</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Figure C.1 (refer Question A.1 in Appendix B)
### Importance of ICT Infrastructure

<table>
<thead>
<tr>
<th>Importance</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unimportant</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Slightly unimportant</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Neutral</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Important</td>
<td>4</td>
<td>30.8</td>
</tr>
<tr>
<td>Extremely important</td>
<td>9</td>
<td>69.2</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

**Figure C.2** (refer Question A.2 in Appendix B)
Appendix C: Survey Analysis

### EFFECTS OF AVAILABILITY COMPROMISE

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>4</td>
<td>30.8</td>
</tr>
<tr>
<td>9</td>
<td>69.2</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
</tr>
</tbody>
</table>

Figure C.3 (refer Question A.3 in Appendix B)
### EFFECTS OF CONFIDENTIALITY COMPROMISE

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not affected</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Lightly affected</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Moderately affected</td>
<td>6</td>
<td>46.2</td>
</tr>
<tr>
<td>Seriously affected</td>
<td>7</td>
<td>53.8</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

![Effects of Confidentiality Compromise](image.png)

Figure C.4 (refer Question A.4 in Appendix B)
Appendix C: Survey Analysis

EFFECTS OF INTEGRITY COMPROMISE

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not affected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lightly affected</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Moderately affected</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Seriously affected</td>
<td>12</td>
<td>92.3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Effects of Integrity Compromise

Figure C.5 (refer Question A.5 in Appendix B)
Appendix C: Survey Analysis

**EXISTENCE OF POLICY**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>2</td>
<td>15.4</td>
</tr>
<tr>
<td>No</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Yes</td>
<td>11</td>
<td>84.6</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

**Existence of Information Security Policy**

![Bar chart showing responses to existence of information security policy](chart.png)

1 = don’t know  
2 = no  
3 = yes

Figure C.6 (refer Question B.1 in Appendix B)

**EXISTENCE OF SECURITY PROCEDURES**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>2</td>
<td>15.4</td>
</tr>
<tr>
<td>No</td>
<td>2</td>
<td>15.4</td>
</tr>
<tr>
<td>Yes</td>
<td>9</td>
<td>69.2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Appendix C: Survey Analysis

**IMPORTANCE OF AWARENESS PROGRAMMES**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Yes</td>
<td>13</td>
<td>100.0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

**ATTENDING AN AWARENESS PROGRAMME**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>8</td>
<td>61.5</td>
</tr>
<tr>
<td>Yes</td>
<td>5</td>
<td>38.5</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Appendix C: Survey Analysis

WHEN THE AWARENESS WAS ATTENDED

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 12 months ago</td>
<td>3</td>
<td>23.1</td>
</tr>
<tr>
<td>10-12 Months ago</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>7-9 Months ago</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>4-6 Months ago</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>1-3 Months ago</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>MISSING</td>
<td>8</td>
<td>61.5</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Appendix C: Survey Analysis

HOW OFTEN SHOULD BE OFFERED

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 3 years</td>
<td>1</td>
</tr>
<tr>
<td>Once every 3 years</td>
<td>0</td>
</tr>
<tr>
<td>Once every 2 years</td>
<td>3</td>
</tr>
<tr>
<td>Once in a year</td>
<td>6</td>
</tr>
<tr>
<td>Twice in a year</td>
<td>3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>
Figure C.11 (refer Question B.6 in Appendix B)

DATA BACKUP AND STORAGE

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>12</td>
<td>92.3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Figure C.12 (refer Question B.7.1 in Appendix B)

Appendix C: Survey Analysis

SOCIAL ENGINEERING

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>3</td>
<td>23.1</td>
</tr>
<tr>
<td>Not recommended</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Recommended</td>
<td>9</td>
<td>69.2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Appendix C: Survey Analysis

**MOBILE/REMOTE WORKER SECURITY**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>2</td>
<td>15.4</td>
</tr>
<tr>
<td>Recommended</td>
<td>11</td>
<td>84.6</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

**MALICIOUS CODE**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>13</td>
<td>100.0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>
Malicious Code

Figure C.15 (refer Question B.7.4 in Appendix B)

Password Security

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>13</td>
<td>100.0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Figure C.16 (refer Question B.7.5 in Appendix B)

Appendix C: Survey Analysis

Internet/Web Browser Security

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>12</td>
<td>92.3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Appendix C: Survey Analysis

**Internet/Web Browser Security**

![Internet/Web Browser Security Chart]

Figure C.17 (refer Question B.7.6 in Appendix B)

**EMAIL SECURITY**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
</tr>
<tr>
<td>Recommended</td>
<td>13</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

![EMAIL SECURITY Table]

Figure C.18 (refer Question B.7.7 in Appendix B)

**TELEPHONE SECURITY**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>5</td>
</tr>
<tr>
<td>Not recommended</td>
<td>2</td>
</tr>
<tr>
<td>Recommended</td>
<td>6</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

![TELEPHONE SECURITY Table]
Figure C.19 (refer Question B.7.8 in Appendix B)

![Graph of Telephone security responses]

**Wireless Security**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>12</td>
<td>92.3</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Figure C.20 (refer Question B.7.9 in Appendix B)

![Graph of Wireless Security responses]

Appendix C: Survey Analysis

**Physical and Environmental Security**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Not recommended</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Recommended</td>
<td>11</td>
<td>84.6</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

185
Appendix C: Survey Analysis

**Physical and Environmental Security**

Figure C.21 (refer Question B.7.10 in Appendix B)

**Computer Ethics**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
</tr>
<tr>
<td>Recommended</td>
<td>13</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

Figure C.22 (refer Question B.7.11 in Appendix B)

**Hacking/IT Related Fraud**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>2</td>
</tr>
<tr>
<td>Not recommended</td>
<td>5</td>
</tr>
<tr>
<td>Recommended</td>
<td>6</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>
Hacking/IT related fraud

Figure C.23 (refer Question B.7.12 in Appendix B)

<table>
<thead>
<tr>
<th>PRIVACY AND CONFIDENTIALITY</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>13</td>
<td>100.0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Privacy and Confidentiality

Figure C.24 (refer Question B.7.13 in Appendix B)

PHOTOCOPY SECURITY

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>2</td>
<td>15.4</td>
</tr>
<tr>
<td>Not recommended</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Recommended</td>
<td>10</td>
<td>76.9</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Figure C.25 (refer Question B.7.14 in Appendix B)

**PAPER-COPY DOCUMENT SECURITY**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>2</td>
<td>15.4</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>11</td>
<td>84.6</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Figure C.26 (refer Question B.7.15 in Appendix B)

**ACCOUNTABILITY AND RESPONSIBILITY**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>13</td>
<td>100.0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>
### Copyright, Piracy and Intellectual Property

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don't know</td>
<td>1</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
</tr>
<tr>
<td>Recommended</td>
<td>12</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

Figure C.27 (refer Question B.7.16 in Appendix B)

### Anti-Virus Software and Firewalls

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don't know</td>
<td>1</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
</tr>
<tr>
<td>Recommended</td>
<td>12</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

Appendix C: Survey Analysis
INFO SECURITY POLICIES, STANDARDS AND PROCEDURES

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
</tr>
<tr>
<td>Recommended</td>
<td>13</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

Policies, Standards and Procedures

AWARENESS OF TECHNICAL DETAILS TO EVERY EMPLOYEE

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>4</td>
</tr>
<tr>
<td>No</td>
<td>7</td>
</tr>
<tr>
<td>Yes</td>
<td>2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>
Figure C.31 (refer Question B.8 in Appendix B)

### INFORMATION SECURITY RISK MANAGEMENT

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Recommended</td>
<td>12</td>
<td>92.3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Figure C.32 (refer Question B.9.1 in Appendix B)

### CONTINGENCY PLANNING

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Recommended</td>
<td>13</td>
<td>100.0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Contingency Planning

Figure C.33 (refer Question B.9.2 in Appendix B)

INCIDENT MANAGEMENT

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>2</td>
<td>15.4</td>
</tr>
<tr>
<td>Recommended</td>
<td>11</td>
<td>84.6</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Incident Management

Figure C.34 (refer Question B.9.3 in Appendix B)

IT LAWS, REGULATIONS AND STANDARDS

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Not recommended</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Recommended</td>
<td>11</td>
<td>84.6</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Appendix C: Survey Analysis

Computer Auditing

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>3</td>
</tr>
<tr>
<td>Recommended</td>
<td>10</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

Figure C.36 (refer Question B.9.5 in Appendix B)

Information Asset Management

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>1</td>
</tr>
<tr>
<td>Not recommended</td>
<td>2</td>
</tr>
<tr>
<td>Recommended</td>
<td>10</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
</tr>
</tbody>
</table>

Appendix C: Survey Analysis
Appendix C: Survey Analysis

**Information Asset Management**

![Bar chart showing responses](chart1.png)

Figure C.37 (refer Question B.9.6 in Appendix B)

**IT Governance**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Recommended</td>
<td>12</td>
<td>92.3</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

**CHANGE MANAGEMENT**

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Not recommended</td>
<td>4</td>
<td>30.8</td>
</tr>
<tr>
<td>Recommended</td>
<td>9</td>
<td>69.2</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Appendix C: Survey Analysis

**Preference for Examination**

<table>
<thead>
<tr>
<th>Preference</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>No</td>
<td>5</td>
<td>38.5</td>
</tr>
<tr>
<td>Yes</td>
<td>7</td>
<td>53.8</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

**Preference for Taking an Examination**

1=not sure
2=no
3=yes

**Offering of Awareness Certificate**

<table>
<thead>
<tr>
<th>Offering</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should not be offered</td>
<td>7</td>
<td>53.8</td>
</tr>
<tr>
<td>Should be offered but not examined</td>
<td>1</td>
<td>7.7</td>
</tr>
<tr>
<td>Should be offered after being examined</td>
<td>5</td>
<td>38.5</td>
</tr>
</tbody>
</table>
Opinion on Offering a Certificate

<table>
<thead>
<tr>
<th>Opinions</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1=should not be offered</td>
<td>7</td>
<td>7.7</td>
</tr>
<tr>
<td>2=should be offered but not examined</td>
<td>3</td>
<td>23.1</td>
</tr>
<tr>
<td>3=should be offered after being examined</td>
<td>8</td>
<td>67.7</td>
</tr>
</tbody>
</table>

Figure C.41 (refer Question B.11 in Appendix B)
### Appendix C: Survey Analysis

#### NEWSLETTERS

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not recommended</td>
<td>5</td>
<td>38.5</td>
</tr>
<tr>
<td>Recommended</td>
<td>8</td>
<td>61.5</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>13</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Figure C.42 (refer Question B.12 in Appendix B)
Appendix C: Survey Analysis

### POSTERS

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not recommended</td>
<td>3</td>
<td>23.1</td>
</tr>
<tr>
<td>Recommended</td>
<td>10</td>
<td>76.9</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Figure C.43 (refer Question B.13.1 in Appendix B)

### Posters

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not recommended</td>
<td>8</td>
<td>61.5</td>
</tr>
<tr>
<td>Recommended</td>
<td>5</td>
<td>38.5</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Figure C.44 (refer Question B.13.2 in Appendix B)
Appendix C: Survey Analysis

**Handouts/leaflets/pamphlets**

![Handouts/leaflets/pamphlets Graph](image)

Figure C.45 (refer Question B.13.3 in Appendix B)

**SCREEN SAVERS**

<table>
<thead>
<tr>
<th>Not recommended</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended</td>
<td>9</td>
<td>69.2</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

Figure C.46 (refer Question B.13.4 in Appendix B)

**COMPUTER-BASED TRAINING**

<table>
<thead>
<tr>
<th>Recommended</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not recommended</td>
<td>5</td>
<td>38.5</td>
</tr>
<tr>
<td>Recommended</td>
<td>8</td>
<td>61.5</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>
Computer-based Training

<table>
<thead>
<tr>
<th>Responses</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1=not recommended</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>2=recommended</td>
<td>100%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Figure C.47 (refer Question B.13.5 in Appendix B)

IN-PERSON INSTRUCTOR-LED TRAINING

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not recommended</td>
<td>2</td>
<td>15.4</td>
</tr>
<tr>
<td>Recommended</td>
<td>11</td>
<td>84.6</td>
</tr>
<tr>
<td>TOTAL</td>
<td>13</td>
<td>100.0</td>
</tr>
</tbody>
</table>

In-person instructor-led Training

<table>
<thead>
<tr>
<th>Responses</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1=not recommended</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>2=recommended</td>
<td>100%</td>
<td>0%</td>
</tr>
</tbody>
</table>

Figure C.48 (refer Question B.13.6 in Appendix B)

Appendix D

Research Paper
This is the research paper that was written as a result of the project.

Information Security Awareness: Towards a Generic Content

Hope Mauwa$^a$ and Rossouw von Solms$^b$

_Nelson Mandela Metropolitan University, Port Elizabeth, South Africa_
Abstract:

Basing information security awareness programmes on existing information security policies in organizations is a sound approach, since policies are basically seen as the basis for effective information security within organizations. But this approach does not satisfy the needs of organizations without these policies in place. Therefore, another approach, which does not entirely depend on existing policies in organizations, is needed, so that organizations, even those without the policies, can implement such a programme.

Keywords: Information Security Awareness Programmes, ISO/IEC 17799, ISO/IEC 13335-3

1. Introduction

In today’s computing environment, awareness programmes play a much more important role in organizations’ information security programmes because the maintenance of effective security is now more dependent on the vigilance of users. Even though awareness programmes have become increasingly important, the level of awareness in most organizations is still low. The current approach of developing these programmes recommends that they should stem directly from information security policies already existing in organizations (Du Plessis & Von Solms, 2002).

Appendix D: Research Paper

It is the objective of this paper to illustrate that this current approach of developing these programmes does not satisfy the needs of most organizations, resulting in the current low levels of awareness. Further, to propose an alternate approach suitable for most organizations that do not depend entirely on existing policies in organizations.
In order to accomplish this, this paper will look at several issues, including the role that information security awareness programmes play, in order to gain an understanding of the impact they have in information security. The current approach to the development of these programmes will be discussed to highlight its limitations. Once these have been established, an alternate approach will be proposed by examining the topics discussed in information security awareness programmes. Then, sources used to identify the contents for the proposed approach will be discussed. Finally, topics that can form part of the contents for the proposed approach will be identified based on the above studied sources.

2. Why Information Security Awareness

Information security awareness efforts are designed to change behaviour or reinforce good security practices, and they provide a baseline of security knowledge for all users, regardless of job duties or positions (Du Plessis & Von Solms, 2002). Security awareness allows individuals to recognize information security concerns and respond accordingly. Courtney Gilbert (2003) described security awareness as a learning process, which changes individual and organizational attitudes and perceptions so that the importance of security and the adverse consequences of its failure are realized. Thomson and Von Solms (1998) motivate that information security awareness gives employees the necessary knowledge to maintain information security by ensuring that confidentiality, integrity and availability of information are maintained.

Information security awareness focuses on developing an organizational culture that is both aware and capable of responding to security-related risks. It aims at changing the way employees behave towards an organization’s vital information and cultivating an information security culture right through an organization.

Appendix D: Research Paper

The way in which people work with information assets in their daily job functions eventually become the way things are done in an organization, and this eventually become part of the culture of an organization (Du Plessis & Von Solms, 2002).
Achieving this level of understanding represents a major challenge, because no amount of technology can reduce the overriding impact of human complexities, inconsistencies, and peculiarities (Ernst & Young, 2004). Ernst and Young (2004) claim that any strategy that overlooks this realization is inherently flawed. With proper awareness, employees become the most effective layer in an organization’s security defence.

With the important role that these awareness programmes play in organizations’ complete information security programmes, experts developed guidelines to assist organizations in developing these programmes.

3. The Current Approach to Security Awareness

The current approaches to the development of information security awareness programmes need to be examined. Studying these current approaches will assist in understanding the effect such programmes have on various organizations.

3.1 Guidelines and standards

The current guidelines recommend that awareness programmes should be developed, based on the security policies and procedures currently in place in organizations. This is advocated prominently in current information security guidelines and standards. Two such standards are ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005. This is so because management instructions, i.e., policies, are basically seen as the basis for effective information security within an organization (ISO/IEC 13335-1, 2004).

Appendix D: Research Paper

It has to be said that every organization is unique, and as such, different organizations have different management instructions on how their organizations should be run (Du Plessis & Von Solms, 2002). Therefore, the awareness programmes that stem from these management instructions are also different from one organization to another.
This could be called a company-specific approach to information security awareness, since it is based on elements that are very specific to a particular organization (Du Plessis & Von Solms, 2002).

Despite the illustrated importance of information security awareness and the widespread acceptance of this fact in current guidelines and standards, the level in most organizations is still low, according to some of the recently conducted surveys (Ernst & Young, 2004; Deloitte Touche Tohmatsu, 2005).

3.2 Limitations of Current Approaches

According to the Global Information Security Survey by Ernst & Young (2004), respondents named the “lack of security awareness by users” as the top obstacle to effective information security; however, only 28% listed “raising employee information security training or awareness” as being a top initiative in 2004. In the Global Security Survey, conducted by Deloitte Touche Tohmatsu – Australia (2005), respondents pointed to a host of continuing challenges to their businesses. One of the most prominent among them was the “lack of employee awareness and training” - (48%). According to the same survey, overall, security awareness and training implemented, or maintained, decreased from 77% in 2004 to 65% in 2005.

A possible reason for such a lack of awareness programmes in organizations could be the approach used to implement such programmes (Du Plessis & Von Solms, 2002). As pointed out in the last section, both ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005 stress the need for implementing these programmes, based on the information security policies and procedures already in place in the organizations. But not all organizations have these policies in place.

A recent survey conducted by PricewaterhouseCoopers LLP (2004), Information Security Breaches Survey 2004, reveals that a third of all companies in the United Kingdom, and two-thirds of large businesses, also in the United Kingdom, now have information security policies. Now, if these policies were the only basis for awareness
programmes, it would mean that only those organizations with policies in place would have a basis on which to formulate their information security awareness programmes.

The current lack of awareness programmes in most organizations suggests that a problem exists with the traditional method of basing awareness programmes on the policies and procedures already in place in organizations (Du Plessis & Von Solms, 2002). Therefore, an alternate approach to the development of information security awareness programmes has to be developed that will not depend entirely on existing policies in organizations.

4. **A Generic Information Security Awareness Programme**

An examination into the different areas of security knowledge covered in awareness programmes reveals that some aspects are company-specific while others are generic components that are non company-specific.

Company-specific information includes an organization’s information security policy’s contents and specific procedures. Policy documents are different for different organizations, since the goals and directions are also different. As such, employees of different organizations are, therefore, educated by different awareness material concerning the policies of their organizations. Procedures are based on the broad guidance provided by policies, and as such, they are much more specific for every organization. It is through policies and these procedures that employees within a specific organization are guided in their role of securing the organization’s information technology environment (Du Plessis & Von Solms, 2002).

*Appendix D: Research Paper*

Du Plessis and Von Solms (2002) argue that the focus in today’s information technology environment is not only on educating employees on the policies of the organization, but also on changing their behaviour and cultivating an information
security culture right through the organization. To achieve this, an information security programme would include aspects other than only the policies of that organization. Such aspects include general procedures, basic information technology concepts, threats to and vulnerabilities of computer systems and the importance of protecting information in today’s business environment (Du Plessis & Von Solms, 2002), which tend to be general and common aspects that affect most organizations. Generally, these aspects are part of a company-specific contents but could be catered for in a non-company specific way. Such an approach to implementing an awareness programme can be called a generic approach to information security awareness (Du Plessis & Von Solms, 2002).

An information worker in most organizations needs to be aware of the general information threats and vulnerabilities that exist today, specifically when using electronic means. All such aspects should form part of such generic information security awareness programme.

Having examined what would constitute a generic programme, several sources were studied in order to formulate the actual contents of this programme.

5. **Towards a Generic Information Security Awareness Programme**

Several internationally recognised sources, information security awareness programmes located on the Internet and a survey conducted by the authors, were used to identify the contents of a generic information security awareness programme and to ensure that the foundation on which it is based is as broad as possible.

*Appendix D: Research Paper*

5.1 **The Standards**
The ISO/IEC 17799:2005 and the ISO/IEC 13335-3:2005 were used because they comprehensively cover awareness programmes. Both standards recommend that information security awareness programmes should reflect on the contents of a corporate information security policy, and should cover all objectives of an information security plan. The ISO/IEC 13335-3 goes on to say that the programme should ensure that the IT staff and the end-users have enough knowledge of the hardware and software systems that they understand why safeguards are necessary, and that they know how to use them correctly.

5.2 The Internet

Some awareness programmes offered on the Internet were studied thoroughly to gain more insight into the topics covered in them. A well-known one is the SANS Security Awareness Programme. This covers general security areas affecting most organizations, such as passwords, computer viruses, malicious codes, personal use and gain, data backup and storage, incident response, environmental security, inventory control, physical security and social engineering. It also covers true-life stories that have happened to people and organizations to reinforce the concepts covered. Each one demonstrates the consequences of simple mistakes or lapses in information and computer security.

Having studied what is covered in these sources and the Internet, a questionnaire was drafted and sent out to some well-known South African organizations, which are known to follow sound information security principles.

5.3 The Author’s Survey

The main aim of the survey was to solicit ideas on what organizations think should be included in a generic programme. It is important to point out that the organizations that participated operate in different industrial sectors.

Appendix D: Research Paper

This was done in order make sure that the identified content is suitable for interdisciplinary organizations. Consequently, industries from mining, manufacturing,
food and beverages, education, communications and IT sectors, participated in the survey. Important conclusions were drawn from the survey results, and some need some discussion.

It was encouraging that all the organizations that participated in the survey realise the importance of information and the ICT infrastructure to their daily operations. Over 60% of the organizations rated their business information and the ICT infrastructure as very important, and that they are directly impacted upon in their daily operations if the confidentiality, integrity and availability of information and the ICT infrastructure are compromised in any way.

Over 75% of the respondents indicated that they have organizational information security policies, procedures and guidelines. This percentage indicates that most of them realise the important role that these play in protecting information assets. It is very important for organizations to have them and to make their employees aware of their existence. Moreover, any information security initiative starts with these policies. But there are still some organizations where employees are unaware of their existence. This is confirmed by the survey: about 20% of the respondents indicated that they did not know whether their organizations have policies or not.

It is an encouraging development that all the respondents realise the important role that awareness programmes play. Unfortunately, about 60% of the respondents indicated that they have never attended any such programme. Another discouraging fact is that out of those that attended awareness programmes, most of them (23%) attended them more than a year ago.

The guidance and recommendations provided by the above sources and the survey are sufficiently broad to base the contents of a generic programme on them. Therefore, a single content of such a programme will be identified, based on these.

Appendix D: Research Paper

6. Generic Contents of an Information Security Awareness Programme
It is important to bear in mind that general and common aspects affecting most organizations’ employees would need to be included when identifying the topics for a generic programme. Any company-specific information, such as information security policies, guidelines and procedures, would only be introduced to the employees to make them aware of their existence, and encourage them to find out more from their respective organizations. Based on the guidance and recommendations from the sources studied and the survey, the following broad topics were identified as part of the contents of a generic information security awareness programme:

- Data backup and storage
- Social engineering
- Remote/mobile worker security
- Malicious code security
- Password security
- E-mail security
- Physical and environmental security
- Computer ethics
- Privacy and confidentiality
- Paper-copy document security
- Accountability and responsibility
- Anti-virus software and firewalls
- Information security policies, standards and procedures.
- Information risk management
- Contingency planning
- Incident management
- IT laws, regulations and standards
- Computer auditing
- Change management

Appendix D: Research Paper

It is important to point out that a generic awareness programme has to sacrifice the scope of the material that it presents. The scope needs to be sacrificed in order to
satisfy the primary goals of keeping the programme generic. All that the generic approach tries to achieve is to provide a baseline of awareness by educating the employees on the essentials of information security. Having such a baseline in place can provide organizations with the assurance that some basic level of awareness exists among employees.

7. Conclusion

It was established that the general approach of basing awareness programmes on company policies and procedures already in place in organizations is a limiting factor to those without policies and procedures. Organizations without these policies and procedures do not have a basis on which to support their programmes. This has contributed to the current low level of information security awareness in most organizations.

The contents of awareness programmes identified on the Internet were examined, and it was realized that these programmes do have a generic component that is company-independent. Therefore, a generic approach, which does not depend entirely on existing policies and procedures in organizations and caters for only this non-company-specific component, was further investigated and proposed. The actual contents of the generic programme were also formulated using guidance from the ISO/IEC 17799:2005 and ISO/IEC 13335-3:2005, the Internet and the survey that was conducted with some South African organizations. These sources were used to make sure that the foundation, on which the contents of the generic programme are based, is as broad as possible.

The generic approach would allow for the creation of an awareness programme that would be suitable for most organizations, even those without policies and procedures in place. As such, it is expected to improve the levels of awareness programmes in organizations.

Appendix D: Research Paper

It must be noted though, that such a generic information security awareness programme, as suggested in this paper, should be augmented eventually with some
contents to cater for the company-specific information that cannot be included in such a programme.

Appendix D: Research Paper

Bibliography


Appendix D: Research Paper

Port Elizabeth, Nelson Mandela metropolitan University, North Campus. Magister Technologiae.