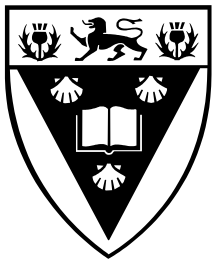


RHODES UNIVERSITY

INVESTEC BUSINESS SCHOOL

Where Business Leaders Learn

An Investigation of Information Security in Small and Medium Enterprises (SME's) in the Eastern Cape

Research Dissertation

Submitted in Partial fulfilment of the Requirements for the
Degree of Master of Business Administration
Rhodes Investec Business School
Rhodes University

By

Christopher Tennant Upfold

January 2005

Abstract

Small and Medium Enterprises (SME's) embrace a wide range of information systems and technology that range from basic bookkeeping and general purpose office packages, through to advanced E-Business Web portals and Electronic Data Interchange (EDI). A survey, based on SABS ISO/IEC 17799 was administered to a select number of SME's in the services sector, in the Eastern Cape. The results of the survey revealed that the level of information security awareness amongst SME leadership is as diverse as the state of practice of their information systems and technology. Although a minority of SME's do embrace security frameworks such as SABS ISO/IEC 17799 or the International equivalent, BS7799, most SME leaders have not heard of security standards, and see information security as a technical intervention designed to address virus threats and data backups. Furthermore, there are several "stripped-down" standards and guidelines for SME's, based mostly on SABS ISO/IEC 17799, but designed as streamlined, more easily implemented options. Again, these "lighter" frameworks are scarcely used and largely unknown by SME's. Far from blaming SME leadership for not understanding the critical issues surrounding information security, the research concludes that SME leadership need to engage, understand and implement formal information security processes, failing which their organisations may be severely impacted by inadvertent threats / deliberate attacks on their information systems which could ultimately lead to business failure.

Acknowledgements

I would like to thank the following people for their help and contribution during the process of producing this dissertation:

My supervisor Professor David Sewry. Dave, thank you for your unrelenting guidance and support. This has been a long process for both of us. I have really appreciated your selfless commitment, especially over Christmas 2004. Thank you.

To Andrea, I would not have completed the MBA without your encouragement and enthusiasm at each milestone. Thank you for believing in me and giving me the time and support.

Nicky and Jenny, you have been so patient and understanding. Thank you.

My colleagues, thank you for your encouragement.

To the MBA Class of 2001, thank you for sharing your learning with me.

To my family and friends, your continued enthusiasm and encouragement has been so welcome. Thank you.

I acknowledge that all references are accurately recorded, and that unless otherwise stated, all work contained herein is my own.

Christopher Upfold

Table of Contents

Chapter 1: Introduction

Abstract

Chapter 1 introduces the research context, describes the goals and objectives of the research, lists the summary of key results of the research, and finally, describes the organisation of the dissertation.

1.1 Introduction

Information is an asset that needs to be strategically managed and protected much like any other business asset. Information security is the protection of information within a business, and the systems and hardware used to store, process and transmit this information. (Whitman and Mattord, 2003: 15) It is imperative that business leaders understand the value of information contained within their business systems, and have a framework for assessing and implementing information security. Various security frameworks as well as standards exist, and are available for adoption by business / organisations:

- National Institute for Standards and Technology (NIST), SP800-12, SP800-14, and SP800-18
- Internet Engineering Task Force (IETF) Security Architecture: RFC2196
- South African Bureau of Standards (SABS) ISO/IEC 17799
- Information Institute of South Africa, (ISIZA) framework. (BS7799 based) Similarly, a number of Certification schemes exist and are available for adoption by businesses / organisations:
- Certification Scheme for Certification of Information Technology, (ICIT)
- Pentana Checker
- BS 7799 Part 2 (Provides both recommendations for establishing an effective Information Security Management Systems (ISMS) and serves as assessment guide for certification)

Control Objectives for Information and Related Technologies (COBIT) is a popular IT framework often used by larger organisations to address security.

While many of the security frameworks with their associated certification schemes are considered to be complex, all embracing, and ultimately costly to implement, they are

well conceived, internationally approved frameworks and schemes that will safeguard an organisation against information loss and liability, if implemented properly.

Small and Medium Enterprises (SME's) are a priority focus area of government economic policy and are considered to be of key importance to socio-economic growth in South Africa. (National Small Business Act, 1996). SME's are usually born out of entrepreneurial passion and limited funding, with business systems that are often 'patched together' lacking any degree of integration and sophistication. Policies and frameworks for information security planning and disaster recovery are usually non-existent. Moreover, a basic understanding of information security risk in SME's does not extend much beyond viruses and anti-virus software. Inadvertent threats pose some of the highest information security risk to SME's and yet personnel training and awareness programmes are often neglected. Recent surveys highlight a few of the many concerns surrounding information security (drawn from: PricewaterhouseCoopers DTI information security breaches survey (2004) and Special Report, Imation Small Business Survey (2003))

- Between 19% and 25% of small and medium businesses do not have any formal data backup and storage facilities.
- 26% of small and medium businesses are not confident they could restore files after an e-mail virus.
- Two thirds of businesses surveyed had a premeditated or malicious incident during 2004 compared with just under half in the previous two years.
- A quarter of businesses surveyed had a significant incident involving accidental systems failure and data corruption.
- Virus infections and inappropriate use of systems by staff were the cause of most of the incidents. Viruses also caused the greatest number of serious incidents.

Ironically, a lack of adequate information security policies and procedures in SME's is prevalent at a time when business connectivity to public networks is increasing, and E-Business is enabling SME's to leverage markets that were previously the reserve of enterprise business. SME management must be aware that information security risk extends to legal, regulatory, and to a lesser extent, governance liability. The South African Electronic Communications and Transactions Act, (ECT Act, 2002)

highlights the regulatory framework within which electronic communications and transactions must be conducted. The Act is expected to have far reaching consequences for businesses not adhering to policies contained in the Act, especially in terms of the collection, usage, storage and disposal of data.

Although implementing information security may initially be seen as a costly exercise, it need not be so. There are numerous resources freely available including policy document templates and guidelines. The benefits to SME's in formalising information security processes will manifest in numerous ways including increased operational efficiency. Information security is no longer a nice-to-have option for SME's. The potential losses incurred in a security attack or the litigation faced through accidental disclosure of confidential information, may deal an unrecoverable blow to an SME.

1.2 Goals and Objectives of the Research

The goals of this research are to:

- Investigate information security, especially with regard to Small and Medium enterprises (SME's).
- Explore some of the more widely known security frameworks before focusing on SABS ISO/IEC 17799.
- Construct a list of information security issues, pertinent to SME's, and to map these issues to each of the ten (10) Control Domains contained in SABS ISO/IEC 17799.
- Assemble and administer a questionnaire, based on the ten (10) SABS ISO/IEC 17799 Control Domains, and to evaluate the information security state of practice in select SME's in the services sector, in the Eastern Cape.
- Make recommendations, for improved information security in SME's.

1.3 Summary of Results

- SME leaders often have differing perceptions and enthusiasm for information systems, technology and security.
- SME leadership must understand that information systems need to be maintained.
- SME's management must contractually manage service providers

- SME leadership should try to obtain 3rd party advisory assurance
- SME leadership must not under estimate the asset value of human knowledge. This should be nurtured and protected.
- There are various options when it comes to managing risk, including outsourcing. SME management must understand risk management choices. This will imply an understanding of information security.
- Personnel training and security awareness is synonymous with information security. SME's will not achieve secure information systems without well trained, security conscious personnel
- SME leadership must work hard to establish a co-operative environment where staff buy-in to the information security process. Without staff co-operation, there can be no information security in an SME.
- Numerous security frameworks, certification schemes and other resources abound, many of these are freely available off the Internet. SME's must research and capitalise these resources.
- SABS ISO/IEC 17799 is the fully adopted South African version of the international security standard, ISO/IEC 17799, which in turn originated from the British Standard BS7799.
- Although SABS ISO/IEC 17799 is a comprehensive standard, it can be tailored to suit SME's, as each of the 10 domains offer a variety of security controls.
- Adopting information security demonstrates good governance.

1.4 Organisation of Thesis

Chapter 2: introduces the characteristics of Small and Medium Enterprises (SME's) and is intended to give the reader an understanding of the environment that SME's operate in, as well as the components that make up an information system.

Chapter 3: introduces information security and describes the types of risk associated with inadvertent and deliberate information security risks / attacks.

Chapter 4: explores different methods that may be used by an organisation to examine threats and vulnerabilities.

Chapter 5: introduces the legal, regulatory, governance and personnel considerations impacting on business and information systems.

Chapter 6: describes the various security standards and models that are commonly available for organisations to adopt.

Chapter 7: focuses on SME information security issues and SABS ISO/IEC 17799. SME security concerns are mapped to SABS ISO/IEC 17799 Domain Controls.

Chapter 8: explores the design of the experiment.

Chapter 9: presents the results of the survey.

Chapter 10: explores further meaning and the implication of the results obtained in chapter 9.

Chapter 11: offers a conclusion to this research.

Chapter 2: Information Systems in Small Businesses

Abstract

This chapter introduces the characteristics of Small and Medium Enterprises (SME's), as well as information and information systems. The components or building blocks of an information system are discussed, and an attempt is made to indicate how SME's need to maintain these components, if they wish to leverage the benefits of their information systems.

2.1 Introduction

Small, Medium and Micro Enterprises (SMME's) range from so called survivalist enterprises that provide minimal subsistence to entrepreneurs, and with no IT infrastructure, to medium sized enterprises that employ up to 100 staff members, operate within a well supported IT infrastructure and boast good access to financial institutions and equity funders. Small and medium enterprises increasingly depend on information systems, which consist of well integrated computer hardware, software, data, people and procedures. While SME's may need to upgrade or replace computer hardware and patch / update computer software, it is often people and procedures that are overlooked, and pose the greatest risk to information systems and security. Staff members working in an organisation enjoy the closest access to informational data. A breach of procedures such as a staff member leaving a terminal unattended while walking around the building, or a systems administrator failing to store backups off-site, may result in severe consequences for the organisation. There is a need to raise information technology skills and security awareness amongst personnel, not least through deliberate training programmes.

2.2 Small, Medium, Micro Enterprises (SMME's)

The National Small Business Act (National Small Business Act, 1996) classifies Small, Medium and Micro enterprises according to five different categories, ranging from Survivalist to Medium-Sized enterprises. Each of the five SMME categories are summarised below.

- Survivalist enterprises

  Survivalist enterprises typically have no paid employees, minimal asset value and generate income below the minimum income standard or poverty line. These

enterprises provide minimal subsistence means for the unemployed and their families. Most of the entrepreneurs in this category are involved in hawking, vending and subsistence farming. Entrepreneurs operating in the survivalist sectors generally have little or no collateral and no access to formal financial institutions. Furthermore, these entrepreneurs lack basic computer literacy skills and do not employ any form of Information Technology within their enterprises.

- Micro-enterprises

  Micro-enterprises usually have less that five (5) paid employees, lack formality in terms of tax-registration, labour legislation, business premises and accounting procedures. Examples of micro enterprises are spaza shops, mini taxis, and household enterprises. Although Micro entrepreneurs are likely to have slightly better access to formal financial institutions than Survivalist enterprises, they are most likely to finance their businesses through family and friends, money lenders, and Non-Governmental Organisations (NGO's). Micro-enterprises, like Survivalist-enterprises, are unlikely to have in-house IT skills and usually lack any IT infrastructure.

- Very small enterprises

  Very small enterprises typically employ less than ten (10) staff members although in the mining, construction and manufacturing sectors this may be less than twenty (20). The businesses run by self employed artisans and consultants are also classified as very small enterprises. These enterprises have access to formal financial institutions, and although they could benefit from debt and equity, are generally too small to attract equity financiers. Very small enterprises usually have access to modern technology and this may include the deployment of rudimentary Information Technology (IT) such as a stand-alone PC or a small Local Area Network (LAN). Often entrepreneurs carry around a laptop with little consideration given to the strategic importance of data stored on the device. Much is written on the disastrous consequences of data loss due to theft or malfunction of IT equipment.

- Small enterprises have fewer than 50 employees, are more established than the previously described SMME's, and usually have more complex business processes. They have greater financing needs than very small enterprises and often use leases and credit facilities to address operational expenses, although

business expansion is usually addressed by equity injections. Loan finance requirements normally range between R20 000 to R5 million. Although many small enterprises have sophisticated information systems used by their management team to support business decisions, they often lack information security rigor and at best make use of rudimentary backup processes.

- Medium sized enterprises normally employ up to 100 staff members and their management structures are usually more complex than small enterprises. Medium sized enterprises normally have well established relationships with their banks and those firms with growth potential are targeted by equity financiers. Medium sized enterprises most likely seek a listing on the securities exchange and have a complex, remotely connected and well supported IT infrastructure. There is generally a better understanding of the need for information security in medium sized enterprises.

Small, Medium and Micro Enterprises (SMME's), are a priority focus area of government economic policy and are considered to be of key importance to socio-economic growth in South Africa. It is highly unlikely that Micro enterprises would adopt any form of information systems and technology, and therefore, this research focuses on small and medium enterprises (SME's). Some examples of SME's included in this research can be found in Table 2.1.

Nature of SME	No of Personnel	Type of IT Deployed
Environmental Services Consulting company	3	Bookkeeping system, Office Network with printers / scanners / fax system Document storage
Electronic Goods and Services Retailer	8	Bookkeeping system Inventory / Sales system
Travel Agency	11	Bookkeeping system, Office Network with printers, Galileo ticket booking system
Video / DVD Rental Business	4	Video Rental Admin System
Electrical Retail Business	12	Bookkeeping system, Inventory / Sales system
Financial Services Broker	4	Bookkeeping system Client Database Office Network with printers / scanners / fax system

Building Suppliers Business	14	Bookkeeping system, Office Network with printers / scanner / fax system Bar Code Point of Sale System
Private Bank	50	Proprietary banking system, Other financial Systems, Office Network with terminals, printers / scanners / fax systems

Table 2.1 Types of SME's covered in this research

SME's are often born out of entrepreneurial passion and opportunism combined with limited funding. As SME's gradually develop in size, so does the complexity and disparity of their business systems. Growth is usually constrained through limited financial resources and expertise. Existing business information systems are often 'patched' together, lacking integration and sophistication and at best there are ad-hoc attempts to instil basic security. There is quite often the misperception that information security is the same as Information Technology (IT). Michalson (2003) states, "*although technology is a part of security, it is only one part of an overall process – the devil is in the detail*". He refers to a custom process of information security where organisations may argue convincingly that "out-of-the-box" solutions such as fire-walling solutions or anti-virus programs are inappropriate and greater flexibility may be more appropriate for dealing with information security.

2.3 Information and Information Systems

Szymanski, Szymanski and Pulschen (1995: 588) define Information as data that have been processed into an organized, usable form and are meaningful to the recipient for the task at hand. A telephone directory contains data in a form that provides useful contact information on private individuals, companies and organisations. An information system is defined as a system whether manual or automated, that comprises people, machines and /or methods organized to collect, process, transmit and disseminate data that represent user information. (Laudon and Laudon, 1995). Using the telephone directory example, an information system would comprise of personnel, computer database systems and the methods used to collect and maintain the records of private individuals, company's and organizations contained within the

telephone directory. This may also extend to the publishing and printing of the actual telephone directory.

2.4 Information System Components

According to Schultheis and Sumner (1995) a system is a collection of people, machines, and methods organized to accomplish a set of specific tasks. Information is the feedback required to determine whether a system is achieving its objectives, operating with the necessary components, and meeting the required standards. Information Systems are designed to give managers the information they require as feedback. Long and Long (1996) suggest that the term information system is a generic reference to a computer based system that:

- Provides information processing capabilities for an individual or an entire organisation.
- Provides the information enabling people to make better, more informed decisions

Whitman and Mattord (2003: 16) emphasize that information systems consist of computer hardware, software, data, people and procedures and not only the computer hardware on which information systems run. This emphasis is noted as in the field of information security, there is a tendency for people to view security solutions as one dimensional, either hardware or software based, often leaving out the most important components, namely, people and policies.

2.4.1 Hardware

Hardware refers to actual physical, tangible equipment such as cables, solid state devices such as computers, computer monitors, printers, and fax machines. Most SME's are likely to have at least one computer, connected to a printer. The hardware configuration often includes a modem that is used to connect (dialup) to a service provider which in turn facilitates on-line banking and Internet usage. A variety of office automation systems are currently available for SME's which include printing, scanning, copying and faxing facilities integrated into a single device. Many SME's run simple peer-to-peer networks, connecting several computers together and enabling the sharing of peripheral devices such as printers and scanners. These simple networks consist of hubs or switches and the requisite cabling which is used to connect different devices together. Computers that are connected to one another in a

small office environment are said to be connected in a Local Area Network (LAN). The hardware used in such a networked environment consists of hubs / switches as well as special cabling.

Wireless networking equipment enables computers and other network enabled devices to communicate with one another using radio frequencies. Although wireless networks are a fairly recent innovation, they are becoming increasingly popular, especially in localized areas such as office buildings or factory loading bays where the laying of cabling may pose difficulties or the network may require rapid and / or temporary deployment. Wireless networking is not only improving in bandwidth capability, but is increasingly affordable, easy to deploy, and has become an off the shelf purchase. For these reasons, it is gaining rapid acceptance amongst SME's where conventional cable ducting and the cables themselves may be considered too costly to install. Most new laptops, as part of their standard configuration, have built-in wireless network cards. Difficulties that may face SME's, however, is that due to radio transmission used in this medium, expertise is required to configure and fine-tune wireless equipment so that data communication is secure and not open to eavesdropping.

2.4.2 Software

Software refers to computer operating systems such as various versions of Microsoft's Windows or alternatively certain Open Source operating systems such as Linux or FreeBSD. In addition to computer operating systems, there are many 'applications' or software programs written by software programmers / developers. These software applications provide for additional functionality and include accounting packages used by bookkeepers and accountants or Computer Aided Design (CAD) packages used by engineers, architects and other designers. A minimal software installation found in a SME would typically include a version of Microsoft Windows such as XP, an office suite such as Microsoft Office 2003, a book-keeping / accounting package such as Pastel or Quick-books. A variety of specialised packages are available for professionals, such as administrative / patient billing systems for Doctors and Dentists. Quite often business management opt to have a custom software system developed to meet their specific needs. Whether a business implements 'off-the-

shelf' software products or has custom software developed for their purposes, software needs to be maintained and updated. Software maintenance patches are released, sometimes quite frequently by software suppliers, and are applied by technical staff to software installations, in order to 'fine-tune' and 'patch' problems or known 'bugs' within a particular system. Software remains one of the major security obstacles for organisations, as 'hackers' (people that either professionally or as a hobby, enjoy breaking into other people's systems), may explore every known and unknown vulnerability to gain access to a particular system.

SME's are frequently challenged with a lack of in-house IT expertise and this leads to ad-hoc maintenance and the erratic application of software updates / patches to the various computer systems found within SME's. This difficulty is exacerbated as both hardware and software becomes increasingly complex and large organisations, let alone SME's, battle to keep up to date with technology developments and in-house expertise.

2.4.3 Data

Data, according to Long (1994: 7) is the raw organisation / user specific information that is stored within an Information System. To illustrate this, an accounting system used by an enterprise will hold the information relating to debtors and creditors. The format and structure of this data depends on the application being used to process this data.

Information is data that has been collected and processed into a meaningful form. To continue with the accounting example, a bookkeeper may use an accounting application to produce a report of the number of company debtor days. Effectively the bookkeeper has used the accounting package to process the data contained within the system to provide the necessary information so that company debtors can be chased up. Data found within the context of an SME may include:

- Accounting information
- Customer Details
- Supplier Details
- Inventory codes and prices
- Contractual Details
- General Correspondence

Data is normally stored in Databases and it is important that these databases are correctly maintained. Although databases may be set-up or installed as part of an information system roll-out, they do require regular maintenance, which may range from daily / weekly backups through to data recovery and hardware resource upgrades. It is important that SME's understand the need to look after data contained in organisational systems.

2.4.4 People

People are the originators, designers, implementers, maintainers, and users of information systems. Laudon and Laudon (1995: 18) refer to the interrelation between people and technology and suggest that individuals need to adjust to rapid advancements in technology. They mention the need for developers to design systems that individuals can understand, operate, and use responsibly. This process involves studying and understanding Human Computer Interfaces (HCI). It serves no purpose to design a state of the art computer system that users cannot operate because the man machine interface is illogical and unclear. Information System users in SME's, are often, modestly skilled IT practitioners who simply use their computer infrastructure as a set of tools to perform various tasks. These tasks may include on-line banking, word-processing, customer data capture, and bookkeeping applications. User training is critical and cannot afford to be overlooked. Users need to take ownership and must want to use an information system. It is important that users understand the consequences of their actions when working within an Information technology environment. A person working in a high risk environment such as a financial institution must be made aware of the consequences of leaving their terminal open while taking a tea break, for example. The owner of a small business, who carries around a laptop, needs to be aware of the risks involved in the loss of data through equipment damage or theft. A part time book-keeper working for a small business needs to make sure that company financial data is secure and correctly backed-up.

2.4.5 Procedures

Whitman and Mattord (2003: 17) refer to procedures as written instructions, detailing how specific processes are achieved. According to Peltier (2002: 26), procedures are the detailed steps to be followed by users, support personnel, or others to achieve a

particular task. A doctor's reception assistant may be required to capture client information including medical aid details, prior to sending the patient through for a consultation with the doctor. A travel consultant may be required to process a client's VISA application successfully, prior to issuing tickets for a particular destination. A bookkeeper working for an SME may be required to perform a complete accounting system back-up at the end of each working day.

2.5 Conclusion

SME's are usually run by entrepreneurs who view information systems and technology as tools that can be used to assist in running a business more efficiently. It is important that SME management not only leverage off the advantages inherent in well functioning information systems, but also understand the importance of maintaining, upgrading, and correctly configuring the hardware and software components of these systems. Information systems may be robust, but they cannot run continually without some form of maintenance. Access to good in-house or outsourced technical expertise is important, and trained, disciplined, personnel are equally important, if a sustained advantage is to be enjoyed through information systems.

Chapter 3: Information Security

Abstract

Chapter 2 explored the nature of SME's and the components that make up an information system. The nature of information and information systems was introduced as well as the difficulties that may be experienced by SME's, if the building blocks of information systems are not correctly maintained.
This chapter introduces information security and details the nature of risk associated with both inadvertent and deliberate threats facing organisational information systems.

3.1 Introduction

Most definitions of information security refer to information assets, which include hardware and software systems, as well as the policies and practices put in place to manage and protect the integrity of information assets. In order to mitigate against the impact of information asset loss, organisations need to understand the nature of threats facing information assets. Whitman and Mattord (2003: 43), refer to inadvertent threats caused by poorly trained / ill disciplined staff members, or deliberate well orchestrated malicious attacks aimed at bringing an organisation to its knees, such as a Denial of Service (DOS) attack.

This Chapter explores the types of information security threats and attacks that may face an organisation, and highlights the importance that personnel play in ensuring the security and integrity of an information system. The challenges facing SME's with regard to outsourcing information security expertise are explored. The chapter concludes that outsourcing is a real option for organisations that cannot afford in-house expertise, but the ultimate responsibility lies with an organisations management team to ensure that the services delivered by outsourced staff meet the security requirements of the organisation.

3.2 Definition

Whitman and Mattord (2004: 28) refer to security as a state of being secure or to be free from danger. They define information security as the protection of information and its critical elements. Michalson (2003) defines information security as the

umbrella concept that includes intangible information assets as well as the underlying computer hardware, software, networks and infrastructure used for the secure collection, storage and dissemination of Information. Volonino and Robinson (2004: 1), define information security as incorporating the policies, practices and technology that must be in place for organisations to transact business electronically via networks with a reasonable assurance of safety. According to them, assurance not only applies to all online activities, transmissions, and storage, but includes business partners, customers, regulators, insurers, or others who might be at risk in the event of a breach of that company's security. Whitman and Mattord (2003: 9) refer to information security as the "*protection of information and the systems and hardware that use, store, and transmit that information*"

3.3 Importance of Information Security

Information and the systems and hardware that support it are the lifeblood of any organisation which, if compromised, can have devastating consequences. Whereas in an industrialized economy, assets are often classified as plant and machinery, in an information / knowledge based economy, assets are vested in people who informally network, hold and process information. Just as steps have to be taken to protect physical property and people in an organisation, information security must be deployed to ensure that intellectual property is protected. (Peltier, 2003: 21).

Both Volonino and Robinson (2004: 24) and Michalson, (2003) emphasise the legal consequences of inadequate information security procedures. According to the Information Technology – Code of Practice for information security Management, SABS ISO/IEC 17799:2000, information can exist in different forms such as printed or written documents, stored electronically, transmitted by post or electronic means and in films or spoken in conversation.

The importance of information and its security is embodied in 8 characteristics of information (Whitman and Mattord, 2003: 11)

- Confidentiality

  Confidentiality refers to people or systems having controlled access to information. Confidentiality is breached when information is accessed illicitly.

- Integrity

  Integrity refers largely to controlled user access and discipline in working with information and introduces the concept of correctness and accuracy of information stored within an information system. Information contained within a computer database may be corrupted in a number of ways: system hardware failure, a computer virus, deliberate damage / deletion caused by a disgruntled employee, accidental damage caused by operator error.

  Information transmitted across a network may be corrupted through interference within the communication medium, resulting in faulty or inaccurate data.

- Availability

  Availability refers to a user or computer system having access to information without interference or obstruction. The assumption is made that users or systems have the requisite permissions to access information without interference or obstruction.

- Privacy

  Privacy refers to collected / stored information strictly used for the purposes for which it was intended. An organisation that collects and stores client information with client consent, but then sells off the information to a third party without the clients knowledge, is behaving in an unethical manner and may face litigation from the client and the state. Information that falls into the wrong hands through a security breach may also result in legal repercussions for an organisation storing information.

- Identification

  Identification refers to the control of access to information by some form of user or system authentication. All current Network Operating Systems (NOS) have a security level that requires a user id and matching password.

- Authentication

  Authentication refers to the verification process in which a system is able to verify the identity of a user, based on access permissions which are usually stored centrally within a secure database.

- Authorisation

  Authorisation refers to the process in which a user or system is granted access to an information resource based on pre-determined user or system permissions Authorised permissions are often read, write, create, and delete but may include additional permissions based on the file system being used.

- Accountability

  Accountability refers to the levels of confidence or trust within the management integrity of information and the way in which it is stored and protected". Accountability may exist when an information systems is managed in such a way as to address all of the above security issues, and there is a metric in place to monitor and track user and system activities so as to provide evidence of these measures.

3.4 Threats

Whitman and Mattord (2003: 43) refer to a threat as an object, person, or other entity that represents a constant danger to an asset. Geiger and Pendegraft (1999: 2) suggest that these dangers can occur as a result of internal weaknesses in organisational structure and procedures, employee access and control, or external attacks occurring over the Internet. Whitman and Mattord, (2003: 44) site the example of a bank consultant who managed to transfer millions of dollars to an illegal account through internally gaining access to the banks procedures on money transfers. Although an organization needs to be aware of the risks associated with dishonest, unethical employees, improperly trained honest employees may accidentally bring a business to its knees, simply by not following procedures and misunderstanding the consequences of a particular action. An organisation may incur huge expense, installing state of the art fire-walling systems in order to isolate its network against attacks from the outside world. An employee, dialling-into a personal service provider from within the organization, using his / her standard office telephone line and a modem, may

inadvertently provide the connectivity that a hacker, outside, is looking for to gain access to the heart of the companies internal network. In this case, an acceptable usage policy to do with the organisations network, and the requisite training, may be all that is needed to enlighten staff members, as to the dangers of bypassing the organisations fire-wall.

Volonino and Robinson (2004: 41) suggest that undisciplined practices and unregulated Internet usage have made employees dangerous. They, (Volonino and Robinson, 2004: 42) argue that it is unrealistic to expect employees to restrict their email and Internet activities to those of the business unless the employee's firmly understand the consequences of doing so.

An organisation may believe they have introduced sufficient procedures to assist them recover data and services in the event of a site disaster such as a fire or flood, but until these procedures have been thoroughly tested, and staff properly trained in using the procedures, the organisation may be unnecessarily exposed in the event of a real disaster. Peltier (2003: 21) concurs with Geiger and suggests that the protection problem is compounded by the interconnecting of corporate (private) networks and the public media. Peltier (2003: 23) suggests that many information systems were not designed to be secure. The Internet, itself the basic building block of many inter-organisational initiatives, was not designed to communicate and security has become an add-on process. Table 3.1 indicates categories and examples of information security threats:

Categories of threat		Examples
1.	Acts of human error or failure	Accidents, employee mistakes
2.	Compromises to intellectual property	Piracy, copyright infringement
3.	Deliberate acts of espionage or trespass	Unauthorized access and / or data collection
4.	Deliberate acts of information extortion	Blackmail of information disclosure
5.	Deliberate acts of sabotage or	Destruction of systems or information

	vandalism	
6.	Deliberate acts of theft	Illegal confiscation of equipment or information
7.	Deliberate software attacks	Viruses, worms, macros, denial-of-service
8.	Deviations in quality of service from service providers	Power and WAN service issues
9.	Forces of nature	Fire, flood, earthquake, lightning
10.	Technical hardware failures or errors	Equipment failure
11.	Technical software failures or errors	Bugs, code problems, unknown loopholes
12.	Technological obsolescence	Antiquated or outdated technologies

Table 3.1 Category and Description of information security threat.

Whitman and Mattord (2004: 47) suggest that the list of threats, described above, may be manifested as deliberate attacks against an organisations assets whereby a vulnerability is exploited. The authors describe vulnerability as an identified weakness of a controlled system in which necessary controls are not present or are no longer effective. Whereas attacks may exploit vulnerabilities in information systems resulting in losses to an organisation, it is critical that organisations do not lose sight of inadvertent threats or non-malicious threats to information system that may be as damaging as deliberate attacks, to an organisation.

- **Inadvertent Threats**

  Although hostile and deliberate attacks on information systems receive much publicity, there is often little exposure given to unintentional / accidental threats to information systems. Inadvertent information security breaches may be the result of poor staff training and / or inadequate enforcement of information security policies. Ultimately this may suggest ineffective operational management policies.

The way people conduct themselves is critical when it comes to building and maintaining a secure Information System. Companies and organisations are investing vast sums of money to install state of the art security systems which include fire-walling, Virtual Private Networks (VPN's), sophisticated switching and routing equipment as well as up-to date anti-virus software. Justifiably, much attention is given to the outside risk and threats posed by so called hackers or people who break into an organisations network infrastructure. This security is all in vein, however, if employees within an organisation ignore internal security policies. There are numerous documented case studies describing companies that have suffered information violations through staff members handing around / sharing computer system passwords. Whitman and Mattord (2003: 45) argue that employees constitute one of the greatest information security threats because they have access to the organisations data on a daily basis. An employee may forget to collect a classified document off a shared printer, potentially resulting in compromised strategic information. Another employee may inadvertently delete a directory on a file server or a table in a database, not realising the consequences of critical, data loss. A third employee may loose his/her laptop through theft out of a motor vehicle. The replacement cost of a stolen laptop may be inconsequential when compared to the repercussions of critical data loss and possible espionage.

Threats may also be caused by *force majeure* commonly known as the forces of nature or acts of God. These threats may be unanticipated such as fires, floods, earthquakes and lightening.
Part of the difficulty in planning for these threats is that human lives are often impacted as well, making the recovery process a lot more difficult.

Threats also come about as a result of technical failure. A computer hard-disk may cease to function, commonly known as a "crash", causing downtime in an Information System. While technical staff source and replace faulty components, services that are not duplicated may have to be suspended. Inadvertent threats may also be caused by poor performing service providers. This could range from an electricity supplier providing unstable, erratic electricity, ultimately damaging hardware components, to a service provider who miss configures a router resulting in lost data packets and no

communication with the "outside world". Service Providers provide the means for small, medium and large organisations to connect to the Internet.

3.5 Deliberate Attacks

Deliberate attacks are pre-meditated attacks against information systems that occur either from outside or inside an organisation. External attacks may originate from Malware (malicious software), hackers (people who accesses computer networks to steal, corrupt, extort), script kiddies (novice hackers who uses hacker tools and scripts to disrupt / corrupt), former employees, espionage, adversaries, terrorists. There are two types of hackers: expert hackers and unskilled hackers. Panko (2004: 37) defines hacking as "intentionally (using) a computer without permission or beyond authorized permission". Expert hackers are usually highly skilled deviants who hold a different set of values and beliefs. According to Panko (2004: 37) hackers may see attacking a corporation as their civil duty in order to benefit society by keeping greedy "corporates" on their toes. Skilled hackers often develop scripts and codes which are then used as tools to break into systems. Whitman and Mattord (2003: 49) refer to skilled hackers as extremely talented individuals with high levels of skills who will stop at nothing to break into a 'chosen target' site.

Internal attacks may originate from management, employees, consultants, contract workers, maintenance crew, and temporary staff. According to Volonino and Robinson (2004: 42), a third type of attack may be an external threat with internal intervention. This takes place when an external attack is aided or facilitated by an insider. Before exploring some of the different methods used to orchestrate an attack, the reasons and motives for these attacks are discussed. Volonino and Robinson (2004: 43) refer to *deliberate and directed attacks* as well as *deliberate but random attacks* and site the following as possible reasons:

Deliberate and Directed	Deliberate but Random
Focused attack by an adversary	Malware
Focused attack for financial gain	Script kiddies
Focused attack for revenge or mischief	Proof of concept
For fame or notoriety	

Table 3.2 Sourced from Volonino and Robinson (2004)

According to Volonino and Robinson (2004: 35), the intent or motive of the Intruder may be:

- Political or military objectives
- Retaliation or vengeance
- Ideological objectives
- Financial gain, extortion or blackmail
- Curiosity or the thrill of vandalism
- Competitive advantage
- Focused attack against security companies for trophy hunting

Different methods are used to launch attacks on organisations.

- **Malicious Code**

  Whitman and Mattord, (2004: 65) describe malicious code as the execution of software written for the purpose of destroying or undermining information systems. Examples of malicious code are viruses, worms, Trojan horses and active Web scripts.

  According to Panko (2004: 499) a virus is "a piece of code that attaches itself to a file (file-infector) or, infrequently, to a sensitive system sector of the victim computer's hard disk; malware that infects files and spreads when the file executes or is executed by another program". Worms on the other hand are autonomous attack programs that spread themselves to other computers without human intervention. (Panko 2004: 500). Volonino and Robinson (2004:40) describe a Trojan as an enticing, harmless-looking piece of software or software program that when executed, can damage / destroy data and computer hardware. Trojan's are mostly sent as attachments via email. Users pick on the attachment file which executes the Trojan horse, which in-turn propagates to other computers. According to Volonino and Robinson (2004: 40), certain dangerous Trojan horses set-up what is known as a 'backdoor' on victim computers. This backdoor provides computer hackers with the means to illegally access the victim computer, in the process circumventing all security. Once these hackers have gained illegal access, they can steal, damage, destroy data on the computer or stage further attacks on 3rd party systems. Web scripts are programs created and used by

hackers that are posted up on Web sites. A user may inadvertently browse an infected web site or alternatively receive email enticing the user to visit a malicious Web site. Once the user picks on the infected site, stealth downloads are activated in which malicious code is sent down to the users computer, causing damage in the process. Although companies have put policies in place that prohibit staff from opening un-scanned email attachments and or surfing the Net, according to Wylder (2003: 29) surveys have indicated that nine out of ten employees are likely to open an email attachment without questioning it's source or authenticity. This happens despite numerous security initiatives such as:

- Security policies in employee handbooks
- Self-study course attendance prior to being allowed to logon to the network
- Annual testing of security awareness
- Campaigns, posters, Web and e-mail reminders

People still abuse and disregard their company security. Stronger user awareness programs and greater involvement from top management are still seen as chiefly important. (Wylder 2003: 29)

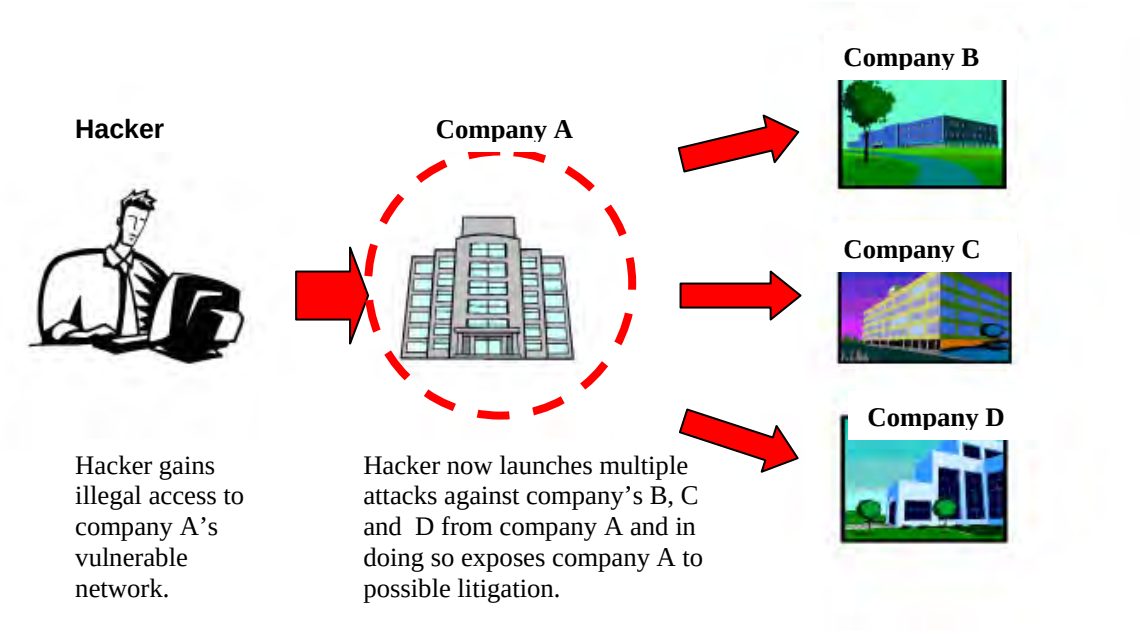


Fig 3.1 Diagram of hacker gaining illegal access to company A's network and then mounting attacks on company B, C and D.

- **Back Door**

  Back doors are either installed by malicious software, as discussed in the previous section, or they may be configured by an administrator or someone with administrator rights. According to Volonino and Robinson (2004: 40) "backdoor's are used for quick remote access because they circumvent most security defences". There have been cases reported in which disgruntled administrators have setup backdoor accounts, prior to leaving an organisation. This backdoor access has then been used for remote illegal access which has resulted in tampering, theft or destruction of data.

- **Password Crack**

  Password cracks consist of hackers attempting to gain illegal access to a system by guessing and / or calculating a password. There are several ways in which a hacker can go about obtaining a password to access a system:

  - dictionary attacks
  - brute force attacks
  - man in the middle attacks

  According to Whitman and Mattord (2004: 45) dictionary attacks occur by narrowing down the target accounts and then trying out several commonly used passwords instead of random combinations. An example of such an account may be guest or administrator. Brute force, as the name implies, refers to the application of "computing and network resources to try every possible combination of characters to crack a password" (Whitman and Mattord, 2004: 45)

- **Man-in-the-middle**

  Man in the middle or TCP/IP hijacking attacks take place when the attacker manages to gain access to a network and intercept data that is communicated from one network node, (such as a computer), to another (such as a server). By intercepting IP packets, modifying them, and inserting them back onto the network, the attacker appears to be the legitimate other computer. According to Whitman and Mattord (2003: 68), attackers are then able to change, delete, reroute, add, forge, or divert data. Hackers are able to gain access to passwords using this technique.

- **Denial of Service (DoS) and distributed denial-of-service (DDoS)**
  A Denial of Service or (DoS) attack is launched against an organisation by flooding their network infrastructure with continuous requests for information or connections. This results in the network being swamped and unable to service legitimate network requests, which in-turn means the organisation is unavailable or off-line. During 2001, certain virus's such as Code Red and Nimbda clogged the Internet, causing 40% more traffic. According to Volonino and Robinson (2004: 5) the estimations in expenditure to reverse the damage caused by the Code Red and Nimbda DoS attacks amounted to $3 billion.
- **Spoofing**
  Spoofing involves sending network-level messages to a computer with an IP address indicating that the message comes from a trusted host. (Whitman and Mattord, 2004: 67). Put differently, spoofing amounts to a hostile computer masquerading as a legitimate, trusted computer by tampering with the IP address of packets so that they appear to come from a legitimate, trusted source. Spoofing is sometimes used with email messages where the source address is altered so that the messages appear to come from somewhere / someone else.
- **Social Engineering**
  Social engineering may be considered a more passive and cunning form of attack in which grace and charm is used by the attacker to convince the victim to reveal access credentials and other secure information. (Whitman and Mattord, 2004: 45)

During 2002, a mini-survey, Skoudis (2002), was conducted by information security magazine in an attempt to determine what respondents believed were the five (5) worst security attacks during the period 1997 to 2002. The survey did not target any particular group. According to Skoudis (2002) the survey revealed the following:

Five most damaging and disruptive attacks	Nature of attack
Code Red (2001)	Code Red exploited Microsoft Internet Information Server (IIS). Spread to over 250 000 un-patched Web servers within nine hours.

Nimda (2001)	A multi-exploit worm that compromised Microsoft Windows computers. Exploits included: - Flaws in Internet Information Server - Browsers with JavaScript enabled were redirected to an infected Web server - Outlook e-mail clients were infected - Activating Windows file sharing, enabling the guest account and adding guest to the administrator's group
Melissa (1999) and LoveLetter (2000) Melissa was a Microsoft Word macro virus and LoveLetter a VBScript virus.	Spread by an application-level scripting language and propagated primarily via Outlook attachments. When activated, the virus propagated through a victims email address book, spreading exponentially. Both these threats brought down email systems at many companies.
Distributed Denial-of-Service (DDos) (2000)	Zombie flooding agents were used to launch attacks against various sites using packet flooding techniques. Amongst the high-profile sites targeted were: Amazon.com, CNN, E*Trade, ZDNet, Buy.com. Effectively these sites were 'closed-down' for the duration of the attacks.
Remote Control Trojan Horse Backdoor (1998 – 2000)	The Trojan horse installed a backdoor on Windows 95/98/NT target machines allowing a remote attacker to gain full access to these machines. Back orifice was an example of one of these Trojan

	horses. Some users willingly installed Back orifice believing that it would facilitate remote administration. They did not take into account the external vulnerability.

Table 3.3 Five (5) most disruptive attacks between 1997 and 2002 according to Skoudis (2002)

According to Skoudis (2002) lessons learned from the attacks were:

- Microsoft released security bulletins with the associated software patches for their Internet Information Server (IIS) software well in advance of the worm attacks. Poor systems administration meant that organisations failed to apply the patches to their systems. This effectively meant that these organisations were running 'outdated' vulnerable software that contained security flaws.
- There is a need to have incident-response capabilities linked to network management personnel so that an attack such as Nimda can be identified quickly, and the requisite controls applied to prevent further spread of an attack.
- Organisations must hold their systems administrators accountable for constantly monitoring security bulletins and regularly updating and fine tuning their systems. Software and hardware updates not only apply to back-end servers such as Internet Information Server (IIS) but also client desktops. Various exploits have been launched through script execution in e-mail clients and Web browsers. It is vital that systems administrators install and maintain high quality anti-virus software on both servers and client desktops.
- Organisations must work closely with service providers such that in the event of suspicious network traffic as found in Distributed Denial of Service Attacks (DDOS), they can illicit a fast response from their service providers, rerouting or filtering traffic to minimise the impact of such an attack.
- Organisations must create security awareness so that users think twice before inadvertently open file attachments without being fully appraised of the origins and content of such an attachment.

3.6 SME's and Security

SME's are borne out of entrepreneurs who in order to survive, typically collaborate and network well within informal structures, often sub-venting formal traditional 'barriers to entry'. By collaborating within and beyond the confines of their organisations, entrepreneurs form transnational networks that rely heavily on interconnectivity and computer based information systems.
Increased usage of information and communication technologies has led to increased incidents of computer abuse. (Dhillon and Backhouse, 2000: 125)

Both SME's as well as large businesses make use of service providers to connect to the outside world. Besides basic Internet connectivity, service providers offer a variety of additional services. The list below, by no means exhaustive, contains some of the services typically offered by service providers:

- Network connectivity to the Internet including IP address leasing
- Routing and network traffic management
- Web site hosting and the management thereof
- Computer fire-wall security
- Email services
- Back-up services
- Computer desktop management

While large organisations may benefit from the scale of economy gained through installing their own technical infrastructure and staffing posts to run their infrastructure, SME's normally lack the capacity to do this. As a result, there is a strong tendency by SME's to outsource additional services such as those mentioned above. Outsourcing all or part of a businesses information system may be the most cost effective way of managing information security. (Geiger and Wegman, 2002). Ploskina (2001) in Geiger and Wegman (2002), caution however, that there has been much instability amongst service providers and firms offering managed security. Entrusting vital information and security to a firm that may disappear or be taken over, resulting in a lapse in their Quality of Service (QOS) agreement, could have dire consequences for a business. (Ploskina 2001 in Geiger and Wegman 2002) An SME may believe they have adequate protection but could find them vulnerable to a

security violation or in the worst case, unable to recover from a disaster such as a fire or flood. Due to the informality of SME's, there is often a lacking in procedures and documenting processes. Service Level Agreements (SLA's) may not be properly drawn up / fully understood, rendering an SME powerless in the event of a non-performing service provider. A further vulnerability that many SME's suffer from is a lack of staff training. Staff members are often expected to 'muck-in' and do what it takes to get the job done. Because of the size of an SME, people tend to know and trust one-another more readily. Although informal relationships and processes may characterise the way small businesses function, ultimately the information security in these small businesses may be negatively impacted

In a survey of trends and practices in data storage, backup and disaster recovery in 3000 small businesses, Special Report, Imation Small Business Survey (2003), the following security risks were identified:

- **E-mail viruses are a greater concern to small businesses than natural disasters or terrorist attacks**

  National threats seem to pose little impact on small business data backup and storage practices. According to the survey, less than one in ten small businesses responded to the events of 9/11 by reviewing or changing their data backup and storage procedures. Yet, more than one in four small businesses reviewed or changed their data storage backup procedures as a result of a major e-mail virus.

- **Many small businesses are at risk when it comes to protecting their data**

  Fifty-five percent of small businesses rated themselves as "fair" or "poor" when it came to having a documented disaster recovery plan and many denied having a documented disaster recovery plan at all. 30 percent of small businesses admitted that they had no formal data backup and storage procedures, or did not implement their procedures consistently.

- **Review and evaluation of data backup and storage procedures is not a common practice among small businesses**

  The majority of small businesses reported backing up critical data on a daily basis, with daily backups more common amongst companies that deal with higher volumes of data. One in three small businesses still wait until there is a problem

before reviewing and evaluating their backup and storage procedures.
21 percent said that they were doing a "fair" or "poor" job of periodically removing important business data offsite – a vital procedure to protect businesses from physical disaster. An additional 13 percent of small businesses admitted to not removing backup files at all. This amounted to 34 percent at risk.

- **Small businesses use tape and optical media as their primary backup and storage technologies**

  The top two platforms cited by small businesses as their primary backup technology were data tape cartridges and optical discs. Sixty-three percent of small businesses claimed to use tape as their primary backup technology, while 14 percent reported using optical technologies like CD or DVD. 12 percent of businesses reported using floppy disks as their backup medium.

3.7 Conclusion

Information Systems form a vital part of any modern organisation. Successfully managing systems implies that security risks are understood and the appropriate interventions introduced. Security threats may be classified as inadvertent or deliberate. Although deliberate attacks are often launched from outside an organisation, they may also be facilitated or conducted from within an organisation. Staff involvement and or negligence should never be ruled out. Of particular importance to organisations, is the liability that they may face should private or sensitive information be compromised through a security breach. Staff training and awareness is thought to be critical in this regard. Whereas large organisations may have the capacity to hire-in expert staff to maintain their information system security, SME's usually do not. This may result in SME's opting for off the shelf technical solutions, in the process neglecting softer security issues as mentioned above. SME's that choose off the shelf solutions must never loose sight of the need to constantly upgrade and fine-tune systems in order for them to remain reliable and secure. Although outsourcing information security may be the only viable option for SME's, it is critical that service levels between the organisation and the service provider are well specified, understood and monitored. Ultimately, the responsibility for information security lies with the management of an organisation.

Chapter 4: Risk Analysis and Security Controls

Abstract

Chapter 3 explored various information security threats facing organisations, and suggested that inadvertent threats are often overlooked and underrated when the security of an organisation is being considered. This chapter examines some of the processes that organisations should consider when reviewing their information assets. This includes identifying threats and vulnerabilities that place assets at risk, initiating or updating security controls to mitigate against security threats and vulnerabilities, while not forgetting about the costs and benefits associated with the necessary interventions.

4.1 Introduction

Volonino and Robinson (2004: 63) suggest that information security, like any business problem, should receive a measure of analysis to determine risk and consequences. It is essential that organisations properly understand what it is they are protecting and why Shaw (2002) suggests that due to resource constraints, risk analysis has traditionally been performed by larger, better funded commercial and government organisations. He argues that risks analysis is seen to be complex requiring specialist expertise, and for this reason has been outsourced or even neglected in many small to medium sized businesses.

This chapter describes the risk analysis process in general and investigates risk analysis options available to SME's in particular. Volonino and Robinson (2004: 63), Shaw (2002) and Whitman and Mattord (2003: 162) agree that the risk analysis steps include:

- Impact: Measuring the likely impact of a security breach
- Value: Determining and valuing different categories of information such as financial, personal, legal and regulatory, management and operational
- Threats: Identifying the wide variety of threats that may affect the environment
- Vulnerability: Determining the vulnerability of the systems given the identified threats
- Controls: Selecting the appropriate controls to counter the identified risks

- Costs: Ensuring that the costs involved are justified and do not outweigh the benefit gained by controlling the risk.

Although outsourcing the risk analysis process may be an only option for SME's, SME management are ultimately responsible for the security of their Information assets and need to engage in the process.

4.2 Determining Threats and Vulnerability

According to the South African Standard Information technology – Code of practice for information security management, SABS ISO/IEC 17799 (2000), risk assessment is the systematic consideration of:

- The business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;
- The likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

Michalson (2003: 44) refers to risk assessment as "determining the threats to information assets and the degree of vulnerability. Volonino and Robinson (2004: 66) suggest that risk analysis is intended to fully identify and assess risk factors, and then to balance the expected costs (damages) of incidences with the cost of defences needed to avoid incidences. The South African Standard Information technology – Code of practice for information security management, SABS ISO/IEC 17799 (2000), concurs with this view and suggests that expenditure on risk assessment controls needs to be balanced against the harm likely to result from security failures. According to the standard, risk assessment techniques can be applied to the whole organisation, part of the organisation or even individual information systems within an organisation. According to Barnard and von Solms (2000: 185), the accepted standard or practice of introducing Security in an IT environment is to identify, introduce, manage and maintain an effective set of security controls in the organisation. They suggest that given the need for a minimum level of security, the use of base line manuals may eliminate the need for an in depth analysis. The authors do warn, however, that given the need to assess organisations individually, some evidence of business analysis is required, especially to determine the degree of

dependency on information security which in turn dictates the level of security requirement.

4.3 The Nature of Assets and Risk

Peltier (2001: 37) suggests that formal risk analysis provides management with the proof that "due-diligence" has been performed. He argues that a thorough risk analysis leads to an organisation implementing controls and safeguards that are genuinely needed, and suggests that there are several tasks common to most risk analysis methodologies which include:

- Identifying the asset to be reviewed
- Ascertaining the threats, risks, concerns, or issues relating to the asset
- Prioritising the risk or determining the vulnerability of the asset
- Implementing corrective measures, controls, safeguards, or accepting the risk
- Monitoring the effectiveness of the controls and assessing their effectiveness

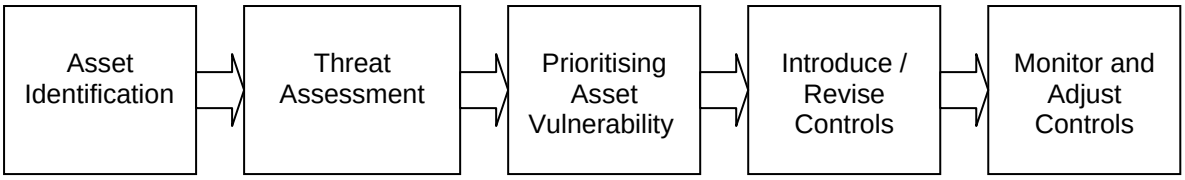


Fig 4.1 5 Stages of the Information Risk Assessment Process

Both Peltier (2001: 37) as well as Volonino and Robinson (2004: 73) make reference to two types of assets. These are *Physical Assets* or those that can be seen, and *Logical / Digital Assets*, commonly referred to as the intellectual property of the organisation. Volonino and Robinson (2004: 73) suggest that physical assets often only exist in one place and therefore need only protection in one instance. They suggest, however, that digital assets are often protected by retaining multiple copies of the asset which ironically introduces additional security difficulties such as the opportunity for theft. They cite examples of physical assets being computer hardware and building infrastructure. Due to the nature of these physical assets, calculations for

determining loss and replacement costs are said to be relatively easy to determine. Digital assets according to Volonino and Robinson (2004: 73) are considered more complicated however and may be broken down into Software assets, Knowledge assets and Goodwill.

The risk associated with software assets may have little to do with the software itself, which according to Volonino and Robinson (2004: 74) can usually be reinstalled off backups or source material. It is rather the down-time or lost revenue associated with a system being unavailable that causes losses and therefore the greatest risks. Volonino and Robinson (2004: 76) cite the example of a Web storefront that may go off-line due to software corruption, and the loss in revenue associated with the on-line store being off-line or "closed for business" as it were. Cowley (2001: 2) provides insight into this type of disruption referring to the terrorist attacks on the World Trade Centre in New York during September 11, 2001. Several on-line businesses based in New York that were dependent on damaged Network switching infrastructure, housed in or close to the World Trade Centre, were unable to conduct business for several weeks, despite there being neither physical harm to personnel nor the equipment belonging to these organisations.

A further example offered by Volonino and Robinson (2004: 76) is software that is installed to enhance productivity. If a software system fails, then whatever margin of productivity the system is said to deliver, multiplied by the duration of downtime of the system, will be the total loss.

In referring to Knowledge assets, Volonino and Robinson (2004: 72) suggest that it is unique knowledge and data within an organisation that creates the greatest risk. When the security of a database is compromised and possibly 'hacked', if the database has been correctly backed-up, it may be easily restored. If information is stolen from the database, it is this stolen information that potentially provides the greatest risk to the organisation. It is what attackers or hackers do with stolen information from a database, that may render an organisation most vulnerable. Breached customer confidential information may result in the organisation facing litigation or punitive measures, especially if it can be proven that the organisation has been reckless or negligent in protecting this information. Personnel working within

an organisation contain an enormous amount of knowledge about the organisation. This knowledge spans activities from customer to supplier details, and from operational activities through to strategic intent. Knowledge management is the discipline of identifying, capturing and embracing the value of knowledge held by individuals and groups within an organisation. Human knowledge is one of the most valuable and volatile forms of assets found in the organisation.

Goodwill is considered to be an extremely valuable asset, especially in service orientated businesses where it is largely as a result of accumulated knowledge, experience, public image, and body of customer relationships the firm has developed over its lifetime. (Volonino and Robinson 2004: 73). According to them, the more an organisation depends on technology to manage its knowledge and face its markets such as a bank or major on-line store, the more vulnerable the organisations goodwill will be to digital assault. A well known, highly traded, on-line store such as Amazon.com, that suffers a security violation rendering customer confidential information at risk, will be highly exposed to goodwill risk. An on-line shopper may think twice about entering credit card details on an unknown retail web site, however, the goodwill surrounding on-line stores such as Amazon.com is such that private individuals and businesses may feel at ease in transacting on-line with these concerns. The same type of goodwill is said to apply to the major banking institutions as well.

4.4 Asset Vulnerability

Once the nature of the Asset type is understood, the organisation needs to implement a process of determining how critical an asset is to the well being of the organisation and to what extent the loss or violation of a particular asset would impact the business.

Whitman and Mattord (2003: 128) recommend that an organisation answer several questions in an attempt to determine the critical nature of a group of assets. Examples of some questions are listed below:

- Which information asset generates the most revenue?
- Which information asset generates the most profit?
- Which information asset would be the most expensive to replace?
- Which information asset would be the most expensive to protect?

- Which information asset would be the most embarrassing or cause the greatest liability if a violation was revealed?

Whitman and Mattord (2003: 129) suggest that the organisation weigh each asset based on the answers to the chosen questions and then list the assets in order of importance by using a weighted factor analysis worksheet. An example of a weighted factor analysis worksheet is illustrated below:

Nature of the risk to the organisation, that is, in what sense would the organisation be impacted by a security breach. The criteria weightings must add up to 100. Must decide which criteria carries more weight i.e. more impact on the organisation. *(Criterion n1 + Criterion n2 + Criterion n3 = 100)*

Description and operational context of the Information Asset being deployed

	Criterion 1: *e.g. impact on revenue*	**Criterion 2:** *e.g. impact on profitability*	**Criterion 3:** *e.g. impact on public image*	**Weighted score**
Criterion Weight (1-100) Must total 100	**30**	**40**	**30**	(100 total)
Information Asset 1 *Description and Operation context* (between 0 – 1)	*To what extent would the loss of Asset 1 impact on the organisations revenue?* *(e.g. high, 0.8)*	*To what extent would the loss of Asset 1 impact on the organisations profitability?* *(e.g. med, 0.5)*	*To what extent would the loss of Asset 1 impact on the organisations public image?* *(e.g. low, 0.2)*	Weighted score: (0.8 X 30) + (0.5 X 40) + (0.2 X 30) ---------- 50
Information Asset 2 *Description and Operation context* (between 0 – 1)	0.8	0.9	0.6	78
Information Asset 3 *Description and Operation context* (between 0 – 1)	0.4	0.5	0.3	41
Information Asset 4 *Description and Operation context* (between 0 – 1)	0.9	0.9	0.8	87 (Indicates asset needing the greatest attention)

Table 4.1 Weighted Factor Analysis worksheet

An example of a weighted factor analysis worksheet can be found in Table 4.2. The table determines the impact on the organisation of loosing one or other Interchange documents, either Electronic Data Interchange (EDI) or Secure Sockets Layer (SSL), using revenue, profitability and public image, as metrics.

	Criteria 1: Impact on revenue	Criteria 2: Impact on profitability	Criteria 3: Impact on public image	Weighted score
Criterion Weight (1-100) Must total 100	**30**	**40**	**30**	
EDI Document Set 1-Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2-Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2-Supplier fulfilment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Table 4.2 Weighted Factor Analysis

Note: EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Referring to the table above, the Customer order via SSL (inbound) data flow is the most important asset on the worksheet, and the EDI Document Set 2-Supplier fulfilment advice (inbound) is the least critical.

4.5 Threat Assessment

Having identified each of the Information Assets and determined the most critical and least critical nature of each asset, each of the twelve (12) information security threats need to be assessed against each asset. This process leads to the organisation's risk assessment which in turn feeds into the introduction of controls.

Whitman and Mattord (2003: 138) refer to twelve (12) major information security threats. (detailed in Chapter 3)

- Deliberate software attacks
- Acts of Human Error or Failure
- Technical software failures or errors
- Technical hardware failures or errors
- Quality of service deviations from service providers
- Deliberate acts of espionage or trespass
- Deliberate acts of theft
- Deliberate acts of sabotage or vandalism
- Technical obsolescence
- Forces of nature
- Compromises of intellectual property
- Deliberate acts of information extortion

Whitman and Mattord (2003: 139) propose using a table with the list of 12 information security threats down the left hand column and the possible vulnerabilities to the asset being assessed, down the right hand column. (See Table 4.3).

Heading: ***Asset being assessed***

	Threat *List of 12 information security threats below.*	**Possible Vulnerabilities**
1.	Deliberate software attacks	Itemised list of possible vulnerabilities to the asset given the nature of the asset and the category of threat
2.	Act of human error or failure	Itemised list
3.	Technical software failures or errors	Itemised list
4.	Technical hardware failures or errors	Itemised list
5.	Quality of service deviations from service providers	Itemised list
6.	Deliberate acts of espionage or trespass	Itemised list
7.	Deliberate theft	Itemised list
8.	Deliberate acts of sabotage or vandalism	Itemised list
9.	Technical obsolescence	Itemised list
10.	Forces of nature	Itemised list
11.	Compromises to intellectual property	Itemised list
12.	Deliberate acts of information extortion	Itemised list

Table 4.3 Asset Vulnerabilities

The output of the process described above should be a list of assets and their vulnerabilities. (Whitman and Mattord, 2003). This list now feeds into the Risk Assessment process.

4.6 Risk Assessment

Having identified the information assets, and assembled a list of security vulnerabilities, a risk assessment needs to be carried out so as to pinpoint the appropriate controls that can be introduced to protect these threats. Risk assessment is the process of assigning risk ratings or scores to each specific information asset based on their threats and vulnerabilities. (Whitman and Mattord 2003: 142). According to Whitman and Mattord (2003: 142), risk equals likelihood of vulnerability occurrence times Value (or impact) minus percentage risk already controlled plus an element of uncertainty.

Risk = (Likelihood of Vulnerability **X** Value) **–**
% Risk already controlled + element of uncertainty

They suggest that by the end of the risk assessment process, the following should be available:

- Lists of information assets and associated vulnerabilities
- Existing controls that are in place

Finally, the ranked vulnerability risk worksheet needs to be created. This document combines the Asset detail, Asset impact, Vulnerability, Vulnerability likelihood and the Risk-rating factor. Not dissimilar to the ranked vulnerability worksheet referred to by Whitman and Mattord (2003: 142), is the Risk Assessment Cube, proposed by Volonino and Robinson (2004: 66). The Risk Assessment Cube is illustrated in Figure 4.2.

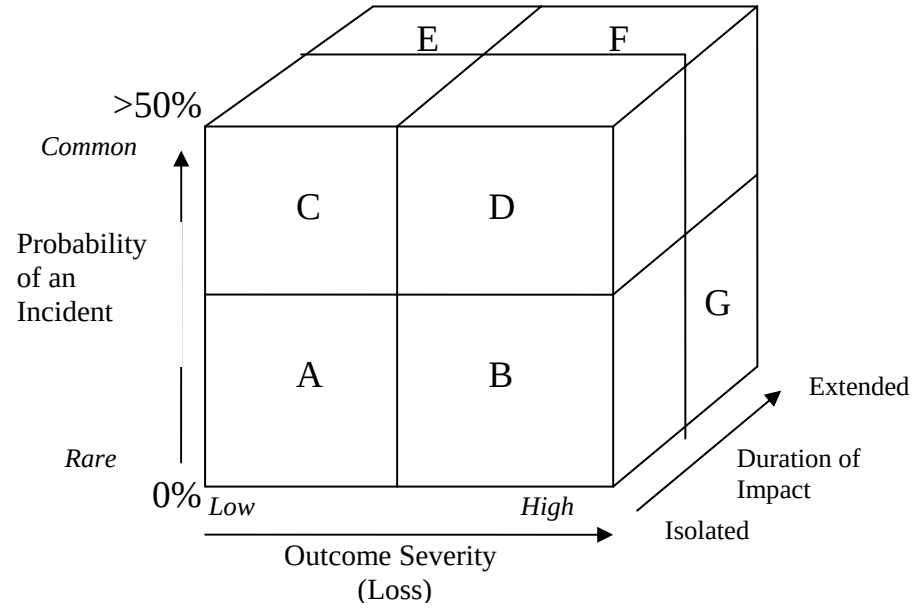


Fig 4.2 Volonino and Robinson's Risk Assessment Cube

The risk assessment cube is a 3 dimensional cube used to define risks along 3 different axis. These are:

- The probability of an incident

  This refers to the likeliness or frequency of an incident. According to Volonino and Robinson (2004: 66), probability ranges from 0 to 100% or from rare to common.

- The severity of the outcome or loss. This refers to direct and indirect financial impacts should an incident occur. The range is from low to high.
- The duration of the impact. This refers to isolated incidents that can be contained, to those that extend over longer periods of time, such as a company losing critical data that has to be manually recaptured over time. A confidentiality breach may ultimately result in customer loss. This would almost certainly turn into a long term impact.

Referring to the risk assessment cube, (Figure 4.2), and the risk assessment table, (Table 4.4), an asset placed in segment 'A' of the cube, would have a low likeliness of suffering an incident in the first place, but would be considered to have a low outcome severity for a short period of time, should an incident actually occur.

An information asset that is mapped to segment 'F' on the cube, is thought to run a high incident risk and should an incident occur, would be both severe and disruptive for an extended period of time.

Segment	*Probability of an Incident*	*Severity of Outcome or Loss*	*Duration of Impact*	*Examples* *(vary according to industry and company attractiveness)*
A	Rare	Low	Isolated	Retaliation or vengeance, civil lawsuit brought by an employee for harassment or discrimination
B	Rare	High	Isolated	Non-sophisticated hacker or DOS attacks, criminal or class action lawsuits for negligence or violation of employee civil rights
C	Common	Low	Isolated	Spam and some malware, possession of unlicensed software
D	Common	High	Isolated	Disruptive or destructive malware
E	Common	Low	Extended	Electronic fraud or extortion
F	Common	High	Extended	Insider theft and exposure of confidential financial, customer, or competitive information
G	Rare	High	Extended	Non-recoverable disruption of customer databases or other mission-critical systems.

Table 4.4 Risk Assessment Cube Table

4.7 Risk Interventions

The final stage in the risk assessment process involves examining existing controls, should these already exist, and revising or instating new controls to cater for the asset risk identified in the previous steps. A cost-benefit analysis may be used so that the costs for the suggested safeguards can be weighed up against the level of protection inherently offered by these controls. Ultimately the business has to justify the investments in defending against security breaches. Various methods may be used for managing this business risk. According to Volonino and Robinson (2004: 66) and Whitman and Mattord (2003: 142), the three most common methods for doing this are:

- Avoidance by implementing preventative measures and safeguards.
- Risk transferral to another party by outsourcing the secure management of a network, mission-critical databases, or e-commerce application. Transferral may also include purchasing insurance to cover losses in the event of a security breach. The cost of this approach will depend on security investments and audits that the organisation has already implemented.
- Mitigation by reducing the impact should a vulnerability occur.
  Whitman and Mattord (2003: 160) suggest three mitigation strategies which include a number of plans:
  - Disaster Recovery Plan (DRP)

    The DRP involves planning and documenting a comprehensive recovery strategy in the event of a disaster. This strategy includes limiting losses before and during a disaster, and planning for the immediate post disaster recovery period.
  - Incident Response Plan (IRP)

    Whereas the DRP looks more at overall disaster management including pre and post disaster planning, the IRP details who should take what actions in response to an incident. Whitman and Mattord (2003: 160) use the example of a systems administrator realising that someone has gained illegally access to a file server, and is copying data from the server. The IRP would involve the specifics of what the systems administrator should do. These details would include, what to do first, whom to contact and what should be documented

The Incident Response Plan enables the organisation to take predefined, organised action that has been properly thought through. It avoids inconsistent, ad-hoc decision making.

- Business Continuity Plan (BCP)

The BCP looks beyond the periods during and immediately after an incident, and considers how the organisation will make a long term recovery. This plan may include relocating a business, setting up a hot-site or business recovery site, which is a remote location with systems identical to a home site.

- Acceptance by taking no action. This refers to the choice / decision that management take to do nothing in terms of protecting a particular vulnerability and accepting an outcome. Acceptance is considered to be a valid strategy providing:
  - The level of risk has been determined
  - The probability of attack has been considered
  - An estimation of potential damage from attacks has been considered
  - A cost benefit analysis has been performed
  - Controls have been evaluated using each type of feasibility
  - Decision has been taken that a particular asset, service, information or function did not justify the cost of protection

4.8 Risk Controls

Acording to Whitman and Mattord (2003: 222) controls are measures taken to assist in avoiding, mitigating and transferring risk. They may be categorised according to:

- Control function

  These are either preventative or detective in nature. Preventative controls stop the exploitation of a vulnerability whereas the detective controls are used to warn the organisation of a violation. These would include an audit control.

- Architectural layer

  These may be classified according to the layer's in which they provide security. The example of a firewall is used in which the controls operate at the external network and the extranet or between an organisations LAN and WAN. Other

controls may be at the organisational policy level where the controls describing password usage and format are specified.

- Strategy layer
  Controls may be classified by the risk control strategy they operate within: avoidance mitigation, or transference
- Information security principle
  These are the more commonly accepted information security principles which include:
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Authorisation
  - Accountability
  - Privacy

Benchmarking according to Whitman and Mattord (2003: 176) is another popular method used for gauging and implementing security. Benchmarking involves seeking out and studying practices used in other similar organisations that produce the desired results in ones own organisation. There are certain benchmarking standards available for organisations, referred to as best practices. Attached to these best practices are the controls and policies that must be implemented to achieve these best practices. Although benchmarking and best practices are considered very useful, they may fall short in organisations that are not prepared to admit failure, and as a result, may not report on a security weakness or compromise. Benchmarking may excessively generalise the organisation not adequately taking into account non-standard criteria / information assets. Base-lining is related to best practice in which a "value or profile of a performance metric against which changes in the performance metric can be usefully compared" (Whitman and Mattord, 2003: 177). Base-lining can set a standard by which an organisations future standard and performance may be measured.

Security may be implemented through the adoption and implementation of a security policy such as the South African Standard Information technology – Code of practice for information security management, SABS ISO/IEC 17799 (2000). Security policies are discussed in Chapter 6.

4.9 SME's, Risk Analysis and Security Interventions

SME's tend to be run on tight budgets with minimum staff that perform in a variety of roles and responsibilities. SME's typically do not have capacity to embark on complex security initiatives, but at the same time, entrepreneurs are continually looking to leverage any advantage the business may gain through implementing information systems and technology, and in some cases, E-Business. "IT security in small organizations is often a balancing act in which every persons actions can tip the scales" (Briney and Prince, 2002: 5). Risk analysis is not a deliberate SME strategy and although an SME owner / manager may consider data loss, the risks assessment process using a methodology as described in the previous section, is highly unlikely to occur. Formalised policies that would normally drive these processes are said to be lacking in the majority of SME's. This is supported by the PricewaterhouseCoopers DTI Information Security Breaches Survey (2004), in which only 34% of small businesses (1-49 employees) and 45% of Medium businesses (50 – 249) in the UK reported having formally defined and documented Information Security Policies. Information Security Policies include user policies about what users may do, and according to the South African National Standard, information security management systems, SANS 17799-2 (2003), quite often this results in users being able to do exactly what they choose to do. Klopper (2002) quotes research conducted by the System Administration, Networking and Security Organization, (www.sans.org). The SANS research highlights the four (4) worst mistakes committed by computer users. These are listed in descending order of prevalence below:

- Opening email attachments from unverified sources.
- Failing to install software security patches for commonly used applications such as Microsoft Office
- Downloading and installing games and screen savers from unknown sources

- Failing to run regular backups and or verifying the integrity of backups that have been made. This concurs with the Special Report, Imation Small Business Survey (2003) as discussed in Chapter 3.

Klopper (2002) suggests that by 2004, 50% of SME's that connect to the Internet and manage their own network security will experience Internet attacks. According to him, 60% of organisations will not even be aware that their systems have been intruded. Besides Firewalls for intrusion detection, it is also essential that SME's monitor incoming mail. He suggests that email attachments can provide the greatest risks for organisations. In an informal environment, that lacks acceptable use policies for staff, there is additional risk from staff improvising and providing their "own" technical infrastructure. An off-the-shelf wireless access point that is summarily plugged onto an existing network may provide a backdoor to an SME's information systems. A users who dials out of his/her network using a modem, may open up a critical security vulnerability to the organisation.

SME's often address issues that are seen to directly effect the business. According to the Special Report, Imation Small Business Survey (2003), email viruses have been a trigger for small businesses to address their anti-virus as well as their backup systems. 27% of the respondents claimed to have revised their backup processes after the Melissa virus attacks. According to the PricewaterhouseCoopers DTI Information Security Breaches Survey (2004), virtually every business surveyed, had implemented anti-virus software linked to systems that automatically download and provide the latest signature updates. This survey covers both large and small business.

4.10 SME's and Outsourcing

Through each stage of the risk assessment process, different approaches may be taken by organisations to ensure they not only understand information security risk, but also choose the best and most cost effective interventions to prevent security breaches. Although securing information is vital for any organisation, not all organisations, least SME's, have the resources to keep up with security risks and interventions. As mentioned in the previous section, many SME's are under-resourced with entrepreneurs already fulfilling multiple business roles such as procurement, sales and

marketing and financial management. For this reason, the option of outsourcing security to professionals becomes an attractive proposition although Endorf (2004: 17) warns that outsourcing is not without risk and should not be taken lightly. Table 4.5 summarises the advantages and disadvantages in retaining proprietary security personnel:

Advantages of proprietary security staff	Disadvantages of proprietary security staff
Knowledge and talent remain in-house with professionals who understand the organisations core-business	Financial impact to the organisation for staffing and retaining security professionals can be substantial
Employee security professionals can keep the company's best interest in hand because it directly reflects on their job security	The fact that an employee is internal does not guarantee that he or she can be trusted more than an external employee
Turnover amongst outsourcing staff is usually at a much higher rate than with internal employees	Employee staffing is less flexible. In emergency events, there may not be sufficient staff, and employees will have to work overtime, which can over-stress employees
Management control is much better when employees are used	

Table 4.5 Advantages and Disadvantages of proprietary security staff. (Endorf, 2004: 17)

According to Endorf (2004: 17), service providers benefit SME's as they tend to have a broader industry view through having a wider perspective on threats and attacks mounted against the other organisations they work for. The advantages and disadvantages in outsourcing security to service providers, is highlighted in Table 4.6:

Advantages to Outsourcing	Disadvantages to Outsourcing
Access to trained security professionals 24 / 7, 365 days per year	Highly confidential organisational information will be available to external associates
The company will not have to resource the hiring and training costs of security staff	Outsourcing staff may lead to internal staffing conflict due to perceptions of inequitable remuneration and loyalty between the two groups
Service level agreements (SLA's) should ensure protection against liability, should a security breach occur *(This is clearly dependent on SLA's being drawn up properly)*	Cultural challenges between the outsourced organisation and the internal organisation may lead to conflict. This may include conflict over the "way things are done" and internal processes.
Service providers offer the benefit of a broader industry view on security	
Staffing flexibility means that a non-performing external staff member can be changed more easily than an internal staff member	
Extra capacity in security staffing as and when needed may be more easily sourced from the service provider	

Table 4.6 Advantages and Disadvantages to outsourcing. (Endorf 2004: 18-19)

Within South Africa, numerous tiers of service providers exist, offering a wide range of services, ranging from basic dial-up connectivity and email through to managed servers and services. Backup administration may also be included as a service. A controlling body known as the Internet Service Providers' Association (ISPA) co-ordinates and facilitates communication and Internet policy in South Africa. ISPA currently boast 83 service provider members, ranging through small, medium and large service providers. A SME manager / entrepreneur may wish to gain access to basic Internet connectivity and an email account, which any South African service

provider could provide. Alternatively, a manager / entrepreneur may wish to buy-in a comprehensive service including Data management, Web hosting, a Fire-walling service, Real-time managed anti-virus protection and access to a hot-site, in the event of a site disaster. The larger service providers such as Internet Solutions, Telkom, M-Web and MTN Network Solutions are geared towards this more sophisticated end of the market. SME managers / entrepreneurs need to understand, that irrespective of the nature and complexity of the service they buy-in, they are ultimately responsible for identifying and prioritising their information assets, ensuring that their information systems are adequately protected.

4.11 Conclusion

Risk analysis is a process that organisations should adopt in order to identify their information assets, determine the nature of threats facing these assets, and prioritise, install and revise security interventions including the controls to protect these assets. SME managers should attempt to determine: which assets generate the most revenue, which assets generate the most profit, which assets would be the most expensive to replace, which assets would be the most expensive to protect and finally which assets would cause the most embarrassment / liability if compromised. Although tools such as a weighted factor analysis worksheet or a risk assessment cube are designed to assist management in determining the value and vulnerability of their assets, at best, it is probably only going to be medium sized enterprises that adopt these tools. Most SME management will, in all likeliness, use guess work to determine which interventions to adopt. These interventions may range from installing avoidance controls to protect assets, transferring the risk to a third party by outsourcing asset protection, adopting a mitigation policy to reduce the impact should a compromise occur. A manager may elect to simply accept the risk. Outsourcing information security may benefit a SME by affording the SME access to highly skilled security professionals with varied experience. Alternatively, SME management may prefer to adopt a best practice approach to information security and or combine this with base-lining. Irrespective of the approach taken, it is SME management who are ultimately responsible for ensuring that information assets are adequately identified, analysed, assessed, and protected.

Chapter 5: Legal, Governance and Personnel Considerations

Abstract

Chapter 4 explored ways in which an organisation may take stock of information assets, identify threats and vulnerabilities and initiate or update security controls to protect information assets. Chapter 5 examines the regulatory framework surrounding the protection and usage of information assets as well as governance and personnel considerations.

5.1 Introduction

Gordon (2003: 60) states that although information risk seems to grow, necessitating continuous assessment of information security procedures and practices, the role of the enterprise security programme extends beyond protecting assets against attack and financial loss. Of major importance, is the protection of information and the associated privacy rights relating to information. Information has a value for which people are prepared to pay. Protecting information assets from external or internal threats is vitally important. However, Tiller (2003: 2) suggests that companies are becoming selective about the form of security in which they invest. He uses the phrase 'proportionate security' and suggests that companies are becoming more discerning, investing in security solutions that support business objectives as well as company regulations and compliance. Regulations are on the increase with governmental agencies revising and introducing new legislation. The South African Electronic Communications and Transactions Act, (, ECT Act, 2002), prescribes a significant tightening up on the acquisition, storage and dissemination of information. It is not just the regulatory environment that should concern business as Michalson (2003: 43) points out, significant legal considerations are also associated with information security.

This chapter investigates the legal considerations companies must be aware of, and then explores some of the regulations with which they must comply such as the Electronic Communications and Transactions Act (ECT Act) of 2002 as well as the Promotion of Access of Information Act 2 (PROATIA) of 2000. Governance, although regulated by shareholders, is receiving increasing attention. Governance is

also explored together with personnel issues which are at the core of the legal, regulatory and governance issues.

5.2 Legal Considerations

According to Michalson (2003: 43), no single South African law deals exclusively with information security. He suggests that it is necessary to have an understanding of the various guides, best practices and relevant sections from existing statutes and the common law which impact on information security. Michalson (2003: 45) lists these areas of law as:

- The law of contract:
  The law of contract exists where information technology contracts such as outsourcing, service provision, application service providers and software licensing agreements impose security obligations on vendors and business partners. Increasingly, providers of these services are required to warrant against security vulnerabilities. Service Level Agreements (SLA's) would fit into this category.
- The law of delict:
  The law of delict is tested where the concepts of reasonableness and duty of care are relied upon to determine whether or not organisations have been negligent in not taking the necessary security precautions, or are liable for loss suffered where a party that suffered loss can prove this was caused by the other party's negligence, loss or damage. To cite an example, a hacker may illegally gain access to a company network (company A). The hacker may then use this network to launch an attack against another company (company B). This is illustrated in Figure 3.1. If company B is able to prove that company A's infrastructure was insecure and non-compliant with state of practice security, they may hold company A liable for whatever damage has been caused through the attack.
- The law of evidence:
  The law of evidence refers to forensic issues relating to information in electronic form which may have been modified or deleted in an attempt to hide evidence and

the taking of the necessary steps to ensure the reliability and admissibility of the electronic evidence will be maintained in a court of law.

- Common law fraud:
  Common law fraud is said to exist when individuals and or companies pirate or use illegal software.
- Computer related fraud:
  Computer related fraud, in terms of Section 87 of the Electronic Communications and Transactions Act (ECT Act) of 2002, is tested where the victim of an information security attack conducted by means of impersonation or spoofing, lay's a criminal charge of fraud against the attacker based on the attacker's attempt to mislead or misappropriate something of value.
- Common law privacy claims:
  Common law privacy claims exist where, for example, a person submits personal information to an organisation for a specific reason or purpose, and the organisation reveals the information to a third party who misuses the information, causing the person to suffer damage or loss.
- Cyber-crime:
  Cyber-crime is said to exist in any illegal act which involves a computer, whether the computer is an object of a crime, an instrument used to commit a crime or a repository of evidence related to a crime. It includes the statutory cyber-crimes set out in sections 85-88 of the ECT Act. The ECT Act is discussed in the following section, section 5.3 regulatory issues.

5.3 Regulatory Conditions

According to Michalson (2003: 42), two Acts in particular impact on the South African regulations governing information security. These are:

- The Electronic Communications and Transactions Act (ECT Act) of 2002
- The Promotion of Access to Information Act (PROATIA Act) of 2000

5.3.1 The Electronic Communications and Transactions Act

The ECT Act, 2002 has received much attention since it was signed into law on the 31 July 2002. The Act, according to Michalson (2003), provides far reaching legislation regarding the development of electronic communications and transactions in South Africa, and aims to promote consumer confidence in electronic transacting as well as online privacy. Disclosure requirements facing companies that trade on the web include:

- The nature of goods and services provided
- Return and exchange policies
- Privacy policies
- Stringent disclosure requirements

The Act highlights the liability facing on-line vendors in terms of payment systems. In the event of a fraudulent on-line transaction, an online vendor may be held accountable for damages if it can be proven that the vendor has not complied with provisions in the act, and failed to provide adequate transaction security.

The Act also specifies a seven (7) day 'cooling off' period in favour of consumers making on-line purchases. All electronic communication and advertising that is sent to consumers has to comply with spamming regulations, and mailing lists must give consumers an opportunity to unsubscribe. A consumer is entitled to request a vendor to disclose their source of information about the consumer. The Act is very strong on the collection, storage and dissemination of confidential information. This includes creating and securing databases. The Act specifies certain data collection principles that must be adhered to for the sake of individual and state security. (Michalson 2003).

Electronic signatures and communication are given legal status by the Act and contracts that have been concluded via email, are legally binding. Electronic information is now admissible in a court of law. The use of products that provide security via cryptology are regulated via the Act and cryptology vendors are required to register their products and services with the Department of Communications.

5.3.2 The Promotion of Access to Information Act

The Act was enacted on the 3 February 2000, to give effect to the Constitutional Court right to access information held by an individual, company or the State, for the protection of any right. In terms of the Act, every public or private entity in South Africa must publish a comprehensive manual. The manual must contain information such as company details, a description of the records of the company, as well as the means by which a record may be accessed. The Act gives effect to Section 32 of the Constitution, which provides that everyone has rights to access any information held by the State or any other person, where such information is required for the exercise or the protection of any rights. (Mostert, 2003).

5.4 Governance

"Corporate governance consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed" (Swindle and Conner, 2004). They suggest the three crucial elements of Corporate governance are: people, process and technology. The people element, according to von Solms (2001) is frequently overlooked, with managers / directors thinking if the problem is information security, the solution must be a technical one. According to von Solms (2001), there is a link between information security and Corporate Governance. He uses a transitive relationship, described as follows: The company board must ensure that reporting systems, both financial and accounting, are properly maintained with the appropriate systems of internal control in place, including independent auditors. This according to von Solms (2001) enables the board to effectively monitor company management, and ensure that the board is accountable to the company and shareholders. Von Solms (2001) quotes a Computers & Security article, author unknown, in which the author states, due to well publicised business failure, moves are afoot to hold directors and senior executives personally accountable for the consequences of failed internal controls, which in turn rely on information security. Corporate Governance includes the responsibility for solid internal controls, and the previous statement suggests that internal controls rely on information security, therefore von Solms (2001) argues that by bridging the two, information security must be an integral part of corporate governance.

Regulations have been passed in certain countries holding company management responsible for meeting certain security measures. In Australia, it is legislated that all companies must have an official information security Policy as well as an Acceptable Internet Usage Policy. (von Solms, 2001). In California, attestations signed by CEO's declare that internal controls are in place to comply with requirements of the Sarbanes–Oxley Act, which in turn specifies corporate governance, public disclosure and the practice of public accounting. Swindle and Conner (2004), argue that companies need to address internal as well as external security issues. They suggest that in the past, companies have focused on external threats and attacks, while the most costly internal threats and breaches, often occur from within an organisations network. This is becoming an even greater concern, as companies' link up systems to other companies. In South Africa, according to the King II report on Corporate Governance, a company must identify and address all material risks, including technology risks the company may face. The King II report states that the onus is on the board of directors to ensure that their organisation is managing IT risk satisfactorily (Leggat, 2003).

5.5 Personnel and Security Compliance

Having discussed the potential liability facing organisations that fall foul of government legislation and or legal compliance, and having established a link between information security and corporate governance, it is necessary to introduce the human link or what Vroom and von Solms (2004: 191) describe as the weakest link when it comes to information security. Vroom and von Solms (2004: 191) argue that although employees play a vital role in the success of an organisation, they also have the ability to undermine the protection of information assets in the organisation. They quote the information security Industry Survey conducted in 2001 which revealed that 48% of security breaches perpetrated in organisations were accidental. The survey revealed that of the remaining 52%, 17% of the security breaches were deliberate and the remaining 35% were neither proven to be deliberate nor accidental. In the same survey, an indication was provided of the number of internal security breaches reported by respondents. (see Table 5.1)

Insider Security Breach	2000	2001
Installation / Use of unauthorised software	78%	76%
Using company resources for illegal purposes	60%	63%
Using company resources for illegal profit	60%	50%
Abuse of computer access controls	56%	58%
Physical theft, sabotage or intentional destruction of computing equipment	49%	42%
Installation / Use of unauthorised hardware	47%	54%
Electronic theft, sabotage or intentional destruction of information	22%	24%
Fraud	9%	13%

Table 5.1 Information security industry survey – insider breaches, Vroom and von Solms, (2004:191)

Given the high percentages of internal breaches, little doubt exists that:

- Employees pose a major threat to information security in organisations
- A major challenge remains for organisations to address employee attitude and discipline.

Wylder (2003: 29) suggests that over several years, information security professionals have focused on developing and motivating employee compliance with security policies. Despite attempting to gain internal and external auditor support in enforcing policies, success has been disappointing. According to Wylder (2003: 30) other attempts at motivating employee compliance have included senior management pep talks, executive memoranda and security awareness campaigns. He refers to the 2002 Computer Security /FBI survey of computer Issues and Trends which found the top three reported sources of financial loss to be viruses, laptop theft and Net abuse. Of these top three breaches, Wylder (2003: 31) points out that both virus's and Net abuse can be mitigated through the development and enforcement of appropriate security policies. Equally concerning, is a separate survey quoted by Wylder (2003: 32) which

revealed that nine out of ten employees would be likely to open an email attachment without questioning its source or authenticity. Vroom and von Solms (2004: 191) as well as Wylder (2003: 32) suggest that despite interventions by businesses to get employees to act responsibly and adhere to security policies, the results have been disappointing. They, Vroom and von Solms (2004: 191) differ from Wylder (2003: 33) in that they believe that to enforce security behaviour and policy compliance, the responsibility must be shifted from a top down approach of awareness and security training to a bottom-up approach where individuals are held accountable for policy compliance. Wylder (2003: 34) believes that by engaging human resources (HR) and ensuring that security policy compliance is fully incorporated into annual or bi-annual performance appraisals, security policy compliance becomes a measured entity and therefore has a direct impact on the outcome of performance appraisals. Wylder (2003: 34) believes that the goal is compliance and the mechanism, enforcement. Vroom and von Solms (2004: 191) suggest that performance appraisals tend to be subjective, and lack credibility when it comes to reliability and validity. They argue that employees react uniquely and independently to situations based on their personalities and the factors that influence them. Vroom and von Solms (2003: 29) rather suggest "winning" employee cooperation and buy-in through examining the organisation, its culture and the organisational behaviour. They propose that organisational behaviour is used to change the shared values and knowledge of the group. This results in a behavioural change in the group which starts impacting and influencing individual behaviour which in turn impacts on the formal organisation. An approach may be found that would have an impact on the overall culture of the organisation, one level at a time. Employees buying in to an organisational culture and gaining an understanding of the need to behave in a certain way would be far more effective than employees feeling forced to behave in a certain way through a method of auditing and policing. The latter may result in employees resisting / refusing to comply.

5.6 Legal, Governance and Personnel Considerations for SME's

Geiger and Wegman (2002) suggest that small businesses have benefited largely through embracing Information Technology, which in the case of electronic commerce, has enabled some small businesses to reach regional, national and

international markets. At the same time, risk exposure has increased with many small businesses suffering financial losses due to a variety of security attacks (Geiger and Wegman, 2002).

From a legal perspective, SME's must put remedies and strategies in place to protect the firm's intellectual property. According to Geiger and Wegman (2002), the firm should not underestimate the risk of intellectual copyright which includes appropriate use of copyrights, patents, trademarks and trade secrets. Staff members may be inclined to copy or install pirated / illegal software, taking the view that being a small business it does not really matter / make a difference. Non-compete and non-disclosure agreements should also be considered to prevent the leak of proprietary information to competitors. Engaging staff with the correct information systems / technology / security skills often eludes SME's and outsourcing these services may present an attractive proposition to SME's. Management must ensure, however, they are protected by Service Level Agreement's (SLA's) that clearly define responsibilities on the side of company management as well as service providers. SME management must shoulder responsibility for information security and not forget they are ultimately accountable to stakeholders in the business.

Governance in small, private business is important as it will become one of the determinants of successful future growth (Davies, 2004). He suggest that accountants, bankers, consultants and venture capitalists are partial to seeing well-established processes and systems in place, as they are indicative of a well managed organisation with implied order and stability. Dimma, in Davies (2004), argues that small business must first determine what Governance means to them. He suggests that Governance should centre on building the business, subject to meeting the law and avoiding fraud. A starting point for small business would be to establish an independent board, either a fully constituted board of directors with legal liability, or an advisory board with as few as three people, who understand the type of business and can provide meaningful advice to the manager of the business. (Dimma in Davies, 2004). He also mentions that one of the ongoing concerns for entrepreneurs wishing to start or grow a business is finance / funding. Banks and bankers, he argues, are risk averse and conservative when it comes to lending money. People

cynically argue that banks only lend money to people / businesses that do not really need the funding. A SME manager with a small advisory board, (two or three individuals with some reputation), may go a long way towards establishing confidence in the organisations governance and operational controls, and in doing so, may unlock his / her potential to raise much needed funding.

Personnel issues are a core component / concern of information security in SME's. Security policies and procedures, although not uncommon in large organisation, are often unheard of in small organisations. Geiger and Wegman (2002) refer to a small business owner being locked out of his IT systems by a disgruntled staff member who eventually led to the owner having to hire a professional hacker to break in and restore access to his customer database. They suggest that small businesses should have active security planning and should engage outside experts to periodically review their IS infrastructure for weaknesses. Due to the nature of small businesses, most small firms only have one full-time staff member responsible for security with perhaps a further two staff members who can assist on a part-time basis. (Briney and Prince, 2002)

Some of the concerns surrounding personnel in SME's include:

- Lack of centralised user accounts, password controls and associated security
- Lack of policies and processes resulting in users not having a procedure to follow in the event of a security incident
- Affording, hiring and retaining the needed talent to maintain and implement information systems, including all related security interventions
- Information security training and staff awareness.

In general, the staffing culture in SME's is usually less formal than large organisations, with SME staff usually more flexible, and having to participate across a variety of duties. It is believed that staff that thrive in a SME environment are stereotypically less risk averse, seek greater challenge and reward, and operate within a more co-operative but less certain environment. It is believed that SME staff would react with greater resistance to the enforcement of security policies through performance appraisals and or auditing procedures. For this reason, Vroom and von

Solms' (2003: 29) suggestion of establishing a culture of employee co-operation and buy-in through the alignment of organisational and individual values and behaviour is thought to offer the best means of staff compliance with security policies.

5.7 Conclusion

From a legal perspective, SME's carry the same risk as large organisations. Illegally copying and installing software in a small business may have the same legal ramifications as it would in a large business. Client confidential data that is stolen / leaked from a small organisation will have the same legal implications than for a large organisation. The control of data is of particular regulatory concern. The Electronic Communications and Transactions Act (ECT Act) of 2002 details regulatory constraints placed on organisations such as how information is collected, stored, processed and disposed of. Stakeholders in an organisation have a right to IT Governance and the protection of information assets, just as they would expect the protection and control of traditional assets such as plant and machinery.
Governance is likely to be taken more seriously in large organisations than in SME's, as the management of large organisations are usually salaried professionals who have to answer to shareholders and boards of directors. These individuals earn high salaries and enjoy good incentives, however tenuously poised on performance these may be. SME's are often owner run and funded. Good or bad decisions generally impact on the owner / manager and his / her staff, and are of little interest or concern to outsiders. As SME's establish themselves and seek to grow, however, it is essential, that management adopt good governance practices, as this is likely to provide the necessary assurance to potential funders, investors and partners that the organisation is well managed, scalable, and carries less risk. Good governance also means that policies are addressed, and these directly impact on information security.

People constitute the least predictable and yet most critical component of any Information System. A badly negotiated / managed Service Level Agreement, (SLA), may result in an organisation severely exposed to risk, without the possibility of recourse. Personnel are what bind the organisation together ensuring that practices do not infringe upon legal, regulatory or governance concerns. Part of the leadership challenge facing organisations, remains how to get staff to support and participate in

the implementation of security systems, policies and practices. Two schools of thought exist on how this can be achieved: the first suggests an enforced top down approach using staff performance appraisals and other auditing techniques. (external or internal) The second proposes a bottom up approach, creating an organisational culture where people feel personally willing and inclined to want to buy-into a set of organisational values, which include embracing security policies and practices. It is believed that given the informal nature of SME's and the way in which personnel typically interact with one another, the second approach would be most appropriate. It is imperative that SME's appraise and train staff so that they are informed as to the impact their actions may have on their organisation.

Chapter 6: Security Standards and Models

Abstract

Chapter 5 reviewed the regulatory and non-regulatory environment in which organisations must operate. The potential liability facing organisations, through ill-disciplined / uncooperative staff members was explored and suggestions were made regarding staff compliance and motivation. This chapter introduces information security standards that are commonly available for implementation by organisations.

6.1 Introduction

Information security frameworks provide the basic structure on which an organisation can 'hang' its security initiatives. Many of the frameworks are divided into three (3) main sections. The highest level consists of policies (living documents) which are usually aligned with the organisation's mission and vision and updated as the organisation grows. They provide rules for the protection of information assets within the organisation. (Whitman and Mattord, 2003)

At an intermediate level, standards are detailed statements of how the policies should be implemented.

At the lowest level, practices, guidelines and procedures detail how to comply with the policy or what has to be done practically to comply with the organisation's information security policy.

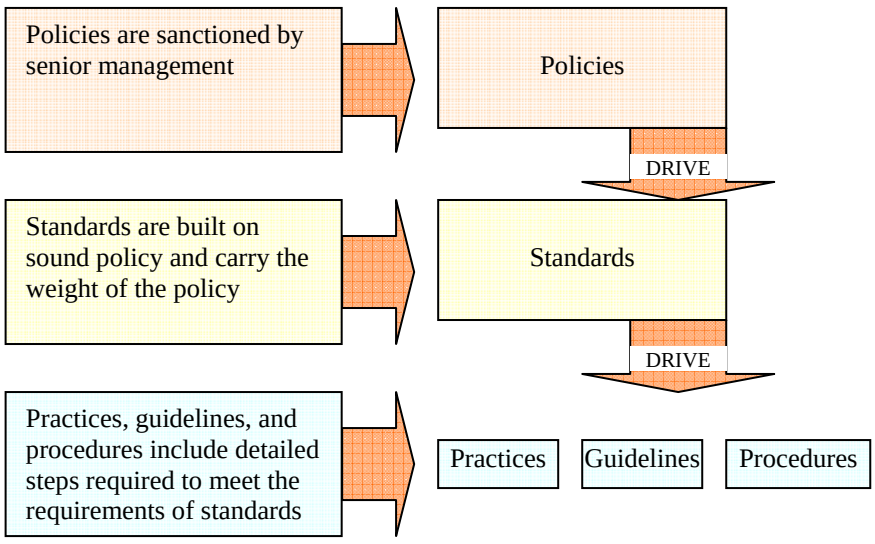


Figure 6.1 Policies, Standards, and Practices (Whitman and Mattord, 2003)

Any one of several information security blueprints may be adopted by organisations. The different frameworks focus on a variety of areas, often with documents aimed at the different levels, that is, policy, standards, guidelines or controls. Whitman and Mattord (2003) point out that security teams often piece together frameworks considered most applicable to an organisation's needs. An organisation that does not transact via the web would not necessarily be interested in a framework, guidelines or controls that focuses on E-Commerce. Once a framework has been selected, a period of fine tuning ensures that the framework best fits the organisation's needs, and vice versa. Eloff and von Solms (2000: 243) argue that an organisation needs to consider the reasons for selecting a particular standard, which may be:

- Accreditation by an external body (certification authority) in order to demonstrate competency and compliance with a particular standard
- To be in a position to perform self-evaluation so as to assess and improve their standards
- For peace of mind knowing that they are compliant with a certain standard and are following recommended guidelines or codes of practice

The following section explores the terminology that is used to describe security frameworks, and, discusses four (4) of the more widely used / documented security frameworks, standards and practices. The South African Bureau of Standards, SABS ISO/IEC 17799 Information technology – Code of practice for information security management is investigated in detail as well as some of the better known auditing standards, based largely on SABS ISO/IEC 17799.

6.2 Terminology

The terminology surrounding information security blueprints can be confusing and ill-defined. Documents refer to frameworks, controls, guidelines, benchmarking and certification. Confusion also prevails over the difference between an information security standard and a code of practice for example. (Eloff and von Solms, 2000: 243)

The following definitions demystify the terminology and are quoted directly from Eloff and von Solms. (2000: 243)

- International Standards

  "documented agreements containing exact criteria that must be followed consistently as rules, guidelines or definitions of characteristics to ensure that any materials, products, processes or services are fit for their purpose"

  As an example, a manufacturer of network equipment may claim that the equipment meets certain criteria in terms of universal compatibility with a particular protocol.

- National or Public Level Standards

  "At a national or public level, each country will have its own standards body. In the UK, this standards body is entitled the British Standards Institution (BSI), whilst the American National Standards Institute (ANSI) and the South African Bureau of Standards (SABS) are nationally accepted in the USA and SA respectively".

- Organisational Level Standards

  "The term 'standards' may be used to refer to a specific set of rules and requirements adopted in or prescribed for the company internally"

  As an example, an organisational standard may dictate that an encryption algorithm with a minimum key, be used.

- Guidelines

  "A guideline should give guidance in applying IS auditing standards. The IS auditor should consider certain guidelines in determining how to implement a standard. Guidelines also form a subdivision, an integral part or a key element of a standard. Although a guideline may form an integral part of a standard, the term standard and guideline are not deemed interchangeable. In this way, a standard shall be deemed to comprise a number of guidelines that should be followed in order to adhere to that standard".

- Code of Practice

  "A code of practice generally constitutes the culmination of years of experience. Organisations will, for instance (oft-times by trial and error), chance upon certain practices or actions that are sure to yield positive results. Such practices or actions are then documented and made available to other members of the organisation or even to rival organisations"

Eloff and von Solms (2000: 243) argue that Guidelines and Codes of Practice may be considered the same, although codes of practice are generally based on practical experience while guidelines may have had different origins. They warn, however, that codes of practice and standards should not be confused. A standard may be achieved by following several codes of practice. Eloff and von Solms (2000:243) site the example of an IS standard that requires good password management. To comply with the standard, several codes of practice may be required: one to manage password changes, another to manage password complexity and a third to manage password confidentiality.

- Controls

  "Can be defined as being a number of measured steps to take in order to realize a specific objective"
- Certification

  "Describes that process whereby an organisation, a product or a process is tested and evaluated to determine whether or not it complies with a specific standard. An individual or an organization duly appointed by a national or an international body effect this certification process."
- Accreditation

  "Is used to denote that process whereby an individual or an organization obtains formal approval from a national or an international body to perform the testing or evaluation for certification.
- Benchmarking

  "Is used to describe that process by means of which one measures one's organization against rival organizations, competitors or business partners"

6.3 Security Blueprints

A number of widely acceptable security blueprints and certification processes are available for use.

6.3.1 NIST

The Computer Security Resource Centre of the National Institute for Standards and Technology NIST (csrc.nist.gov) have produced several special publications which represent research into areas of information security including: cryptographic technology and applications, advanced authentication, public key infrastructure, Internetworking security, criteria and assurance, and security management and support. The NIST documents are publicly available, may be downloaded free of charge from the NIST web site, and should be considered as building blocks in the design of a security framework. NIST provides a trilogy of IT security program-level guidance. These publications are summarised below:

- NIST Special Publication SP 800-12: An introduction to Computer Security – The NIST Handbook

  NIST (2004g) claims that the handbook provides a broad overview of computer security, to help readers understand their computer security needs and develop a sound approach to the selection of security controls. Whitman and Mattord (2003) argue that NIST SP 800-12 provides little guidance on the design and implementation of security controls, but may form a very useful introduction to understanding information security blueprints. NIST SP 800-12 is based on eight (8) major elements:

  - Computer security should support the mission of the organisation
  - Computer security is an integral part of sound management
  - Computer security should be cost effective
  - Computer security responsibilities and accountability should be made explicit
  - System owners have computer security responsibilities outside their own organisations
  - Computer security requires a comprehensive and integral approach
  - Computer security should be periodically reassessed

- Computer security is constrained by societal factors

The NIST handbook served as the template for deriving the practices recommended in the NIST Special publication, described below.

- NIST Special Publication SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems

  NIST (2004h) refers to SP 800-14 as a 'guideline' that organisations can use to establish and review their IT security programs.

  Whitman and Mattord (2003) suggest that the scope of the document is broad and it provides philosophical principles that security teams can integrate into the whole information security process. The document describes eight (8) principles and fourteen (14) practices. The eight (8) principles are listed below:

  - Computer Security Supports the Mission of the Organisation
  - Computer Security is an Integral Element of Sound Management
  - Computer Security Should Be Cost-Effective
  - System Owners Have Security Responsibilities Outside Their Own Organisations
  - Computer Security Responsibilities and Accountability Should Be Made Explicit
  - Computer Security Requires a Comprehensive and Integrated Approach
  - Computer Security Should Be Periodically Reassessed
  - Computer Security is Constrained by Societal Factors

  The fourteen (14) principles are listed below:

  - Policy
  - Program Management
  - Risk Management
  - Life Cycle Planning
  - Personnel / User Issues
  - Preparing for Contingencies and Disasters
  - Computer Security Incident handling
  - Awareness and Training
  - Security Considerations in Computer Support and Operations

- Physical and Environmental Security
- Identification and Authentication
- Logical Access Control
- Audit Trails
- Cryptography

- NIST Special Publication SP 800-18: Guide for Developing Security Plans for Information Technology Systems

  NIST (2004i) suggests that SP 800-18 is intended to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements as well as to delineate responsibilities and expected behaviour of all individuals who access the system. Whitman and Mattord (2003) suggest that the publication provides detailed methods for assessing, designing, and implementing controls and plans for applications of varying size, but that it must be customised to fit the particular needs of the organisation. Templates are also provided for major application security plans.

6.3.2 Control Objectives for Information and Related Technologies (COBIT)

COBIT was developed over 10 years by the financial audit industry. It is a freely available, platform independent, open IT framework on good Information Technology (IT) security and control practices. COBIT is not intended to address IT security only, but rather an overall approach to IT. COBIT is aligned with other standards and regulations, and is intended to provide a reference framework for users, management, IS audit, control and security practitioners. Based on 40 international standards, COBIT has been implemented in over 100 countries. COBIT divides IT into 34 processes belonging to 4 domains and provides a high level control objective for each (figure 6.2). The domains are: Planning and Organising, Acquiring and Implementing, Delivery and Support, and Monitoring. The standard looks at quality, security and fiduciary needs of organisations and provides seven information criteria that can be used to define what the business requires from IT. The seven information criteria are: effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance.

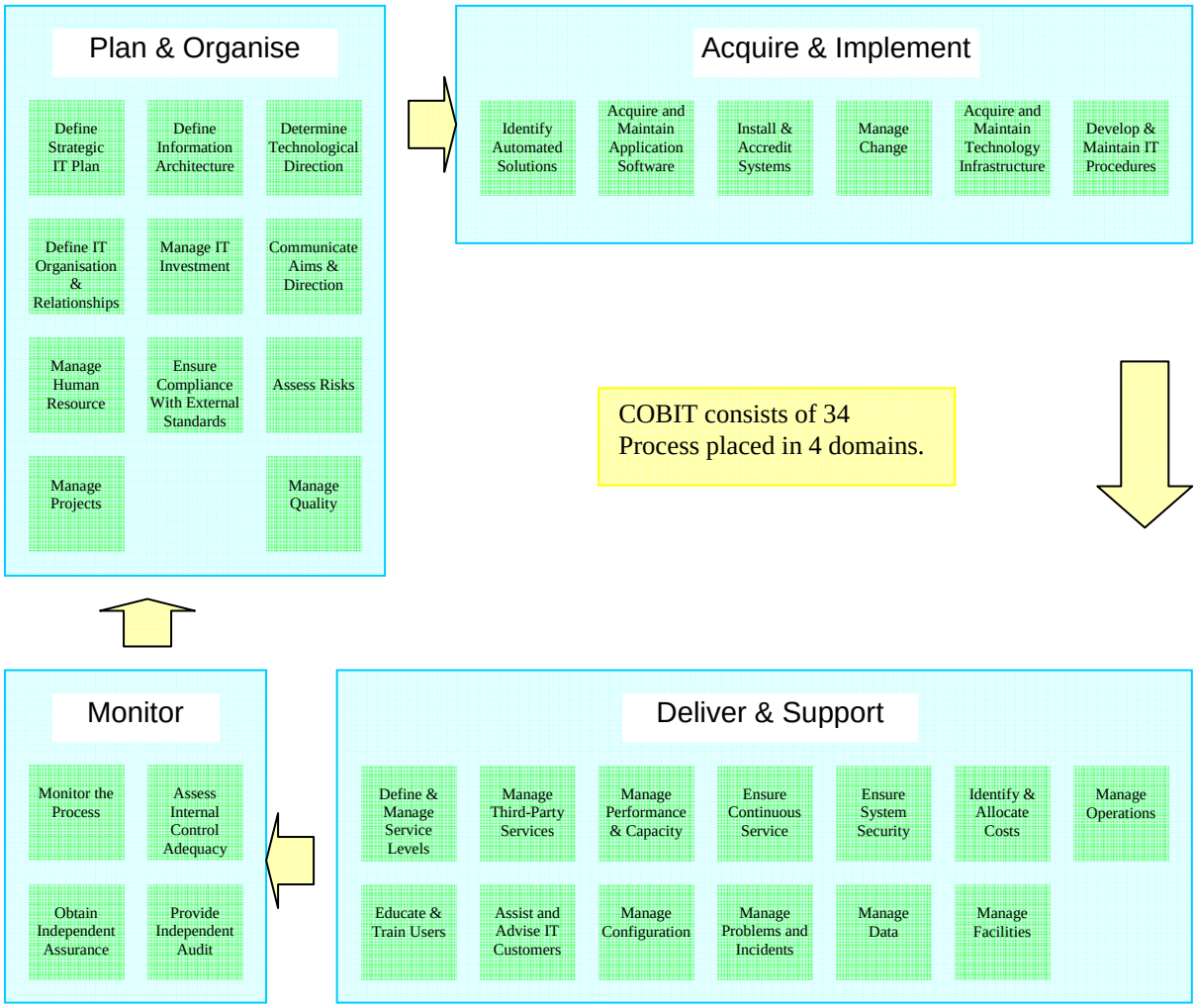


Figure 6.2 Diagram modified from Hardy (2003)

COBIT is not intended to be implemented as is, but should be fine tuned and customised to each organisation's requirements. According to the Information Systems Audit and Control Association (ISACA), (2004), COBIT provides the following functionality / objectives:

- Control Objectives - detailing minimum good control at a high level through Generic statements.
- Control Practices - practical guidance and advice on how to implement practices to achieve the control objectives
- Audit guidelines - guidance for each control area on how to obtain and understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met.
- Management guidelines – Guidance on how to assess and improve on IT process

performance, using maturity models, metrics and critical success factors. A management-oriented framework is provided for continuous self-assessment that is specifically focused on:

- Performance measurement
  how well is IT function supporting business requirements?
- IT control profiling
  what IT processes are important, and what are the critical success factors of control?
- Awareness
  what are the risks of not achieving the objectives?
- Benchmarking
  what do others do and how can results be measured and compared?

Large auditing and business consulting houses such as Ernst & Young, KPMG and PricewaterhouseCoopers support and audit COBIT in a variety of businesses throughout South Africa, including South African Breweries (SAB), which are now the second largest brewery in the world.

6.3.3 Internet Engineering Task Force (IETF) Security Architecture

The IETF is a large open international community of designers, operators, vendors and researchers, concerned with Internet architecture and security. The IETF is sub-divided into working groups, organised by different topics.

The Security Area Working Group, which acts as an advisory board for the protocols and areas developed through the IETF, have put together a request for comment (RFC) specified as the RFC2196: Site Security Handbook. RFC 2196 is intended as a guide (framework) for setting computer security policies and procedures on the Internet. RFC 2196 covers five (5) main areas of security and includes detailed discussions on development and implementation. The specification also includes chapters on: security policies, security technical architecture, security services and security incident handling. (Whitman and Mattord, 2003). RFC 2196 is structured as follows:

- Introduction
- Security Policies
- Architecture
- Security Services and Procedures
- Security Incident Handling
- Ongoing Activities
- Tools and Locations
- Mailing Lists and Other Resources
- References

6.3.4 SABS ISO/IEC 17799:2000 and SANS 17799-2:2003

6.3.4.1 Introduction

The National Technical Committee (SABS TC 5150.71: Information Technology), accepted the text of the ISO/IEC 17799 (2000), Information Technology – Code of practice for information security management, as suitable for adoption as a information security management standard for South Africa, on the 16 February 2001. SANS 17799-2 (2003) edition 2 which is an identical implementation of BS 7799-2 (2002) was adopted by the National Committee STANSA SC 71F, with permission from British Standards Publishing Ltd, during 2003.

The ISO /IEC standard originated from the British Standard Institute (BSI) Information Security Management standard BS7799. During the early 1990's, as a result of industry pressure, a working group was established to address information security. The investigation culminated in a "Code of Practice for information security management" in 1993. This work evolved into the first version of the BS7799 standard, released in 1995. As demand grew for an internationally accredited standard, a special fast track procedure by the Joint Technical Committee (JTC) 1 saw BS7799 receiving rapid accreditation and being adopted as the International Standards Organisation (ISO / IEC) 17799:2000 security standard. Although the standard has two components, only part 1 of the standard, ISO/IEC 17799, was adopted by the

International Standards Organisation. BS 7799 Part 2: information security management – specifications with guidance for use was not adopted by the International Standards Organisation, (ISO).

Part 2 provides information on how to implement Part 1, (ISO/IEC 17799:2000) and set up an information security management system (ISMS) (Whitman and Mattord, 2003). Only Part 1 is considered by the International body as being universally acceptable.

6.3.4.2 Control Domains

Many large businesses contributed towards the guidelines and recommendations that constitute the standard, which is composed of thirty six (36) security objectives and one hundred and twenty seven (127) security controls which are divided amongst ten (10) domains. The 10 domains are summarised below:

- Security Policy

  To illustrate management commitment and support, as well as provide organisational direction for maintaining / improving information security. This document must be communicated to all employees, in whatever way is deemed most appropriate and effective. The policy document must have an owner who is responsible for reviewing and applying updates, to ensure the document reflects any organisational / technical changes that have taken place since any previous risk assessment.

- Organisational Security

  Whereas the information security policy document is an expression of management commitment and support, the organisation security Policy refers to high-level, broad-based controls that counter the risks to which the organisation is exposed at an organisation level. They include policies to deal with:

  - IT Security Forum: composition and responsibilities
  - Consultants: specifically for advice regarding security
  - Asset Owners: nomination of information asset owners and maintenance of assets register
  - Authorisation: levels of authority and authorisation to approve

- External co-operation: lists of service providers
- External Access: contracts and non-disclosure agreements for access to systems and premises by outside parties

A multi-disciplined approach to information security is promoted whereby managers, users, administrators, application designers, security staff, auditors and specialist skills staff are encouraged to co-operate and collaborate with one another.

- Asset Classification and Control

  The organisation must ensure that all major information assets are accounted for and that:

  - Asset protection: someone is overall responsible for the protection of information assets
  - Asset controls: someone is responsible for maintaining the appropriate controls to protect the information asset

- Personnel Security

  Personnel Security Policy refers to controls to counter the risks posed by personnel. They include policies to deal with:

  - Recruitment: the recruitment process
  - Job Specifications: full job specifications
  - Terms and Conditions: general terms and conditions of employment
  - Non-Disclosure Agreements (NDA): standard procedures embodied in NDA
  - User Training: regular training to heighten awareness of security issues
  - Reporting of Security Problems: need to report breaches of security using standard procedures and mechanisms

- Physical and Environmental Security

  Physical and Environmental Security Policy refers to controls to counter the risks posed by physical and environmental factors. They include policies to deal with:

  - Boundaries: premises, locks, alarms, doors, sprinkler systems, keys

- Access: access to which parts of the building and by whom, especially rules for visitors
- Zones: access control to parts of the building (single room, floor of building)
- Equipment: controls to protect machinery against dust, smoke, vibration, chemicals, water
- Power: sources of power, UPS, emergency sources of power
- Cables: power vs. telecommunication cables, burying cables vs. conduit
- Maintenance: need for regular maintenance that is logged
- Off-Site Information Assets: movement of assets for purposes of business (laptop used by director on meeting in JHB), maintenance, private use
- Equipment Lifecycle Changes: roll-down of equipment and the need to ensure no sensitive information is stored on machine
- Good practice: clear desk and clear screen policy, especially after hours

- Communications and Operations Management

  Communications and Operations Management Security Policy refers to controls to counter the risks posed by communication and operational factors. They include policies to deal with:

  - Operations procedures
  - Change Control
  - Incident reporting
  - Segregation of duties
  - Systems changes
  - Separate development, test and live environments
  - Outsourcing
  - Capacity
  - Malicious software policy
  - Personnel awareness
  - Anti-virus software
  - Vulnerability alerts
  - Intrusion detection
  - Equipment setup and maintenance

- Permissions
- Network content
- Backups
- Off the shelf software
- Custom developed software and server configuration
- Test restores
- Archived data
- Operator logs
- User fault logs
- Learn from security incidents
- Networks: planning of networks
- Firewalls and servers
- Policies and procedures: for access to networks, systems, email use, encryption, private use of systems (these may form part of a separate policy)
- Media: need to classify all information and media
- Web sites: currency of information, maintenance
- Penetration testing

- Access Control

  Access Control Security Policy refers to controls to counter the risks posed by unauthorised access to the organizations networks, computers, information systems from internal and external sources. They include policies to deal with:
  - Policy: access policy for various users and groups of users
  - User registration
  - Privileges: users who can override system controls
  - Passwords
  - Equipment: secure placement of equipment
  - Enforced path: secure routes from terminal to system; no free roaming
  - External connections: external access to systems by staff and contractors
  - Application systems access control: logins, permissions, logs, monitors

- Systems Development and Maintenance

  Systems Development and Maintenance Security Policy refers to controls to counter the risks posed by application systems and the need to build security into such systems. They include policies to deal with:

  - Software development environments: shrink-wrapped vs. outsourced vs. in-house
  - Covert channels: malicious code within systems
  - Trojan code: additional malicious code
  - Trust the source: reputable vendors
  - Outsourcing and contractors
  - Personnel
  - Requirements: user requirements
  - Validation
  - Testing
  - Test data
  - Signing
  - Encryption: encrypt before transmission

- Business Continuity Management

  Business Continuity Management Security Policy refers to controls to counter the risks posed by interruptions to business activities from a general perspective. They include policies to deal with:

  - Fundamentals: backups, offsite storage, testing, contact lists, insurance
  - Impact Analysis: impact of loss of any information asset (done as part of the register construction)
  - Policy: plans to manage disaster in terms of deputies, roles and responsibilities, contact lists
  - Plans: steps to take in the event of a disaster
  - Emergencies: emergency drills, emergency services details; first aid training and first aid kits
  - Information assets: plan for each asset; temporary business premises
  - Communication: appropriate PR to communicate current business status

- Prioritisation: what to get up and running first and thereafter
- Practice: plans to rehearse recovery in the event of a disaster

- Compliance

  Compliance security policy refers to controls put in place to ensure that the organisation is not legally vulnerable. To avoid breaches of any criminal and or civil law, statutory, regulatory or contractual. They include policies to deal with:

  - Software storage, usage, piracy and licensing
  - Safeguarding / usage of organisational records
  - Collection, storage, usage, and disposal of client data
  - Reviews of security policies and technical compliance
  - System audit controls

Figure 6.3 below, places the ten (10) SABS ISO/IEC 17799 domains, ordered in a hierarchy, which ranges from organisational policies at the top of the pyramid, which are seen as focused managerial issues, ranging down to broader operational policies at the base of the pyramid. The diagram also discriminates between domains that are administrative, technical and physical by nature.

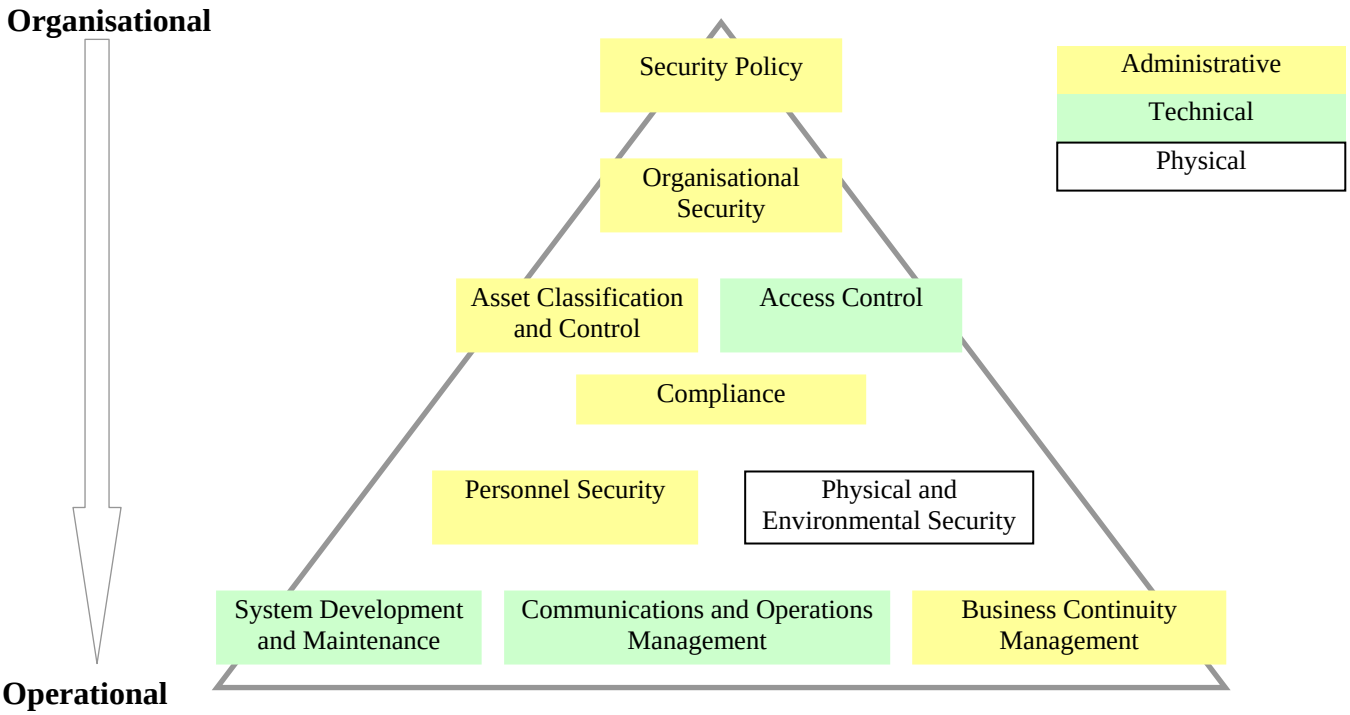


Figure 6.3 illustrates each domain in a progression from Organisational to Operational controls. (Unknown, 2001)

6.3.4.3 Universal Applicability

As mentioned in SABS ISO/IEC 17799 :(2000), the standard specifies controls that apply to most organisations and in most environments. Like COBIT, the standard recommends fine tuning and adding controls to suit an organisation's needs.
Once a risk assessment has been performed, not all guidelines and controls contained within the standard will necessarily be applicable, and additional controls, not included within the standard, may be needed (SABS ISO/IEC 17799:2000). Despite the insistence that a risk assessment precede the selection of security controls (SABS ISO/IEC 17799:2000), a number of controls are suggested that may be considered universally applicable and as "guiding principles for information security management". These are either based on legislative requirements or common best practice guidelines. These controls are detailed below:

Legislative Controls:

- Data protection and privacy or personal information
- Safeguarding or organisations records
- Intellectual property rights

Common Best Practice Controls:

- Information security policy document
- Allocation of information security responsibilities
- Information security education and training
- Reporting security incidents
- Business continuity management

The second part of the security standard, SANS 17799-2 (2003), is an auditing guide based on requirements. Part 2 of the standard was originally published in 1998 as BS 7799-2 (1998), and was intended to provide specification for internal audits or external certification. The original standard was considered too prescriptive and rigid which precluded it from gaining ISO/IEC accreditation. BS7799-2 was republished during 1999 and provided more alignment with controls in BS7799-1. Again the

standard was revised during 2001 and released as BS7799-2 (2002) during September 2002.

It has been fully adopted by the South African Bureau of Standards (SABS) and is known as, SANS 17799-2 (2003). The revised standard, as illustrated in figure 6.4, offers:

- Alignment with the Plan, Do, Check, Act (PDCA) process model
- Greater improvement and further clarification when it comes to:
    - the risk assessment process
    - the selection of controls
- Greater clarification on the requirements of documentation and records
- Enhanced risk assessment and management process

Organisations can administer their own internal audits using part 2 of the standard or they can apply to become BS7799-2 certified, in which case they are audited against BS 7799-2 of the standard, by a third party.

SANS 17799-2 :(2003) provides guidelines on how to build, operate, maintain and improve an Information Management System (ISMS), and is based on the: Plan, Do, Check, Act cycle as.

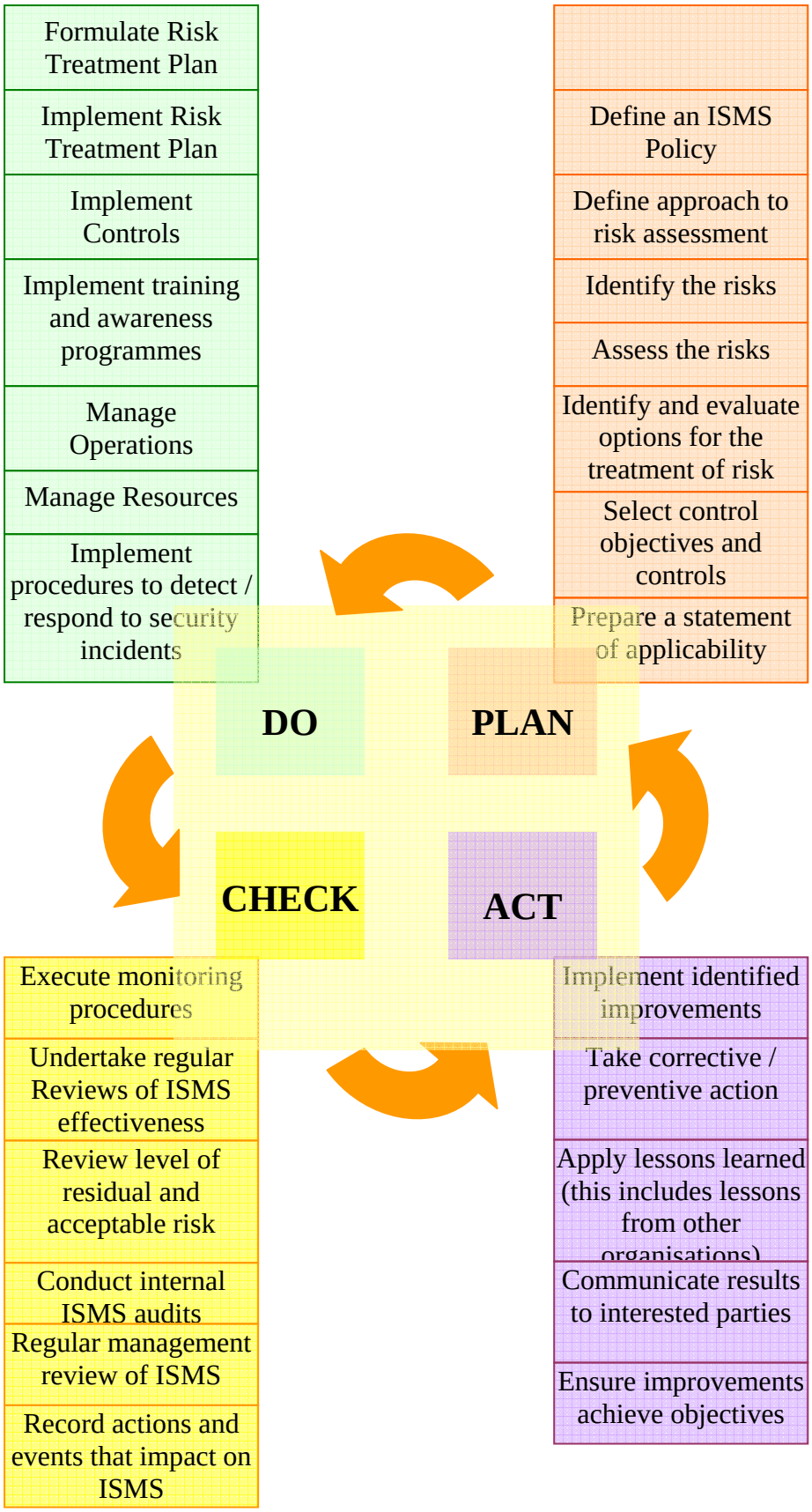


Figure 6.4 Representation of Plan, Do, Check and Act (PDCA) model with processes relating to each phase. Modified from SANS 17799-2 :(2003: 2)

SANS 17799-2 refers to the continuous Plan, Do, Check and Act cycle as a virtuous cycle because the purpose is to ensure that best practices are documented, reinforced and continually improved with time. The following section describes each of the four (4) processes:

- Plan and Do

A period of initial investment ensures that practices are documented, a risk management approach formalised, review methods explored and resources allocated. The plan phase must ensure that:

- Context and Scope for the ISMS are correctly established
- Information security risks are correctly assessed
- A plan for the appropriate treatment of risks is developed.

The Do phase must ensure that:

- Decisions are correctly implemented
- Solutions are correctly identified

- Check and Act

The Check and Act phases are used to reinforce, update and improve security solutions that have already been identified and implemented. Reviews may be:

- Required at any time, based on a given situation and what seems most appropriate at the time
- Built into computerised processes to operate and respond immediately
- Required as a result of security failure or vulnerability
- Required when an asset has been updated / modified requiring changed or enhanced security

SANS 17799-2 (2003) refers to annual or periodic reviews or audits that must be performed to ensure that the management process is working properly and achieving its objectives. These audits should give management confidence that:

- the information security policy still accurately reflects the business requirements

- the appropriate risk assessment methodology is being used
- documented procedures are being followed (as defined within the scope of the ISMS)
- technical controls such as firewalls and physical access controls are in place, correctly configured / up to date
- any risks that were considered residual at the previous audit, have been reassessed, and still remain acceptable to the organisation
- any revisions / agreed action from previous audits have been implemented properly
- the ISMS is compliant with the standard

Although SANS 17799-2 (2003) is complimentary to SABS ISO/IEC 17799 as already discussed, many 3rd party certification schemes are available as are many auditing tools, largely based on SABS ISO/IEC 17799. The following section introduces a certification scheme for Certification of Information Technology (ICIT), a model of certification proposed by the Information Institute of South Africa (ISIZA), and a software auditing tool known as the Pentana Checker software tool.

6.3.4.4 ICIT Certification Scheme

According to Eloff and von Solms (2000: 243) the Netherlands Institute has developed the Certification Scheme for Certification of Information Technology (ICIT). The ICIT scheme is based predominantly on BS7799 and designed to enable organisations to measure their level of compliance to BS7799, by conducting their own self-assessment. ICIT also provides support to organisations wishing to gain BS7799 certification by means of authorised third parties. The certification scheme presents four (4) levels of assessment / certification, based on the desired outcome:

- Self-assessment at entry level
  This is considered suitable for any organisation wishing to establish a first-off (internal assessment), to effectively see how they measure-up to BS7799 Code of Practice.
- Self-assessment at an advanced level is a more comprehensive internal assessment, which starts with an internal declaration and compliance statement and introduces additional controls.

- The first certification level is considered entry level, and involves the organisation being audited and certified by a third party who acts as an ICIT – certified auditor.
- Advanced certification is the real thing, and accredited organisations are rewarded by means of a certificate and statement of compliance. ICIT maintain compliance certificates while the accredited organisation holds the statement of compliance. The statement of compliance may be a valuable marketing / assurance tool, when it comes to interacting / collaborating with other organisations and their information systems.

  ICIT certification is conducted through risk analysis. Each control is assessed against a specific level to determine its (entry or advanced) status of compliance with ICIT controls. Once all controls at a specific level have been sufficiently addressed, a certificate can be issued by a certified auditor. An organisation seeking certification, that does not meet all the requirements / controls at an advanced level, may only receive a certificate at the entry level. (Eloff and von Solms, 2000: 243)

6.3.4.5 ISIZA Model

von Solms and von Solms (2001: 308) suggest that both small and large organisations have been slow to embrace security frameworks such as BS 7799 and this has resulted in a low incidence of BS 7799-2:2002 certification. Given these concerns, von Solms and von Solms (2001: 308) recommend a more phased and incremental approach to the certification process. They refer to a model proposed by the Information Institute of South Africa (ISIZA). The ISIZA model, which is freely available for use off the institute's web site (http://www.isi-za.org), provides a certification scheme which provides five (5) distinct certification levels. The entry level, (level 1), is intended to give the respondent a basic suite of controls against which to evaluate the organisation. As the levels increase, so does the complexity of controls being audited. Each section provides a control objective together with principles, which give the respondent a clear understanding of what is required. At the highest level (level 5), the model audits against compliancy with SABS ISO/IEC 17799. The ISIZA model is thought to be advantageous as it rewards the participating organisation for attaining

the requisite standards at each certification level, and ultimately encourages full compliance with SABS ISO/IEC 17799.

6.3.4.6 Pentana Checker

Pentana Checker for information security is a commercial proprietary software tool developed for auditing and assessing information security in accordance with the standards described in BS7799. The tool provides a full set of questions relating to BS7799 and also allows the auditor access to both overview and detailed information on BS7799 and 7799 part 2. The tool uses five (5) point Likert Scale questions with an option of N (not applicable). The tool allows a good level of granularity in terms of calculating average ratings, and can be done, per subsection of the standard. Results are displayed graphically, and may be used to compare security levels in similar organisations.

6.4 Conclusion

In managing information security, an organisation may piece together its own suite of controls, adopt a code of practice, embrace a security standard and strive for certification, or use a combination of these, to ensure that information assets are adequately protected. Several security blueprints exist such as the NIST special publications, which individually focus on aspects of information security. The IETF working group handbook on Internet architecture and Security is a framework for addressing computer security policies and procedures on the Internet. While ISO/IEC 17799 together with BS7799-2:2002 constitute security standards, COBIT is considered an IT framework. Both COBIT and ISO/IEC17799 together with BS7799-2:2002 may be used by organisations to address security. In order to implement these standards, a risk assessment should be conducted. On completion of the risk assessment, controls deemed irrelevant are dropped from the standards, while at the same time, those controls considered necessary and inadequately addressed by the standard, are then added into the standard. This way, the standards are fine-tuned and customized to meet the security requirements of the organisation. Both standards recommend external audits which culminate in accreditation. Third party certification processes also exist, such as ICIT and ISIZA, both of these based on ISO/IEC 17799. Several software tools such as Pentana Checker, are available, and are designed to

facilitate the certification process so that organisations can administer their own internal audits thereby assessing their compliancy levels, prior to being audited by a third party.

Although an organisation may piece together their own security controls, for reasons of compliance and certification, standards such as ISO/IEC 17799 and frameworks such as COBIT may be considered preferable. The ISO/IEC 17799 standard is comprehensive, however, and achieving SABS ISO/IEC 17799 compliancy is considered difficult for large, let alone small to medium sized organisations, that may consider the process daunting and unachievable. The incremental model proposed by ISIZA, is thought to offer a good balance of short to medium term, attainable certification goals, while culminating in full ISO/IEC 17799 compliance and certification.

Chapter 7: SME Information Security issues and SABS ISO/IEC 17799

Abstract

Chapter 6 described the more commonly known information security guidelines and standards, before focusing on SABS ISO/IEC 17799 and SANS 17799-2:2003. Different certification models such as ICIT and ISIZA were also explored. This chapter reviews SME information security issues, as highlighted in earlier chapters, after which they are mapped to SABS ISO/IEC 17799 controls that are considered suitable for addressing these security issues.

7.1 Introduction

For an organisation wishing to build a sound and comprehensive information security infrastructure, SABS ISO/IEC 17799 is a good option. Critics of SABS ISO/IEC 17799 argue, however, that the standard is too cumbersome and difficult to implement, and question its complexity for small and medium enterprises (SME's). The ITWeb web site, suggests, that small and medium sized organisations perceive security policies as prohibitively time consuming and difficult to implement. The article sites SME managers who claim that common sense and good backups are all that is required to protect their information systems. (Silva, 2004)

Firstly, this chapter:

Lists all of the information security concerns facing SME's, as mentioned in the literature review, and maps these security concerns to the controls mentioned in the previous chapter, considered to be:

- Regulatory
- Common best practice

The purpose of this exercise is to determine which of the security issues listed as needing addressing by SME's, may be considered generic security issues, that is, perhaps of concern to larger organisations as well.

Secondly, these security concerns are mapped to the SABS ISO/IEC 17799, 10 control Domains, to determine which of the Domains are relevant to the security needs of SME's and which Domains need to be most urgently addressed.

7.2 Regulatory vs. Common Best Practice Controls

In Table 7.1, the author indicates which of the SME security concerns as discussed / highlighted in the previous chapters, fit into which category of so called generic controls that is regulatory or common best practice. Controls, part of the SABS ISO/IEC 17799 security standard, have been placed on the top row of Table 7.1. These are either based on legislative requirements or common best practice guidelines. The security issues, raised as concerns for SME's, are listed down the left hand side of the table.

	Regulatory Controls			Common Best Practice Controls				
SME information security concerns (as explored in the literature survey)	Data Protection and privacy of personal information	Safeguarding of organisational records	Intellectual property rights	Information security Policy Document	Allocation of Information security Responsibilities	Information security Education and Training	Reporting Security Incidents	Business Continuity Management
Lack of security policies				√	√			
Lack of information security procedures					√			
Lack of staff training						√		
Poor staff awareness						√		
Lack of staff contracts (risk to intellectual property / business continuity)	√	√	√		√			√
Minimal concern over piracy / copyright			√					
Everyone mucks in, no one person responsible					√			
Poor control of assets		√			√			
Outsourcing but no Service Level Agreements	√							√
Poor access / password control						√		
No incident response plan							√	

Table 7.1 Nature of Security issues facing SME's, legislative or common best practice

	Regulatory Controls			Common Best Practice Controls				
SME information security concerns (as explored in the literature survey)	Data Protection and privacy of personal information	Safeguarding of organisational records	Intellectual property rights	Information security Policy Document	Allocation of Information security Responsibilities	Information security Education and Training	Reporting Security Incidents	Business Continuity Management
Informal data backup procedures (at best)		√				√		
Staff discipline (indiscriminate opening of email attachments)						√		
Systems left open and unattended	√	√				√		
Irregular or no patching of systems,					√			
Assumptions that security is in place					√			
No disaster recovery plan								√
Outsourcing of most technical issues					√			
Lack of non-compete / disclosure agreements	√		√					
Off-the-shelf fire-walling irregularly maintained / updated					√			
No policy for staff using portable computers, high incidence of theft		√				√		√
Irregular backups with data integrity seldom if ever tested		√				√		√
Shared user accounts (common passwords)	√					√		
Lack of assurance that data and systems are adequately protected	√	√				√		√
Lack of cyclical risk analysis / assessment					√			
Ad-hoc updates / upgrades to systems. Lack of update plan					√			
Little or no usage of audit logs / trails					√		√	

Table 7.1 *(continued)* Nature of Security issues facing SME's, legislative or common best practice

	Regulatory Controls			Common Best Practice Controls				
SME information security concerns (as explored in the literature survey)	Data Protection and privacy of personal information	Safeguarding of organisational records	Intellectual property rights	Information security Policy Document	Allocation of Information security Responsibilities	Information security Education and Training	Reporting Security Incidents	Business Continuity Management
Abuse of Informational Resources i.e. Internet abuse						√		
Indiscriminate access to information assets i.e. databases	√	√			√			

Table 7.1 *(continued)* Nature of Security issues facing SME's, regulatory or common best practice

The information policy document column has been shaded in Table 7.1 to indicate its commonality to all information security concerns. The process starts with the Information policy document which indicates management commitment and intent. Without the policy document being in place, there is no plan driving the process. All interventions are then ad-hoc by nature.

Based on Table 7.1, of the information security concerns expressed in SME's, 35% are Regulatory and the remaining 65% are considered to be Common Best Practice concerns.

Figure 7.1 Regulatory vs. Common Best Practice

Of the security issues that are considered to be regulatory, 16% are deemed to require controls to address intellectual property rights, 40% are deemed to require controls to address data protection and privacy and the remaining 44% are deemed to be needed for addressing safeguarding of organisational records.

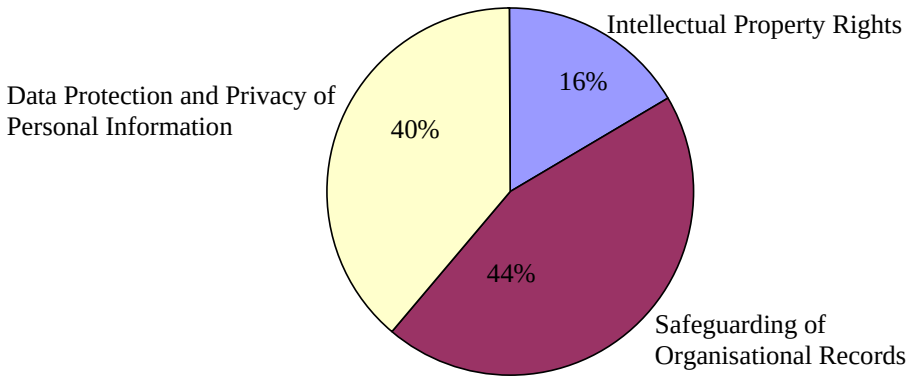


Figure 7.2 Type of regulatory controls most pressing for SME's

Figure 7.3 Indicates the percentage composition of specific controls, required to address common best practice issues.

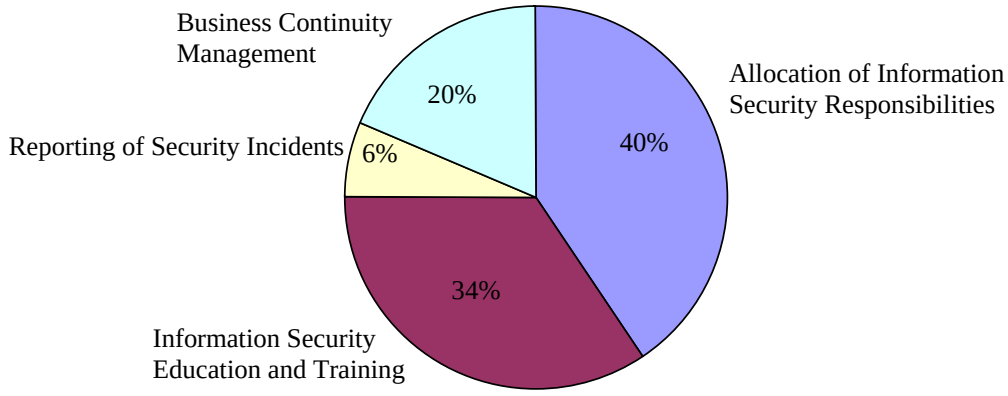


Figure 7.3 The percentage composition of the common best practice controls needed to address SME security

7.3 SME security concerns vs. SABS ISO/IEC 17799 security domains

In Table 7.2, the author indicates which of the SME security concerns as discussed / highlighted in the previous chapters, fit into which of the ten (10) Domain controls belonging to SABS ISO/IEC 17799.

Security issues, raised as part of the literature review, are mapped against the ten (10) Domains, in Table 7.2. The left hand column in Table 7.2 lists twenty nine (29) SME information security concerns, evidenced from the literature review. The top row in table 7.2 lists the ten (10) SABS ISO/IEC 17799 domains. A tick (√) exists where the security concern may be addressed by the corresponding security domain. Note, the first Domain in Table 7.2, (Security Policy), is considered core to every other control and is therefore shaded.

SME information security concerns (as explored in the literature survey)	**Section 1** Security Policy	**Section 2** Organisation Security	**Section 3** Asset Classification and Control	**Section 4** Personnel Security	**Section 5** Physical and Environmental Security	**Section 6** Communication and Ops management	**Section 7** Access Control	**Section 8** Systems Development and Maintenance	**Section 9** Business Continuity Management	**Section 10** Compliance
Lack of security policies						√				√
Lack of information security procedures		√							√	
Lack of staff training		√		√					√	√
Poor staff awareness		√							√	
Lack of staff contracts (risk to intellectual property / business continuity)		√		√		√				
Minimal concern over piracy / copyright		√	√	√		√				
Everyone mucks in, no one person responsible		√		√		√				
Poor control of assets			√	√	√	√				
Outsourcing but no Service Level Agreements		√				√				
Poor access / password control				√			√			

SME information security concerns (as explored in the literature survey)	**Section 1** Security Policy	**Section 2** Organisation Security	**Section 3** Asset Classification and	**Section 4** Personnel Security	**Section 5** Physical and Environmental	**Section 6** Communication and Ops	**Section 7** Access Control	**Section 8** Systems Development and	**Section 9** Business Continuity	**Section 10** Compliance
No incident response plan		√		√		√			√	√
Informal data backup procedures (at best)		√	√			√				√
Staff discipline (indiscriminate opening of email attachments)				√		√				
Systems left open and unattended				√	√		√			√
Irregular patching of systems, (at best)		√	√			√		√		
Assumptions that security is in place		√	√	√					√	√
No disaster recovery plan		√				√			√	√
Outsourcing of most technical issues		√				√			√	
Lack of non-compete / disclosure agreements		√		√		√				
Off-the-shelf fire-walling irregularly maintained / updated (at best)		√	√	√		√		√	√	
No policy for staff using portable computers, high incidence of theft				√	√		√			
Irregular backups with data integrity seldom if ever tested				√		√	√		√	√
Shared user accounts (common passwords)				√			√			
Lack of assurance that data and systems are adequately protected		√	√		√		√		√	
Lack of cyclical risk analysis / assessment		√				√			√	√
Ad-hoc updates / upgrades to systems. Lack of update plan								√	√	
Little or no usage of audit logs / trails		√				√	√			√
Abuse of Informational Resources i.e. Internet abuse & installing unlicensed software		√		√		√				
Indiscriminate access to information assets i.e. databases		√	√		√	√	√	√		√

Table 7.2 Security issues facing SME's vs. ten (10) SABS ISO/IEC 17799 security domains

Table 7.2 indicates that many of the security concerns relating to SME's fall into one or more of the ten (10) SABS ISO/IEC 17799 control Domains. The frequency histogram, Figure 7.4, illustrates the number of SME security concerns that are addressed by each of the SABS ISO/IEC 17799 Control Domains. Note: the information security Policy Domain has been omitted from the frequency histogram as it is considered a universal imperative Domain that impacts on all security concerns.

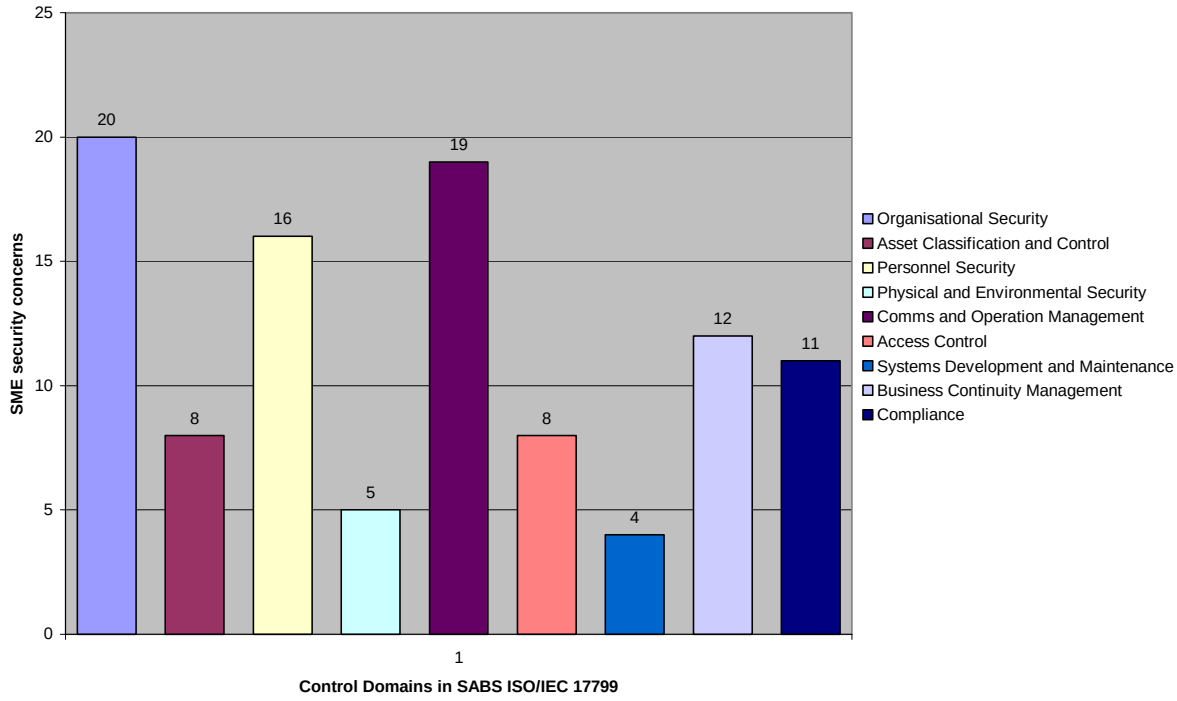


Figure 7.4 Number of SME security concerns in each Control Domain

Figure 7.4 indicates that of the twenty nine (29) SME information security concerns, exposed through the literature review, Organisational Security, Communications and Operation Management and Personnel Security are considered to be the most pressing issues. Systems Development and Maintenance is considered to be the least pressing security issue facing SME's

7.4 Conclusion

Twenty nine (29) information security concerns, thought to be most applicable to Small and Medium enterprises (SME's), were identified. The SABS ISO/IEC 17799 security standard, though very detailed, suggests core security controls that may be considered universal acceptable security controls. Twenty nine (29) SME security concerns were then mapped against the universally-applicable, regulatory controls (3) and the common best practice controls (4). Thirty five percent (35%) turned out to be regulatory with the remaining sixty five (65%), Common best practice concerns. Of the regulatory concerns, safeguarding of organisational records requires the greatest attention / controls.

Of the common best practice controls, information security education and training and allocation of information security responsibility, were considered the most urgent.

After removing information security Policy from the ten (10) control domains, Organisational Security, Communications and Operations Management, followed by Personnel security, were the three control Domains requiring the greatest attention. Systems Development was the least significant Domain, which is not surprising given that most SME's use off-the-shelf systems with minimal customisation / integration.

Chapter 8: Design of Experiment

Abstract

Chapter 7 listed SME security concerns raised in the literature review and compared these to a sub-set of security controls, part of SABS ISO/IEC 17799 standard, considered to be universally applicable for addressing information security. The second step involved mapping the same (29) security concerns to the ten (10) SABS ISO/IEC 17799 control domains. This chapter details the assembly and administration of a questionnaire, based on the ten (10) SABS ISO/IEC 17799 control domains, used to evaluate the information security state of practice in select SME's in the services sector, in the Eastern Cape.

8.1 Introduction

SME's are particularly vulnerable to security issues and concerns. SABS ISO/IEC 17799 is a universally accepted standard, yet considered by many as bulky, complex and confusing. SME's are reported to experience difficulty in implementing security mechanisms, SABS ISO/IEC 17799 or otherwise. A number of surveys on information security, have found that certain SME's ignore the most obvious security interventions such as formal data backup procedures and unique user ID's and password implementation.

This experiment, by means of a survey, determines the levels of awareness and protection of information assets, and the extent to which information security concerns drawn from the literature review, and linked to the 10 Control Domains of the ISO/IEC 17799 Standard, are comparable and applicable to the information security concerns and status of the surveyed SME's.

8.2 Survey Methodology

A survey questionnaire was deemed the most appropriate mechanism by which to collect data. Several questionnaires on information security served as a basis for the research questionnaire. Although some of these questionnaires are aimed at large enterprises, all of them contributed in some way towards the final research questionnaire. Questionnaires and reports, referred to are:

- Special Report, Imation Small Business Survey (2003). This is a specialised survey that explored: the use of Data Backup and Storage technologies, data

Backup & Storage Techniques and challenges in Managing Data Backup & Storage Processes. Although the Special Report, Imation Small Business Survey (2003) is a specialist survey, only dealing in backups, storage and recovery, it reveals several interesting findings and concerns:

- only 51% of small businesses check backup data files on a monthly basis, and small businesses appear to react to issues which directly impact their IT systems
- 27% reviewed backup procedures after the Melissa virus attacks and yet only 6% reviewed their backup procedures after the 9/11 attack.

- Ernst & Young Global Information Security Survey, 2004. (Bennett, 2004). Although this survey is a general information security Survey aimed at corporate business, the survey revealed similar security concerns to the 29 security issues highlighted in Chapter 7. Some of these are:
  - small percentage agreed that their organisations perceive information security as a CEO level priority
  - lack of security awareness is seen as a major problem although only 28% suggest raising employee information training or awareness as a top initiative for 2004
  - less than half of the respondents provide their employees with ongoing security training and controls
- Fujitsu, the third largest IT Company in the World, have a security review. This review consists of a BS7799 health check, gap analysis and a network security review. Fujitsu's health check is administered by means of an on-line questionnaire. The questionnaire in turn, consists of 15 Likert scale type questions. Several of the Fujitsu questions have been cited for use in the research questionnaire. (Fujitsu Online information security Questionnaire, 2001)
- PricewaterhouseCoopers information security breaches survey, technical report (2004). This report is sponsored by the Department of Trade and Industry (DTI) in the UK and is intended to assist UK businesses, (small medium and large) understand information security risk. The report is comprehensive and highlights many security findings and concerns. Some of these include:
  - nine – tenths of UK businesses send e-mail across the Internet, browse the web and have a web site

  - dependence on electronic information and the systems that process it continues to increase. 87% are highly dependent on electronic information
  - a quarter had a significant incident involving accidental systems failure or data corruption
  - a third of all companies now have security policies
  - Virtually every business has implemented anti-virus software and most update virus signatures as soon as they are available
  - fewer than one in ten businesses have tested their disaster recovery plans to see if they would work in practice
  - there is a low overall awareness and implementation rate of BS7799, although, those organisations that have implemented it, have found it has yielded real benefits
  - overall levels of investment in security are still considerably low.

- The Department of Trade and Industry (DTI) in the United Kingdom have produced an information security health check, broadly based on BS7799. (Information Security Health check, 2004). The health-check is available in two forms, either as a high level document or a detailed questionnaire with numerous questions and explanations. Several questions from the DTI detailed questionnaire were adopted for the research questionnaire.
- As discussed in Chapter 7, the Information Institute of South Africa (ISIZA) have produced a survey model which is freely available for use off the Institute's web site. (http://www.isi-za.org) The model provides various levels / assessments and ultimately assesses an organisation's level of compliance to SABS ISO/IEC 17799. (Information Security Self Assessment Instrument, 2004)

8.3 Design of the Questionnaire

The structure of the questionnaire was informed by a number of design imperatives, including:

- Participants should be able to complete the questions in the absence of the researcher. Many small business owners / managers leave business administration for after hours, at home, and they may want to complete the survey after hours as well.

- Respondents should be able to complete the questionnaire in paper form or via the web
- The structure of the Questionnaire should follow the ten (10) SABS ISO/IEC 17799 Security Domains
- The length of the survey should be such that respondents should feel inclined to complete the survey and not lose interest
- The questionnaire should be distributable to a large number of people

At the outset, reference was made to Table 7.4 and Diagram 7.4 in which SME security concerns and risk had been mapped to the ten (10) SABS ISO/IEC 17799 security domains. As mentioned in Section 8.2, several questionnaires were reviewed and several questions selected from both the Fujitsu Health-check as well as the DTI on-line health-check. Both surveys are BS7799 aligned.

The format of the questionnaire is as follows: (a copy of the questionnaire can be found in Appendix A)

- A Business Overview section, with four (4) questions used to establish the nature, size, and age of the business, as well as seven (7) questions that explore the composition and size of information systems deployed within the business. Questions in this section are either multiple select or multiple choice.
- The body of the questionnaire which is considered a security health-check introduces specific control questions aligned to each of the ten (10) SABS ISO/IEC 17799 Security Domains. All these questions are based on a 5 point likert scale. The scale ranges from: strongly agree, agree, undecided, disagree, strongly disagree. Section J: Compliance includes two multiple select questions as well.
- At the end of the survey, respondents are given the opportunity to enter contact details and to request feedback on research findings.

8.4 Administration of the Questionnaire

The researcher intended to administer the questionnaire in three Eastern Cape Province cities, namely Port Elizabeth, Grahamstown and East London, over a period of 3 months. A dual approach was adopted.

8.4.1 Paper Based Survey

The paper based survey was intended to be administered in the following way:

- SME owners / managers would be telephoned and asked whether they would be prepared to participate in the survey.
- The researcher would then visit the SME owners / managers and either administer the survey in person or alternatively leave the survey to be completed at the respondents later convenience. All surveys, left for later completion, were gone through and explained to the respondents.
- A collection date was set, and the researcher either collected the completed surveys failing which prompted the respondents to complete the surveys by a later date.

8.4.2 Web based Survey

The Web based survey was intended to facilitate the administration of the questionnaire in Port Elizabeth and East London. A commercial, web based survey authoring and delivery system, know as Qmark® Perception, was selected for administering the survey remotely. The researcher authored the on-line health-check so that its appearance and functionality were identical to that of the paper based instrument. The Web survey was administered in the following way:

- Each respondent was phoned and asked if they would be prepared to participate in the survey.
- Once respondents had confirmed they would participate, email was sent to them, explaining the purpose of the survey. A link was embedded in the email.
- When respondents picked on the link, they were automatically forwarded to the Perception web server with the online questionnaire.

8.5 Pilot Study

The paper-based survey and its web-based equivalent were both subject to a pilot study. The paper based survey was administered to a local SME owner and several colleagues. The Web based survey was administered to a SME owner in Johannesburg and another in Somerset West.

8.5.1 Intent of Pilot Study

The intent of the pilot study was to gauge the overall impression of the participant and to ensure that:

- Questions were unambiguous and clear
- The length of the questionnaire was not considered excessive
- The respondent would find the layout of the survey, logical and easily navigable.

In addition, from a Web delivery perspective:

- Country wide access to the web server would be unrestricted.
- By picking on an embedded email link, the respondent would be seamlessly directed and logged into the survey.
- The respondent would not loose interest and abort the process, but rather be encouraged to complete the survey and pick on the submit button, to ensure the data was submitted to the database.
- The system could cater for a respondent being interrupted / aborting the process and returning to it later, without duplicating results.
- Survey data collected in the perception database, would correctly reflect the respondent's answers, would be accurate and secure.

8.5.2 Finding and Enhancements

The results of the pilot study resulted in useful comments, which in turn resulted in some changes to the survey. Comments and changes are listed below:

- The survey's, (both paper and Web), took approximately ten (10) minutes to work through. Two of the three respondents were happy with the length of the survey, the third respondent felt the survey was slightly too long.
- Concerns were expressed regarding a question placed in the Demographics section of the questionnaire, asking respondents to rate the level of importance of the contribution IT makes to quality, cost savings and efficiency. A list of thirteen (13) options was supplied and respondents were asked to select the most important item by placing a 10 next to it, and the least important item, indicated by placing a 1 next to it. Comments received, suggested the question was too complex and not directly enough related to information security. The question was awkward once converted to the Web questionnaire as well. A decision was taken to remove the

question. This also reduced the length of the survey, effectively by ten sub-questions.

- Web respondents found the process of picking on an email link, and being redirected to the survey web site, seamless and straight forward.
- A further change to the questionnaire was effected during the pilot study phase after a respondent pointed out that one of the questions was repeated, verbatim. After some embarrassment, the second instance of the question was removed.
- In order to address concerns that certain of the questions could be confusing to non-technical respondents, the decision was taken to conduct a telephonic discussion with each web respondent, prior to granting access to the survey. As mentioned, the paper based survey was conducted / handed over in person, which enabled the researcher to work through the Sections / questions prior to leaving the survey for the respondent to complete.

  The final survey and cover letter can be found in Appendix A.

8.6 Population Sample

8.6.1 Grahamstown

A list of suitable SME's was drawn up after discussion with a local business person, and members of a local Rotary club. Due to the small nature of Grahamstown and the proliferation of SME's, assembling the list was relatively easy. A local telephone directory and newspaper were used to assemble business contact details.

8.6.2 Port Elizabeth and East London

A large banking institution in the Eastern Cape, was approached, and agreed to assist in identifying and approaching their SME banking clients, to see whether or not they would be prepared to participate in the survey. The researcher supplied the bank with the SME profile required for the survey, and in return the bank would provide a list of clients, together with their company names, contact details and email addresses. All people on the list would have already been approached by their respective 'relationship managers' and would have agreed up-front to participate in the process. The bank's assistance in pre-qualifying potential respondents was invaluable.

8.7 Data Analysis

The data is to be analysed to determine:

- The Control Domains that may be considered of least concern to SME's
- The Control Domains that need most urgent addressing by SME's
- The overall state of practice of information security in SME's
- The overall opinion on information security held by SME's
- The relevance of SABS ISO/IEC 17799 to SME's

8.8 Conclusion

A questionnaire survey was deemed the appropriate mechanism to determine the state of information security practice and concerns of select SME's, in the service sector, in the Eastern Cape. An entirely new questionnaire was not considered necessary as a number of survey instruments were found and questions from these instruments were considered suitable for this experiment. As far as conducting the experiment goes, dual delivery mechanisms are appropriate in an IT-centric world, but paper-based questionnaires should not be eliminated. The assistance of outside parties, like the bank, to get respondents is important.

Chapter 9: Survey Results

Abstract

The previous chapter described the design of the experiment, detailing the survey methodology, questionnaire design, pilot study and population sample. In this chapter, the survey results are presented together with tables and graphs for each of the forty nine (49) questions. Discussion and interpretation is reserved for Chapter 10.

9.1 Introduction

Having administered the survey, both in person and electronically, the data can be analysed. The Perception software stores the electronic survey results in an Access database. Through the Perception server administrator logon, the researcher is able to monitor the progress of the survey, and the system maintains log files of when surveys are started and completed. Several on-line respondents started the survey, but unfortunately never completed it. These results were not captured by the system. Once the paper based questionnaires had been collected, the researcher captured this data on the Perception system as well, so that all data was in electronic format. Perception provides comprehensive reports, including graphs, although a text based report format was chosen so that the information could be transferred into a Microsoft Excel spreadsheet. Microsoft Excel was used for all analysis including histograms.

9.2 Response Rate

Thirty seven (37) suitable SME's were identified and approached to complete the paper based survey, in Grahamstown. Personal visits were conducted with 35 of these SME's. Some respondents worked through and completed the survey with the researcher, and other respondents requested to complete the surveys in their own time. In some cases follow-up visits were conducted, and finally, 32 completed surveys were collected.

A list of sixty-nine (69) potential SME's in Port Elizabeth and East London was obtained. Of the 69 SME's in Port Elizabeth and East London, 61 were considered suitable. Contact was only possible with 55 of these. Although all SME owners / managers who were contacted, expressed a willingness to participate in the process,

there were only 39 attempts logged on the Perception server. Despite 39 respondents logging on and commencing the survey, only 34 respondents were recoded by the system as having completed the survey. These 34 completed on-line surveys were used for this research. Table 9.1, below, summarises the Web respondents at each stage of the process.

Respondents	No
Initial List (as supplied by bank)	69
Suitable Respondents (based on SME profile)	61
Respondents Reachable (contact details available)	55
Respondents who started questionnaire	39
Surveys Finally Completed (Usable)	34

Table 9.1 On-line participants in East London and Port Elizabeth.

The researcher found the process of visiting and discussing the survey with SME's in Grahamstown both valuable and enlightening. Several respondents made use of the opportunity to discuss information security with the researcher, and expressed interest in receiving feedback from the survey results. The researcher believes this personal approach resulted in an almost 100% survey completion rate. As indicated, respondents, in Port Elizabeth and East London, were telephoned, but the researcher did not have any personal contact with these respondents.

A possible limitation of this research is that some of the Grahamstown respondents gave the impression of being protective over certain of their results. Given that Grahamstown is a small city and the researcher is known by many of the respondents, the desired level of researcher anonymity could not be achieved. This also accounts for the smaller number of Grahamstown respondents revealing their turnover, despite the researcher assuring respondents that results would be treated as strictly confidential.

The results of 66 questionnaires (34 on-line and 32 paper-based) are described in the following sections: Section 9.2, Demographics, and Section 9.3, results of questions relating to each of the ten (10) SABS ISO/IEC 17799 Domain controls.

9.3 Demographics

9.3.1 SME Overview

Question 1: Business Composition

Consulting	Recruitment	Vehicle Services	Cleaning	Legal	Accounting	Estate Agent	Medical	Equipment Leasing / Rental	Computers	Equipment Repairs	Other Professional Service
10	2	3	1	3	4	3	2	0	6	4	28

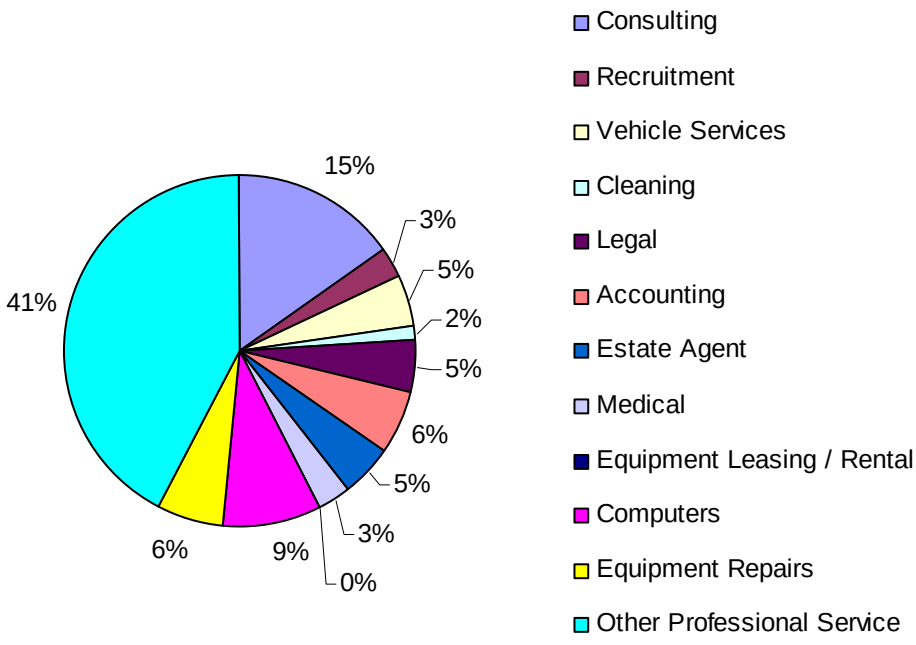


Figure 9.1 Business Composition

Of the 66 respondents, 28 (41%), fell into other professional services which included services such as travel agents, a small private bank, couriers and others. 10% of the SME's surveyed were consulting firms, based in the Eastern Cape, with staff members who consult in other regions such as Gauteng and the Western Cape.

Question 2: Operational Years

0-2	2-5	5-10	10-15	15-20	20 +
0	15	16	12	5	15

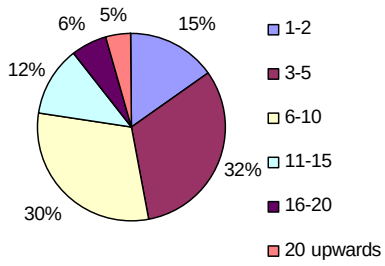


Figure 9.2 Years in Operation

None of the respondents had been trading for less than two years, while the majority had been operational for between 5 and 10 years.

Question 3: Number of Employees

0-5	6-10	11-25	26-35	36-50	51 +
17	17	21	1	1	4

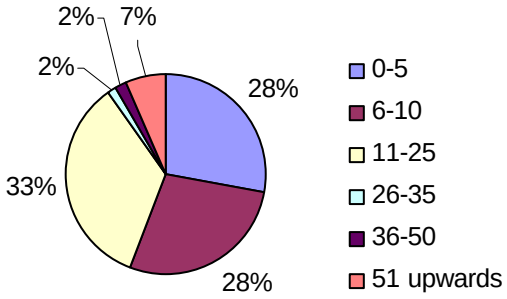


Figure 9.3 Number of Employees

The majority, (33%), of the businesses surveyed employed between 11 and 25 staff members followed by (28%) employing between 0 – 10 staff members. Only (2%) of the SME's surveyed employed 51 or more staff members.

Question 4: Average Annual Turnover (R '000)

0-150	151-1000	1001-1500	1501-2000	2001-10000	10001 +
2	8	7	8	13	10

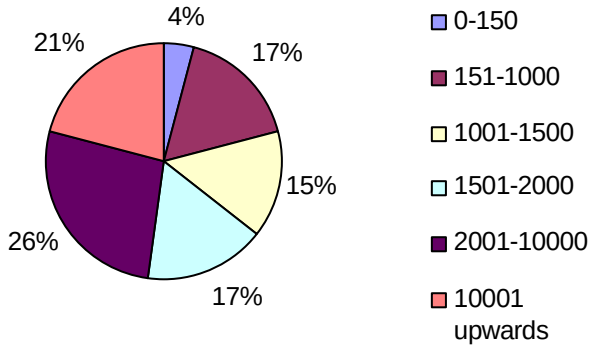


Figure 9.4 Average Annual Turnover (R'000)

Only 48 of the 66 businesses surveyed, responded to question 4. It is believed the low response rate was for reasons of confidentiality. Only two of the SME's, (4%), had a turnover as low as R150 000. The majority of SME's that responded to question 4 have turnovers ranging from R1 million to R10 million. 10 SME's, (21%), boasted turnover in excess of R10 million

9.3.2 Nature of IT Infrastructure

Question 5: Number of Computers

1-2	3-5	6-10	11-15	16-20	20 +
10	21	20	8	4	3

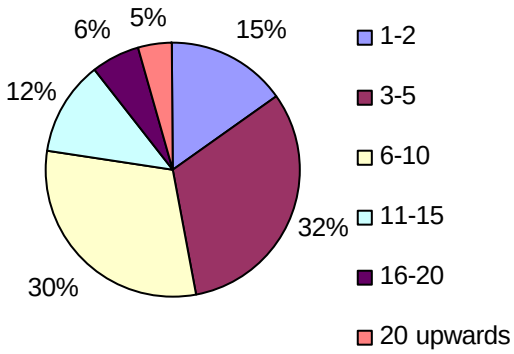


Figure 9.5 Number of Computers in Use

21 of the 66 businesses surveyed, (32%), have between 3 and 5 computers. 20 business, (30%), have between 6 and 10 computers. Only 5% of businesses have in excess of 20 computers.

Question 6: Years of Computer Use

0-2	3-5	6-10	11-15	16-20	20 +
2	11	32	13	4	3

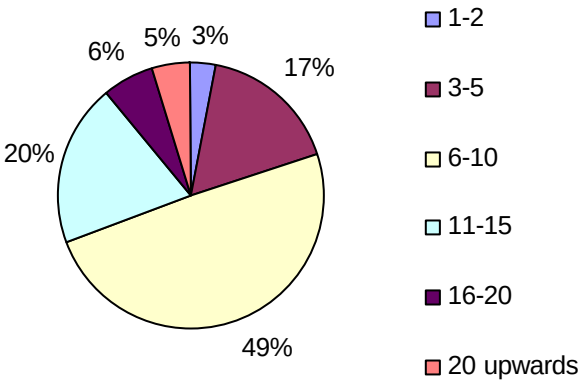


Figure 9.6 Computer Usage (*years*)

Of the 65 respondents who answered question 6, 32 of them (49%) claimed to have used computers in their businesses for between 6 – 10 years. Thirteen respondents (20%) had been using computers for between 11 – 15 years. Only 3 respondents, (5%) claimed to have used computers for over 20 years.

Question 7: Hardware Used

Computers	Fax machines	Printers	Modems	Computer Networks	None of Above	Other (please specify below)
66	64	66	57	60	1	9

Equipment specified as other:
Photocopiers
Scanners
Digitising Tablets (CAD/CAM application)
Satellite Dish

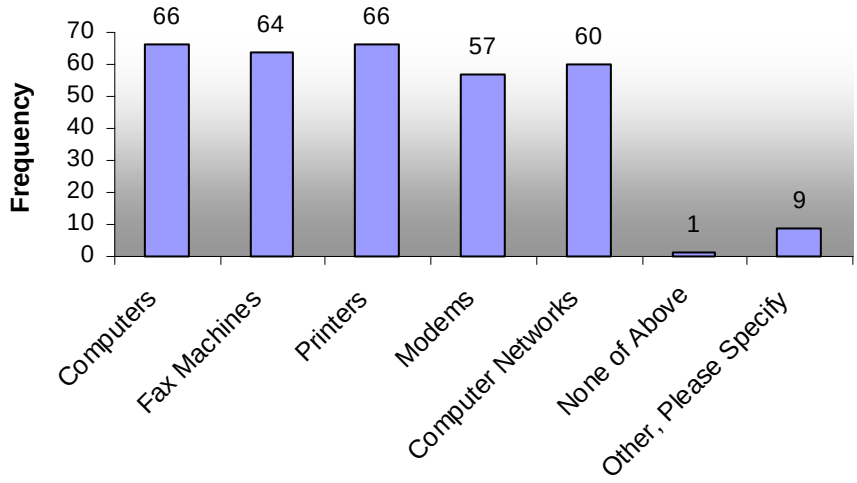


Figure 9.7 Hardware Used

Not surprisingly, computers and printers were used by all respondents, followed closely by fax machines, (97%). 60 respondents, (91%), reported having a computer network. 57 respondents, (86%), reported using modems. The reference to modems

in this sense is thought to be generic i.e. all devices used to connect SME's to public networks as against Question 11, which explores leased line, permanent connectivity vs. dial-up connectivity. One respondent claimed not to use any of the technology. This is considered to be an error.

Question 8: Software Used

Word Processing	Databases	CAD/CAM	Accounts	Desktop Publishing	Spreadsheets	Communications	Integrated Packages	Non of the above	Other (please specify)
59	31	8	58	20	53	38	34	0	8

Software specified as other:
Galileo (specifically used in the travel industry)
Point of sale Software
GIS Software
Financial Planning Software
Project Management Software
Web Enables Proprietary Software

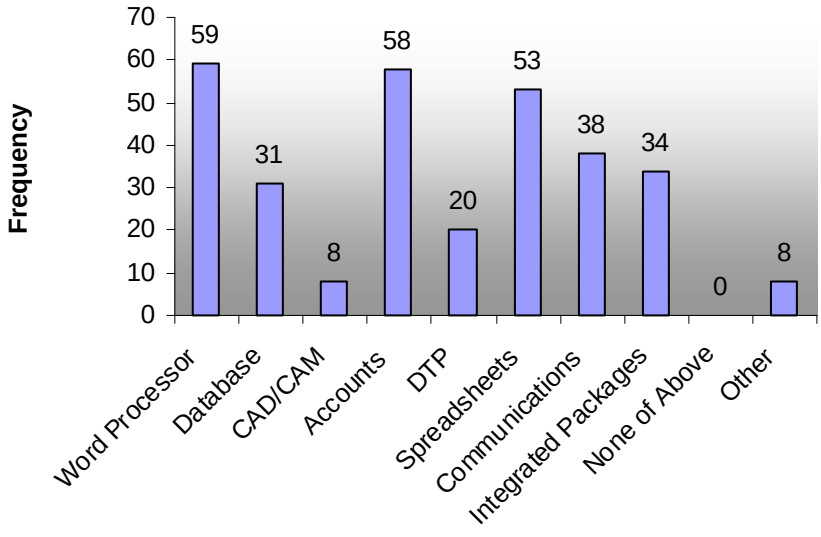


Figure 9.8 Application Software Used

Of the 66 respondents, the most commonly used applications are Word Processors, (89%), followed by Accounting Packages (87%) and Spreadsheets at (80%). 57% use Communications Packages and 46%, Databases. Integrated Packages, such as Microsoft Office or Corel Office are used by 51% of the respondents. Integrated packages usually have a minimum of a Word Processor and Spreadsheet, built-in. For this reason, the figure of 89% for Word Processors seems believable.

Question 9: Indicate Use of Following

Internet	Email	Intranets	Electronic Commerce	EDI	None of Above
65	63	18	29	12	1

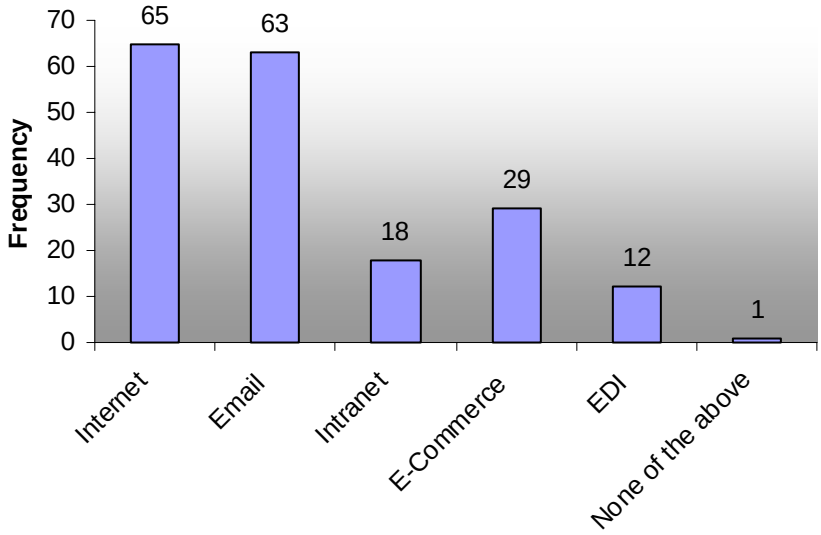


Figure 9.9 Nature of Computer Transactions

The Internet is used by 65 of the 66 (98%) respondents. Email follows in popularity with 63 respondents (95%) making use of this communication medium. This was surprising as Email and Internet services are often 'bundled'. Only 43% of the SME's

surveyed make use of E-Commerce. Intranets are only used by 27% of the respondents and Electronic Data Interchange (EDI) by 18% of the respondents.

Question 10: Internet Used for the Following

Gathering information on customers	Gathering information on competitors	Establishing a business presence	Routine Communications with customers	Routine communications with suppliers	Providing service / support to customers	Selling services to customers	Other (please specify below)
24	15	24	52	50	37	23	11

Equipment specified as other:
Banking
Medical Aid Submissions
Tax Returns / Compliance (SARS)
Research
Data Sets

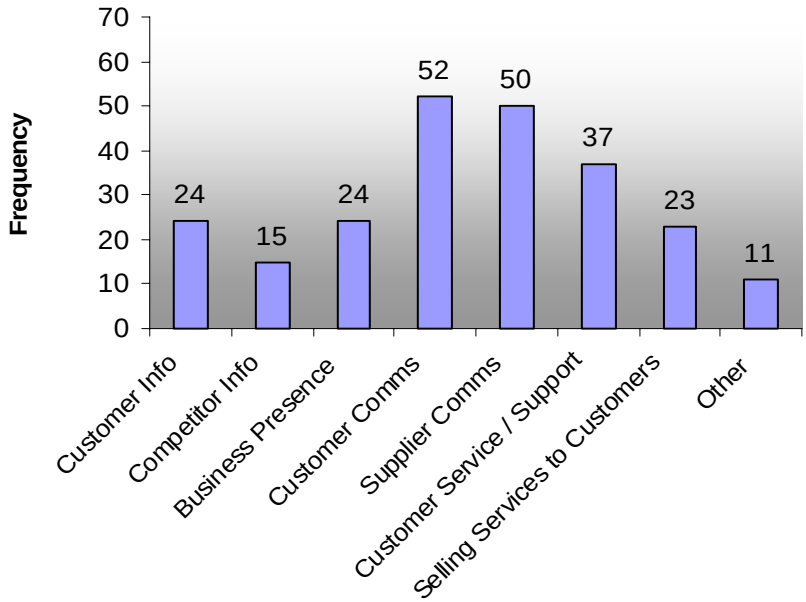


Figure 9.10 Internet Usage

Of the 66 respondents, (78%) use the Internet for communicating with customers. This is followed closely by 75% who communicate with suppliers. 37 respondents, (56%), use the Internet for customer service and support. 24 respondents, (36%), claim to use the Internet for establishing a business presence. 11 respondents, (16%), selected 'other' and specified, Internet banking, medical aid returns, tax returns / correspondence and business research, as areas that are facilitated by the Internet.

Question 11: Access to the Internet

Full time (ADSL, Diginet, Leased Line)	Dial-up Connection (Modem, ISDN)
37	29

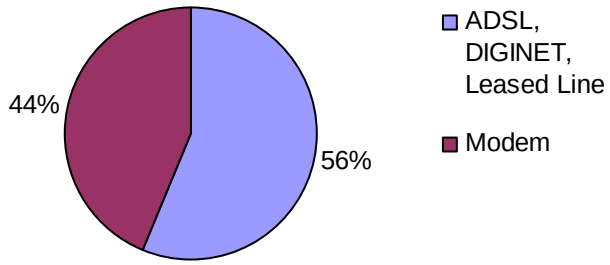


Figure 9.11 Internet Usage

37 of the respondents, (56%), said they use permanent leased lines with ADSL / Diginet connectivity to their service providers whereas 29, (44%), said they dial-up to establish connectivity to their service providers / Internet.

9.4 Security Domains

9.4.1 Section A: Security Policy

This section explores whether or not the organisation has an information security policy, formal or otherwise, and if so, to what extent the Policy is 'lived' and enforced in the organisation.

Question 12:

Roles and Responsibilities for information security in our organisation are well defined, e.g. someone is responsible for backups, registering users on the system, planning against a site disaster, liaising with Service Providers

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
16	37	4	8	1

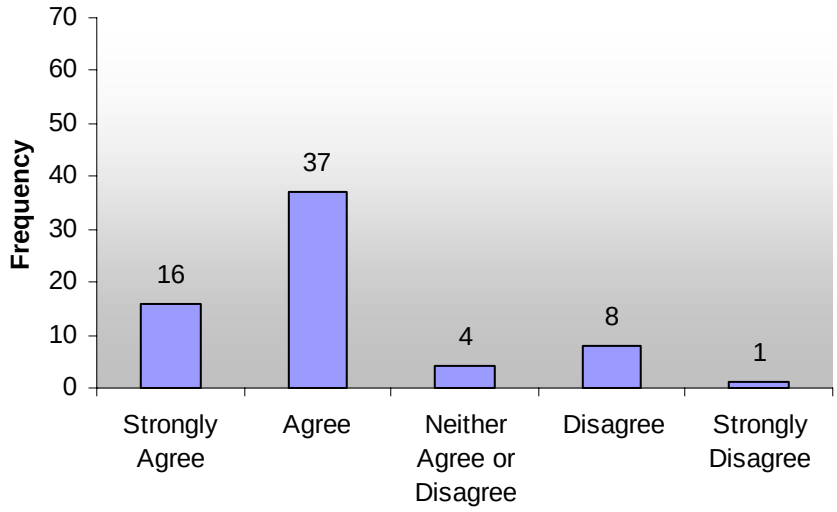


Figure 9.12 Defined Roles and Responsibilities

Of the 66 respondents, 37, (56%), believe that Roles and Responsibilities for information security are well defined in their organisations. 12 respondents, (12%), do not believe that their organisations have well defined Roles and Responsibilities for information security while 1 respondent felt strongly that this was the case.

Question 13:

We have a documented information security policy

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
7	5	5	33	16

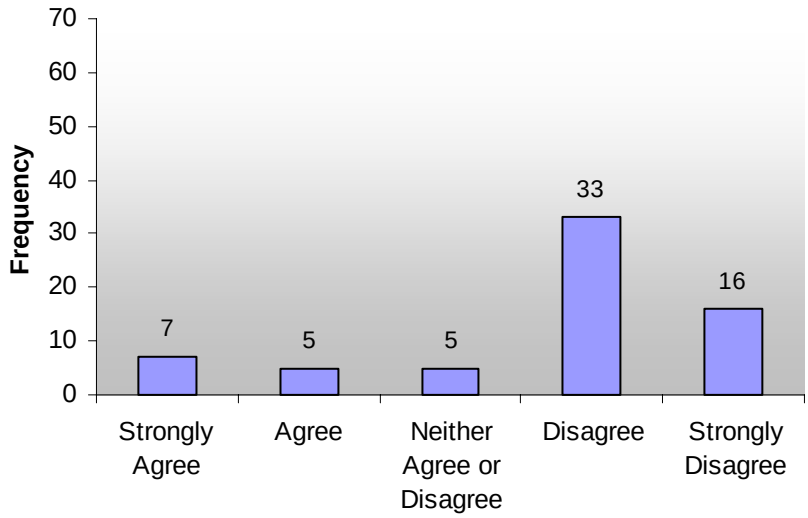


Figure 9.13 Documented information security policy

The majority of respondents disagree that their organisations have information security policies. More specifically, 33 respondents, (50%), disagree that their organisations have information security policy, and a further 16, (24%), strongly disagree that their organisations have information security policies. Only 7 respondents, (10%), firmly believe their organisations have an information security policy.

Question 14:

Staff are aware of our information security policy

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
8	12	10	25	11

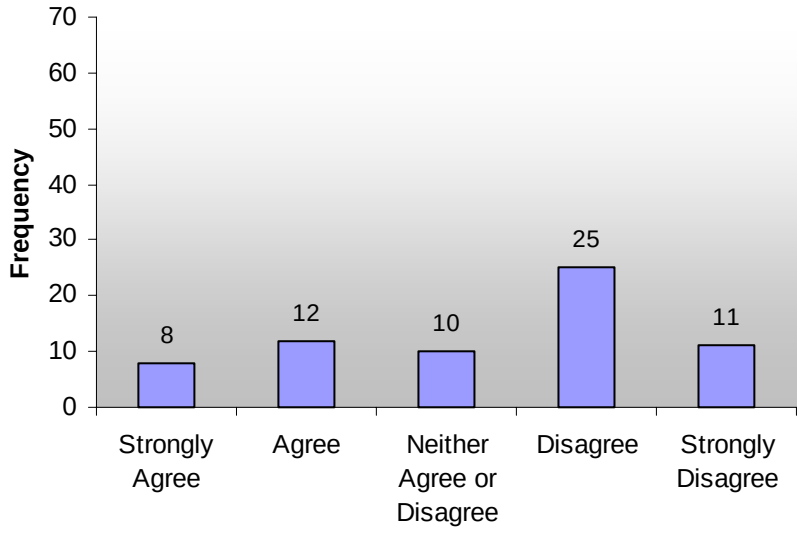


Figure 9.14 information security policy awareness

11 respondents (16%) strongly disagree and a further 25 respondents, (38%), disagree that staff are aware of an information security policy. In contrast, 8 respondents, (12%), strongly agree that staff are aware of the organisations information security policy.

Question 15:

All staff are given adequate and appropriate information security education and training

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
4	13	10	28	10

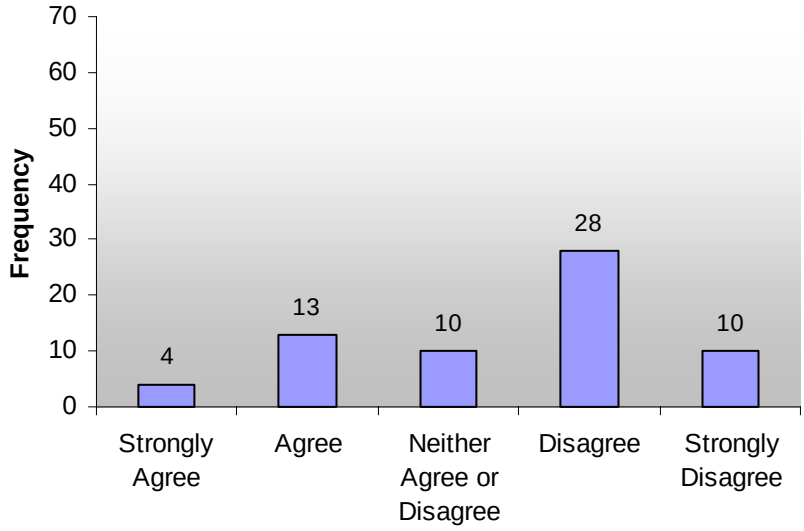


Figure 9.15 Information security education and training

10 respondents (15%) strongly disagree and a further 28 respondents, (42%), disagree that staff are given adequate and appropriate information security education and training. 10 respondents, (15%), are unsure as to whether or not staff receives adequate and appropriate information security training. Only 4 respondents, (6%), strongly believe that staff does receive adequate and appropriate information security training.

Question 16:

Staff are well informed as to what is considered to be acceptable and unacceptable usage of our information systems e.g. Email and Internet conduct

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
14	28	7	11	3

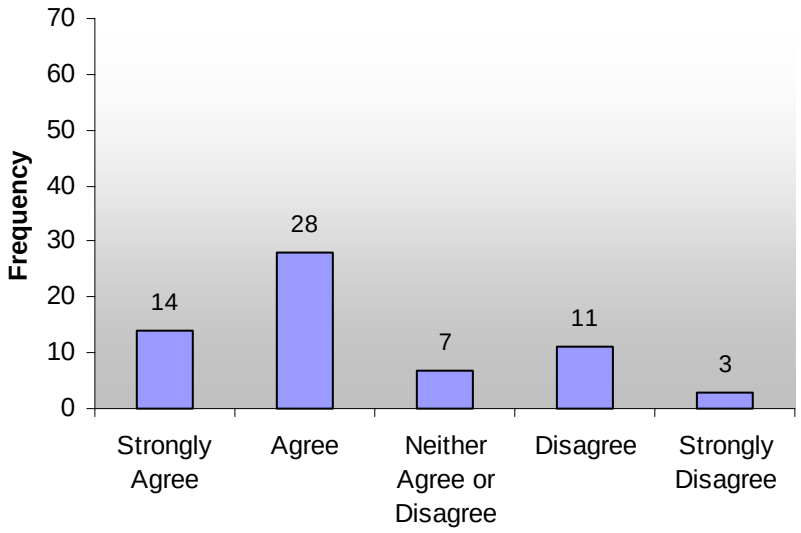


Figure 9.16 Staff Awareness of Acceptable / Unacceptable Usage of Systems

28 respondents, (42%), felt that staff are aware of what constitutes acceptable and unacceptable behaviour when it comes to use of information systems, more specifically email and Internet use. A further 14 respondents, (21%), strongly agreed with this view. In contrast, 11 respondents, (16%), disagreed with this view and a further 3, (1,5%), strongly disagreed that staff are aware of what constitutes acceptable and unacceptable behaviour when using organisational information systems.

9.4.2 Section B: Organisational Security

This section explores the management of information security within the organisation. This should normally include assigned security roles and how expertise is retained and managed in-house or outsourced, or both.

Question 17:

A director (or equivalent) member of our staff has responsibility for information security.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
22	33	3	6	2

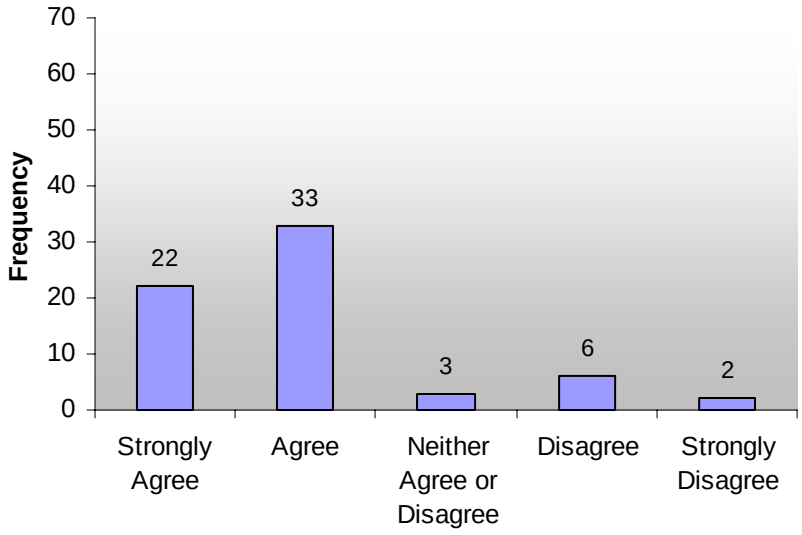


Figure 9.17 Director or someone equivalent is held responsible

The majority of respondents, 55 or (83%) agreed or strongly agreed that a director or equivalent person has responsibility for information security. Only 6 respondents, (9%), disagreed with the statement and a further 2 respondents, (3%), strongly disagreed.

Question 18

Expertise on information security is available internally, and where not, external advice is sought

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
14	28	8	11	5

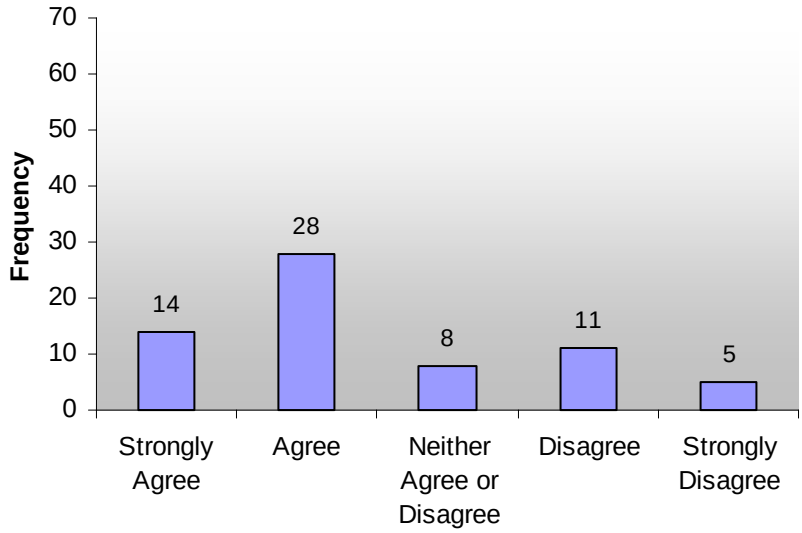


Figure 9.18 Information security expertise (in-house / outsourcing)

42 respondents, (64%), either strongly agree or agree that in-house expertise is available, but when this is not the case, external advice is sought. A total of 15 respondents, (24%) disagree or strongly disagree with this.

Question 19

Third party (outsider) access to our information systems requires approval by a senior manager.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
25	25	7	5	4

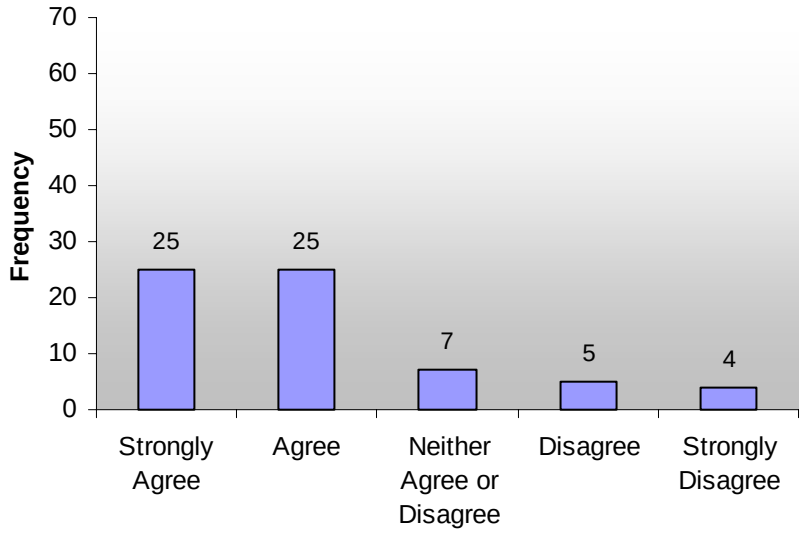


Figure 9.19 Managed Third Party Access

50 respondents, (75%), agree or strongly agree that outsider access to information systems requires approval by a senior manager. 9 respondents, (14%), either disagree or strongly disagree with the statement.

9.4.3 Section C: Asset Classification and Control

This section explores the protection of organisational assets through mechanisms. "All major information assets should be accounted for and have a nominated owner" (SABS ISO/IEC 17799:2000)

Question 20:

We can identify and locate all Assets (including software, hardware, staff and services) used for information handling

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
22	27	9	7	0

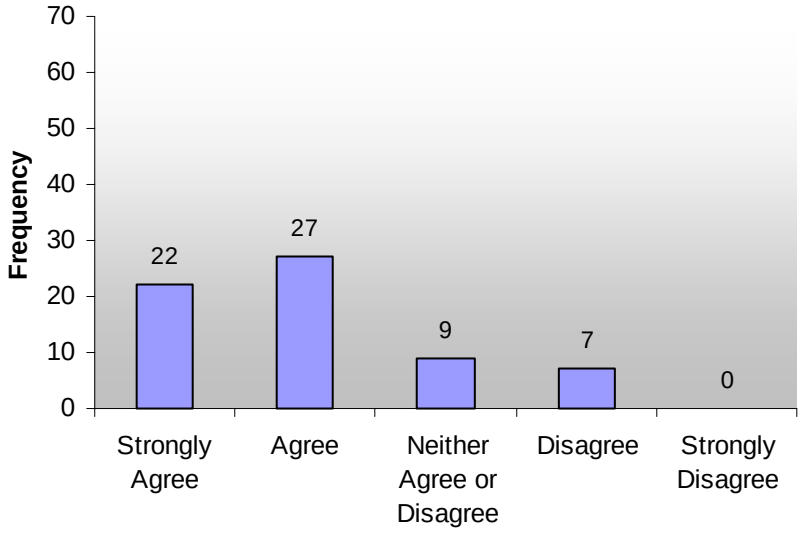


Figure 9.20 We can locate and identify all assets

49 respondents, (74%), claim that they can identify and locate all assets. Only 7, (10%), of respondents said they disagreed with this statement. 9 respondents, (13%), neither agreed nor disagreed with the statement.

Question 21:

We control Local and Remote Access to our information assets adequately

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
16	31	13	5	0

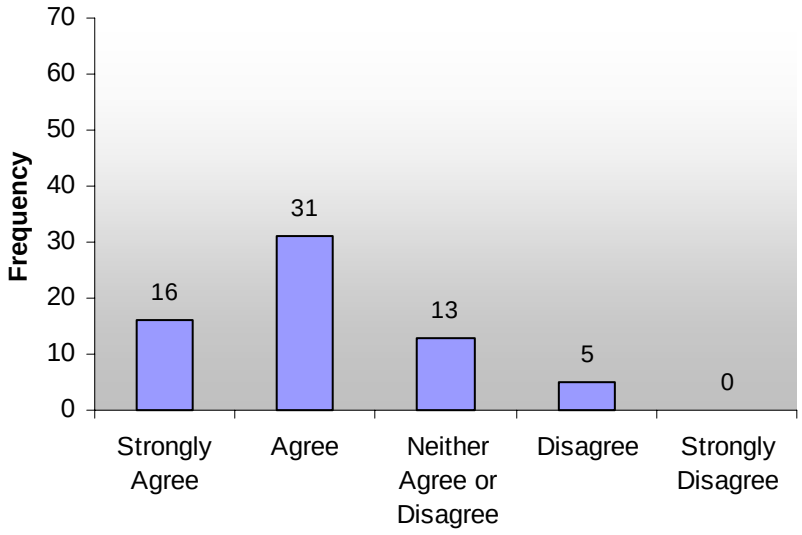


Figure 9.21 Control of local and remote access to assets

47, (71%), respondents believe they adequately control local and remote access to information assets. 5 respondents, (8%), feel that they do not. 13 respondents, (20%), neither agree nor disagree with the statement.

Question 22:

Our staff know what to do with information with regard to its storage, usage, archiving, backup and destruction

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
13	28	13	10	2

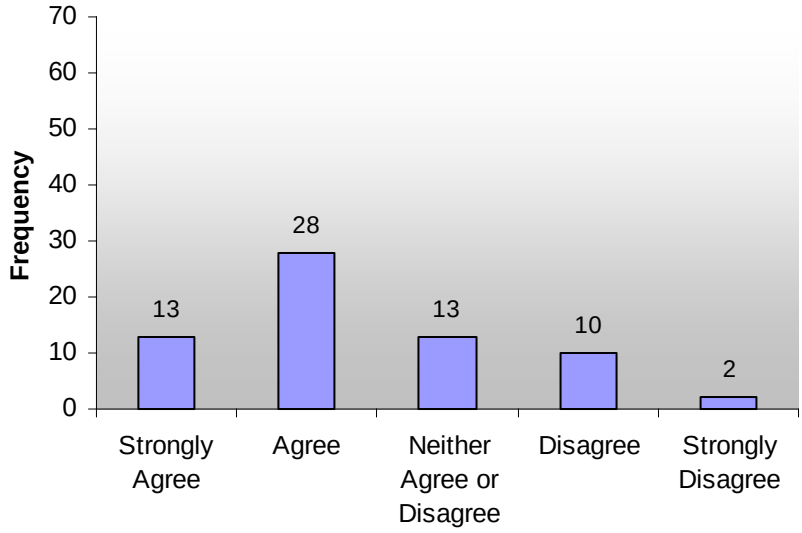


Figure 9.22 Overall staff Information management

41 respondents, (62%), believe that their staff know what to do when it comes to looking after information. (storage, usage, archiving, backup and destruction). 10 respondents, (15%), disagree with this and a further 2, (3%), strongly disagree with this. 13 respondents neither agree nor disagree with this statement.

9.4.4 Section D: Personnel Security

The reduction of human error, theft, fraud or misuse of facilities. "Security responsibilities should be addressed at the recruitment stage included in contracts, and monitored during an individuals employment" (SABS ISO/IEC 17799:2000)

Question 23:

Staff are aware that security incidents must be reported to management immediately

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
19	30	13	2	2

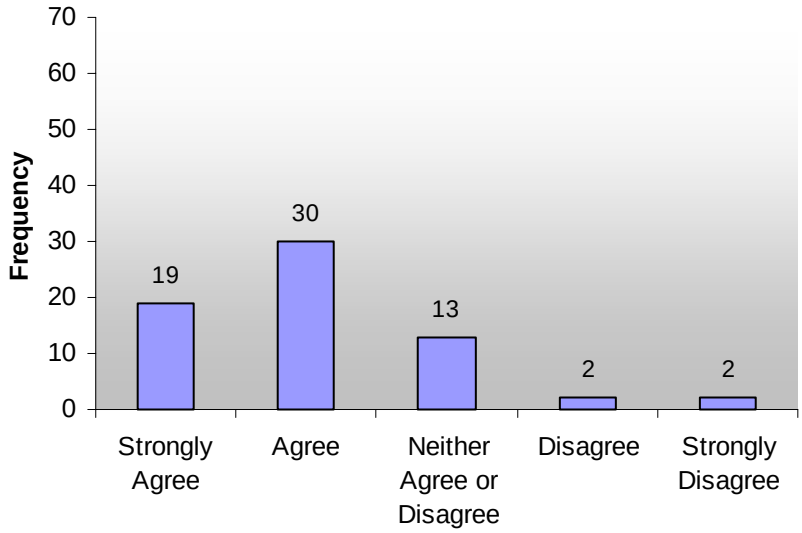


Figure 9.23 Overall staff Information management

49 respondents, (74%), said that they agreed and strongly agreed with the statement that staff are aware that security incidents must be reported to management. Again, 13 respondents, (20%), neither agreed nor disagreed with the statement. Only 4 respondents, (6%), disagreed or strongly disagreed with the statement.

Question 24:

Staff have been trained to secure their computers at all times, when moving away from their work stations. e.g. locking or logging off their computers when going for a tea break or out to lunch.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
11	17	13	21	4

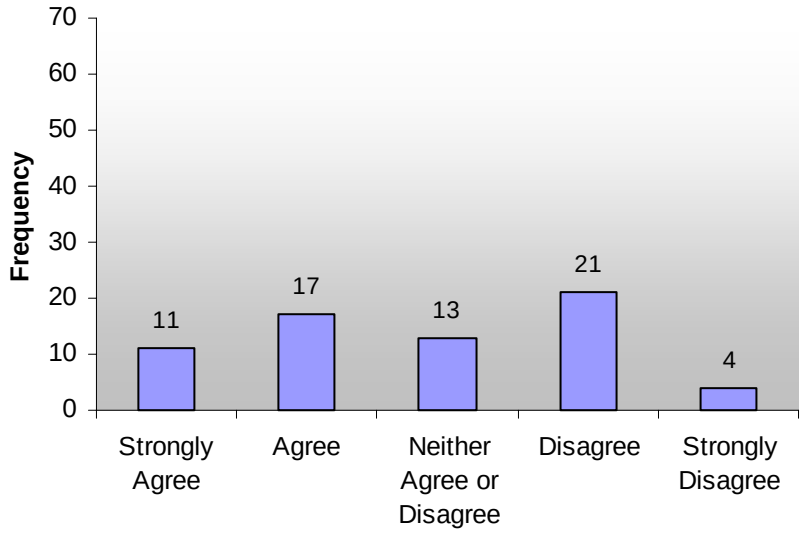


Figure 9.24 Staff securing their computers

28 respondents, (42%), suggest that staff secure their computers / terminals when moving away. 13 respondents, (20%), neither affirm nor deny this statement, and 25 respondents, (37%), do not agree / strongly disagree with this statement.

Question 25:

There is a formal disciplinary process for employees who have violated our security policies and processes

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
7	14	9	28	8

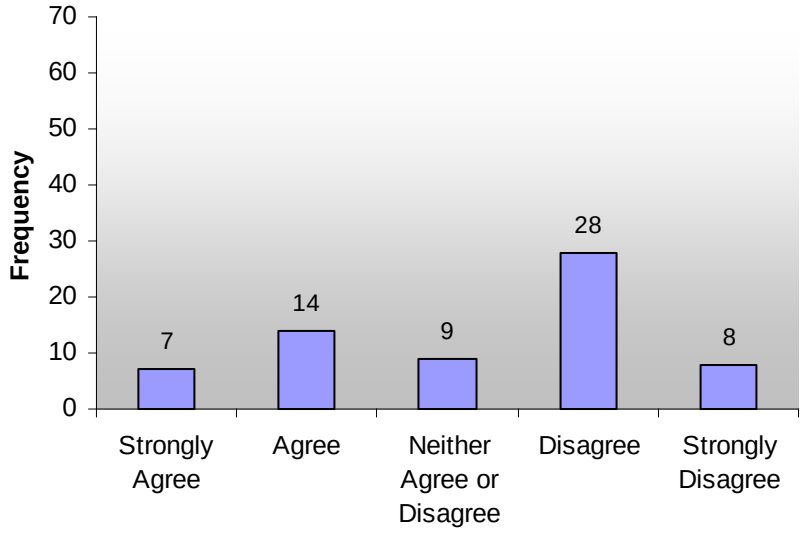


Figure 9.25 Staff securing their computers

21 respondents, (31%), say staff that violate security policies are formally disciplined. 9 respondents, (14%), were uncertain, while the majority of respondents, (55%) said there is no disciplinary process for violating security policies.

9.4.5 Section E: Physical and Environmental Security

This section explores the security of business premises and information systems contained within these premises must be ensured by providing a security perimeter and appropriate security controls. Core IT equipment such as servers and switches must be housed in safe and secure areas.

Question 26:

Our organisation contains high value, portable goods or stock items on the premises

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
17	25	3	9	11

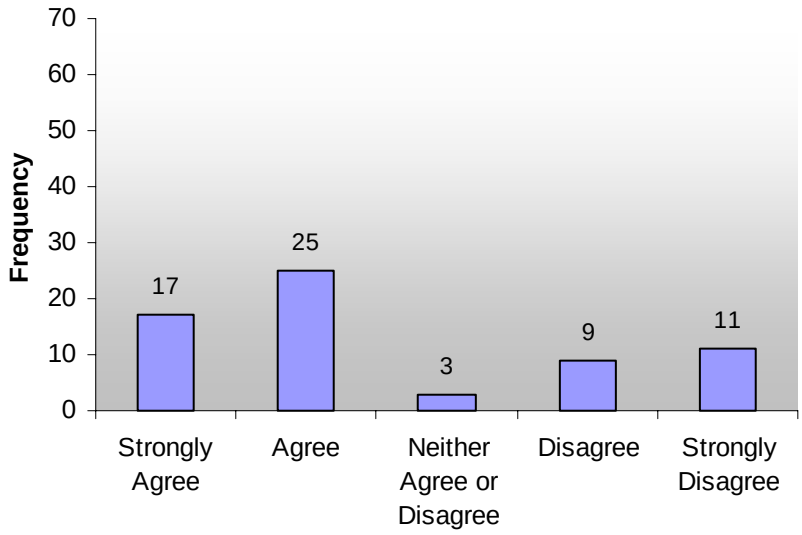


Figure 9.26 High value, portable goods on premises

42 respondents, (64%), claim that their organisations have high value / portable goods or stock items on the premises. Only 3 respondents, (5%), neither agree nor disagree with this statement. 20 respondents, (30%), claim their organisations do not have high value / portable goods or stock items on their premises.

Question 27:

We have appropriate Physical and Environmental security procedures in place to prevent interference with business premises and information systems

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
15	37	7	5	2

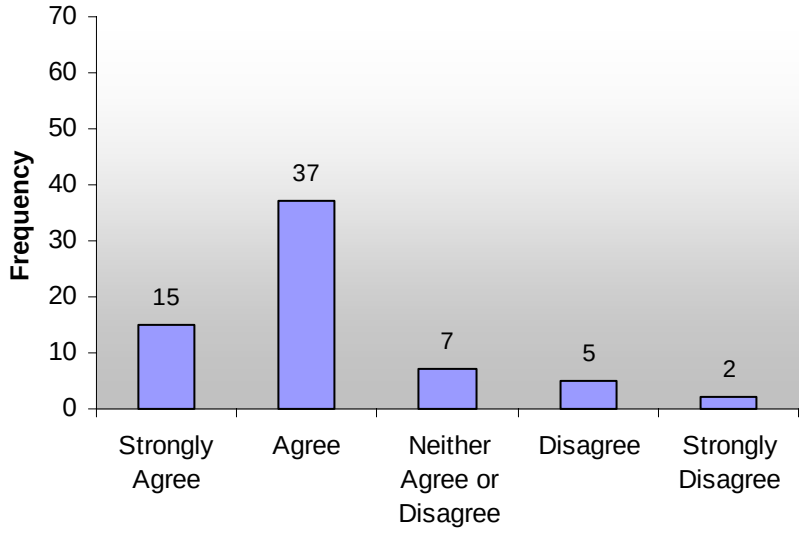


Figure 9.27 Appropriate Physical and Environmental Security

52 respondents, (79%), believe they have appropriate physical and environmental systems in place to protect information systems. 7 respondents, (10%) were unsure, and a further 7 respondents, (10%) do not believe they have adequate security in place to protect their information systems.

Question 28:

Staff that travel with portable computers, are aware of the risk relating to theft and the potential liability through compromised data.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
14	15	26	8	3

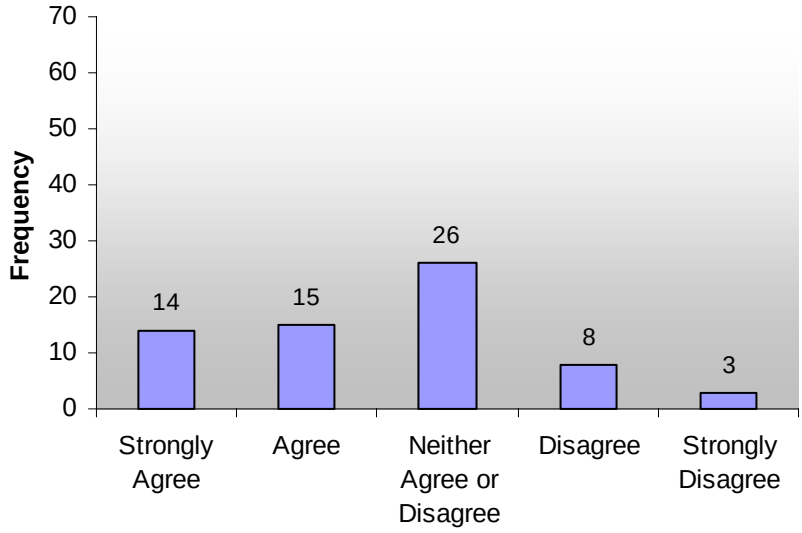


Figure 9.28 Risk awareness relating to portable computers

29 respondents, (44%), believe staff that travel with portable computers are aware of theft risk and potential liability through data falling into the wrong hands. 26 respondents, (40%) neither agree not disagree, and a further 11 respondents, (17%), believe staff to be unaware of the risk associated with portable computers and data loss / theft. It is believed the high percentage, (40%), of those, neither agreeing or disagreeing, are respondents who found this question to be inapplicable i.e. their staff do not travel / have portable computers.

Question 29:

Visitors to our organisation are always escorted around the building and are never left to wander around on their own

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
15	28	14	6	3

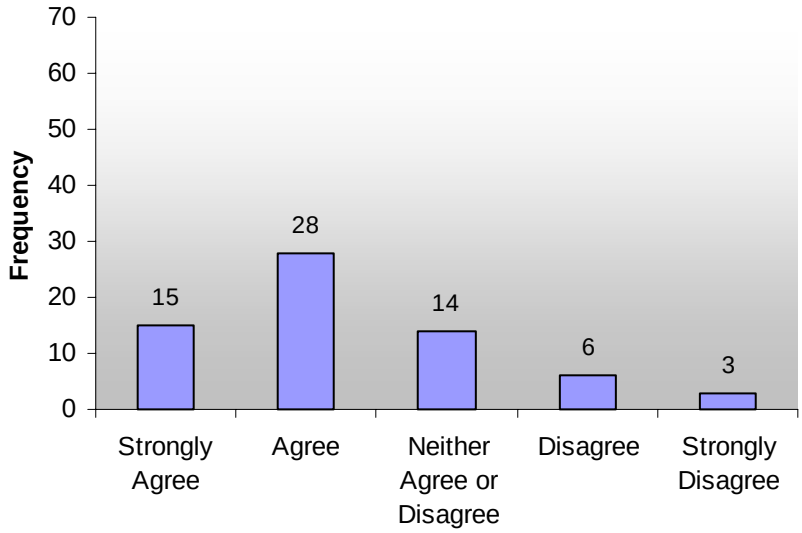


Figure 9.29 Visitors escorted around vs. left to roam around

43 respondents, (65%), claim to control visitor access to their organisation adequately, while 14, (21%), are unsure, and a remaining 9 respondents, (14%), do not believe they adequately control visitor access.

Question 30:

Our servers are maintained in air-conditioned, fire-retardant, power conditioned secure facilities.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
5	9	10	24	18

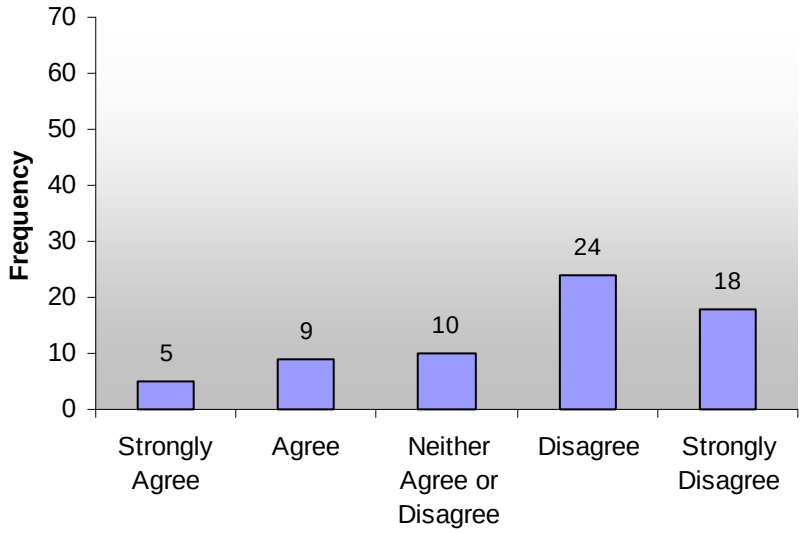


Figure 9.30 Appropriate equipment / server housing facilities

14 respondents, (21%), believe their servers to be maintained in air-conditioned, fire-retardant, power conditioned secure facilities. Ten respondents, (15%) neither agree or disagree with the statement, while 42, (64%), of the respondents do not believe their servers are housed appropriately.

9.4.6 Section F: Communications and Operations Management

This section explores the need for organisations to provide safe and secure information processing facilities. Operational instructions and incident response plans form a part of this. (SABS ISO/IEC 17799:2000)

Question 31:

We are confident, that in the event of equipment failure, theft or a site disaster, our data backups and storage would enable us to retrieve our information with minimal business interruption.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
12	24	10	16	4

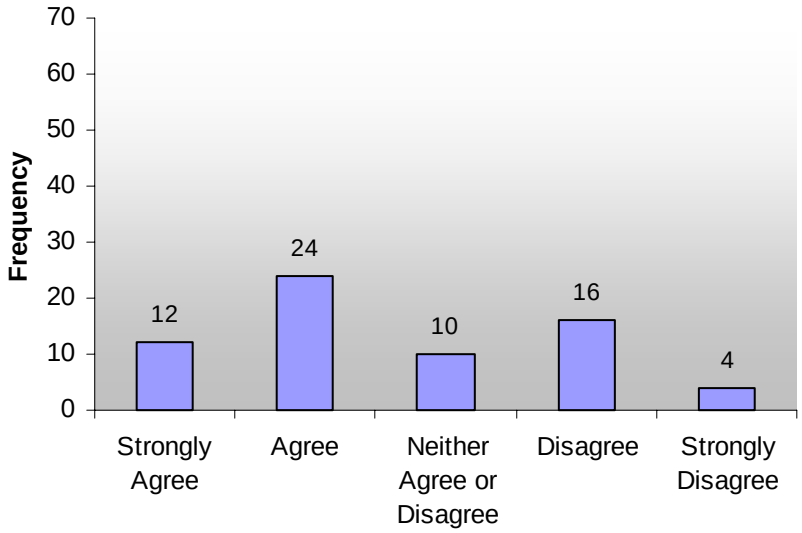


Figure 9.31 Appropriate protection through data backups / storage

36 respondents, (54%), are confident that their data backups and storage processes are of a high enough standard to enable their organisation to get back up on their feet with minimal business disruption, in the event of a site disaster or theft. 10 respondents, (15%) are unsure, and 20 respondents, (30%), do not believe their organisations could recover with minimal disruption.

Question 32:

Our systems are updated / upgraded according to a structured plan and not in an ad-hoc fashion.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
8	17	8	29	3

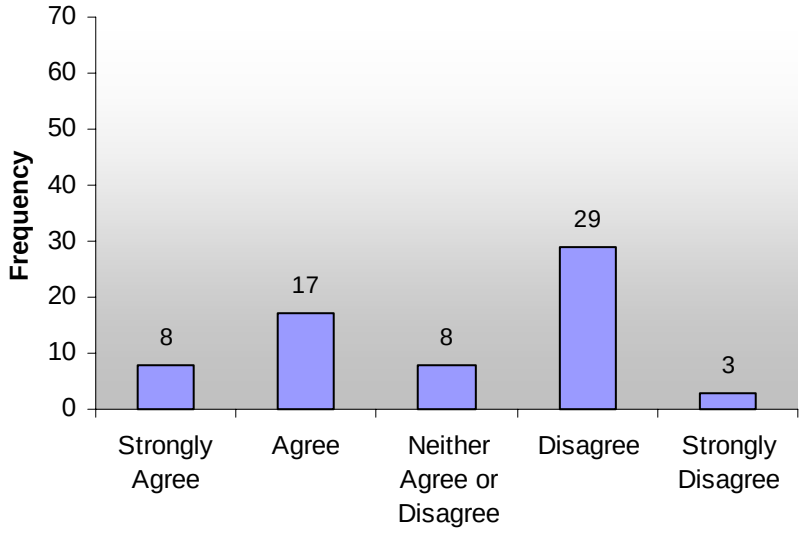


Figure 9.32 Use of system upgrade plan

25 respondents, (38%), suggest that their organisations upgrade systems according to a structured, planned process. 8 respondents, (12%) were unsure, and the remaining 32 respondents, (48%), suggest that their organisations do not follow a structured planning process to upgrade systems.

Question 33:

In the event of a security incident, procedures clearly define what to do and who to call for assistance

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
5	15	15	26	5

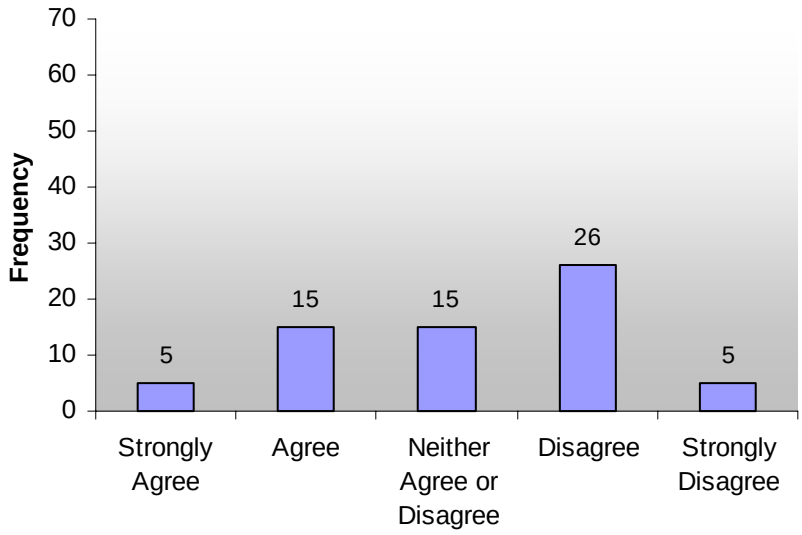


Figure 9.33 Security incident handling procedures

20 respondents, (30%), believe they do have procedures that specify what to do and who to call for assistance, in the event of a security incident. 15 respondents, (23%), were unsure, and 31 respondents, (47%), disagreed with this statement.

Question 34:

We are confident that our anti-virus systems are up to date, and in the event of a virus outbreak, we should be able to protect our systems as best as possible

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
28	27	7	3	0

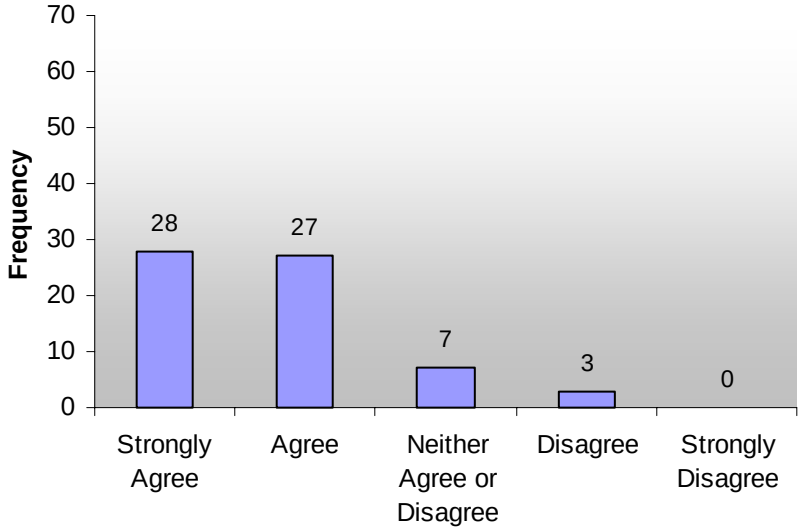


Figure 9.34 Confident that anti-virus systems are up to date

55 respondents, (83%), are confident that they enjoy sufficient protection from anti-virus systems. 7 respondents, (10%), are not sure, and only 3 respondents, (5%), do not believe their organisations enjoy sufficient protection from anti-virus systems.

Question 35:

Despite being connected to public networks, we are confident that our systems are adequately protected by our Internet Service Providers (ISP's) security and / or our own Fire walling systems.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
16	27	20	2	0

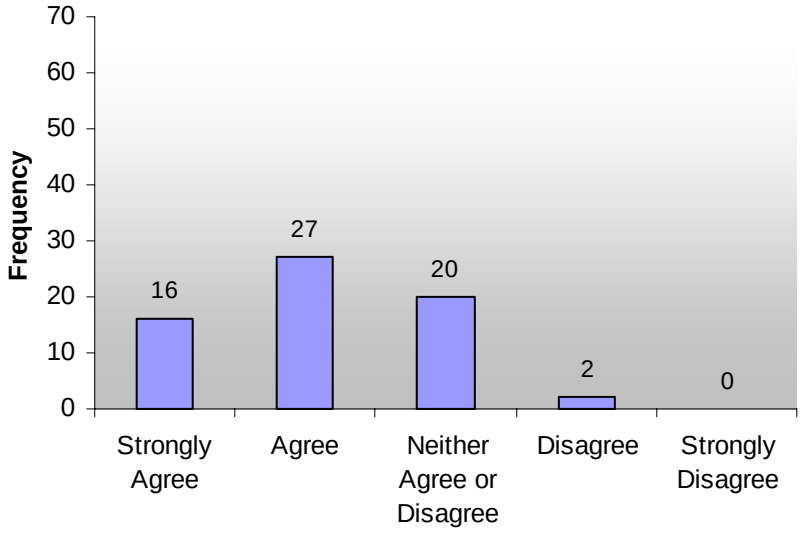


Figure 9.35 Confidence in ISP security protection

43 respondents, (65%), believe their Internet Service Providers, ISP's, and own fire walling systems provide adequate security protection to their organisations. 20 respondents, (30%) are unsure about this, and a further 2 respondents, (3%) do not believe this to be the case.

Question 36:

Appropriate mechanisms are in place to authenticate users logging onto our systems

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
15	28	9	11	3

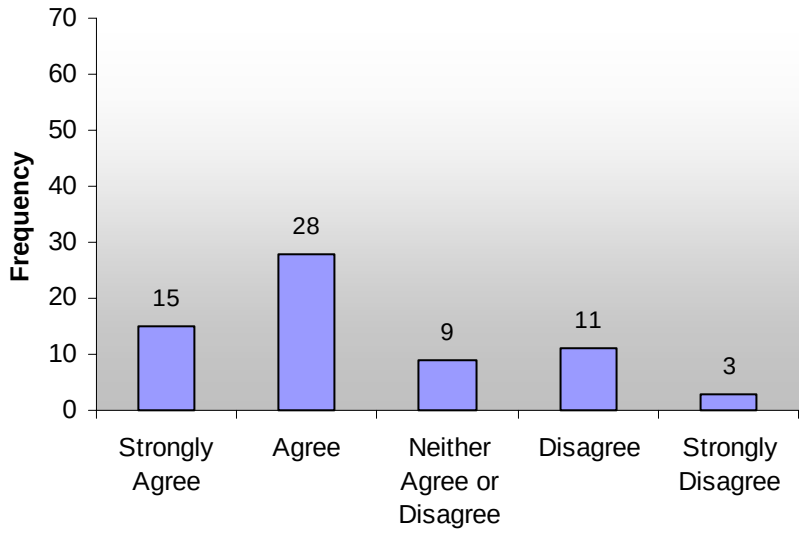


Figure 9.36 Mechanisms to authenticate user access

43 respondents, (65%), believe their organisations have appropriate mechanisms in place to authenticate users logging onto systems. 9 respondents, (13%), are undecided and 14 respondents, (21%), do not believe their organisations have adequate user authentication systems.

9.4.7 Section G: Access Control

This section explores the controls that are in place to manage access to information and systems. "Access to information, and business processes should be controlled on the basis of business and security requirements" (SABS ISO/IEC 17799:2000)

Question 37:

Users may not logon / gain access to our systems without being formerly registered with their own user account.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
16	18	20	10	2

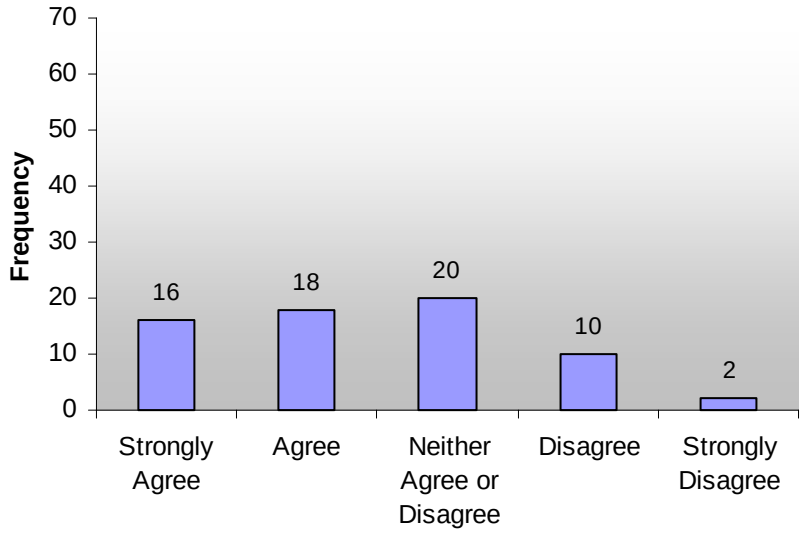


Figure 9.37 Users cannot access our systems without having their own account

34 respondents, (52%), believe their organisations control user access to systems through individual formal authentication methods. 20 respondents, (30%), are unsure, and 12 respondents (18%) do not believe their organisations control user access via individual formal authentication methods.

Question 38:

A password management system is in place which specifies the frequency of password changes as well as the minimum password complexity e.g. password must be changed every two weeks and be at least X characters long

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
7	7	7	25	18

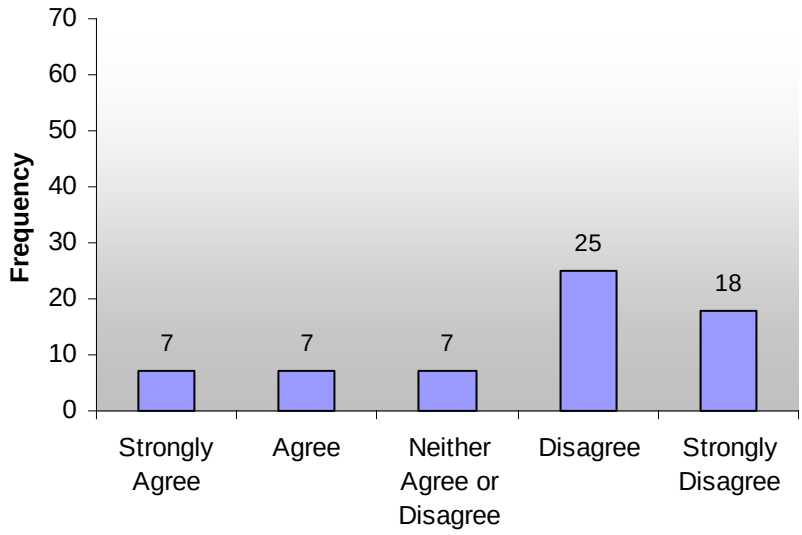


Figure 9.38 Presence of a password management system

14 respondents, (21%), believe their organisations have password management systems in place. 7 respondents, (11%) are not sure, and 43 respondents, (86%), disagree or strongly disagree with this statement.

Question 39:

Our organisation controls access to information via an access control policy which specifies which users have access to what data

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
8	11	13	27	7

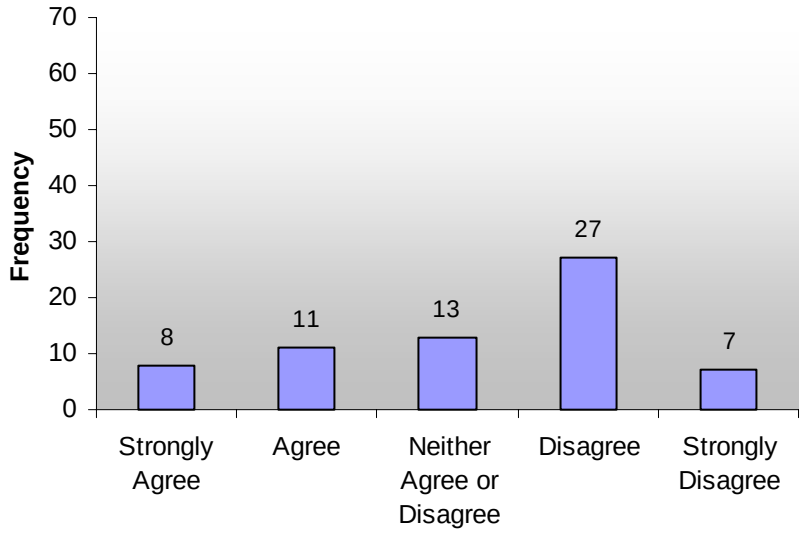


Figure 9.39 Presence of access control policy

19 respondents, (28%), believe their organisations control access to information via an access control policy. 13 respondents, (20%), are unsure and 34, (52%), do not believe their organisations control access to information through the use of an access control policy.

Question 40:

We ensure that information processing facilities are only used for authorised business purposes

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
13	28	10	13	2

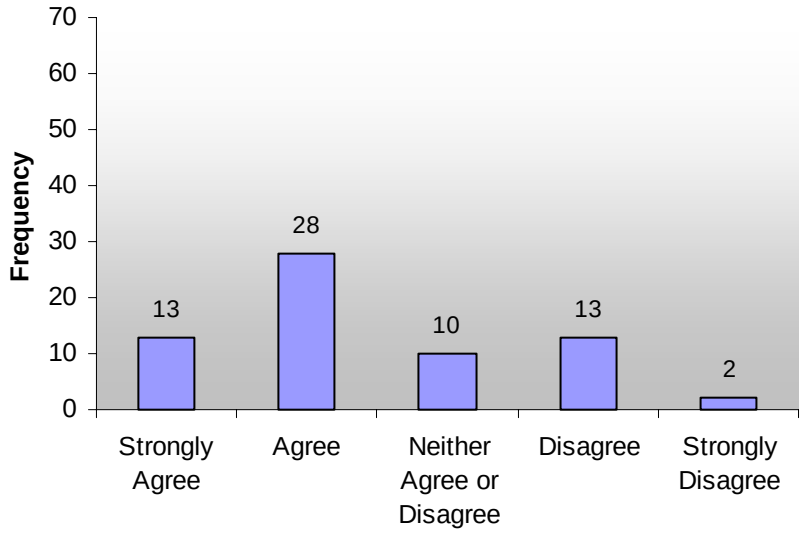


Figure 9.40 Information processing facilities only used for business purposes

41 respondents, (62%), believe that their information processing facilities are used for authorised business purposes only. 10 respondents, (15%), are unsure, and the remaining 15 respondents, (23%), do not believe their information processing facilities are used exclusively for authorised business purposes.

9.4.8 Section H: Systems Development and Maintenance

This section explores the security that should be built into information systems. "Security requirements should be identified and agreed prior to the development of information systems" (SABS ISO/IEC 17799:2000)

Question 41:

Our systems tend to be bought in, either as off-the-shelf software products or customised systems, outsourced from developers

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
24	35	4	2	1

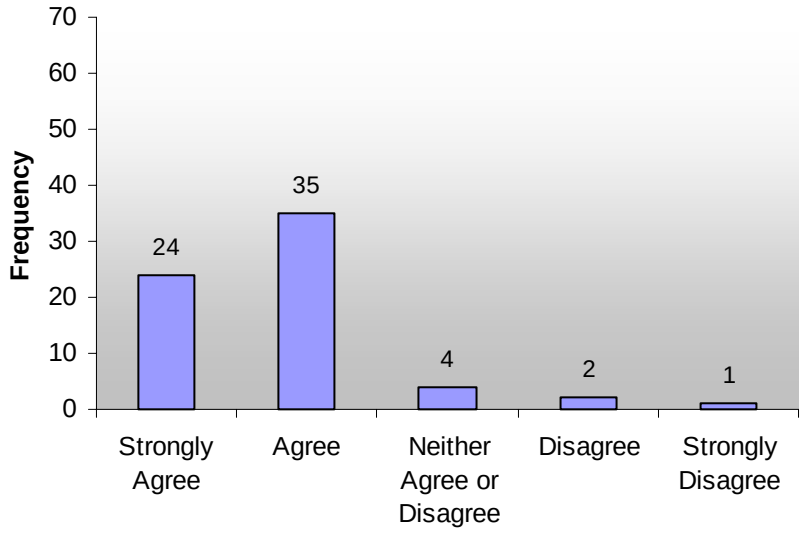


Figure 9.41 Off-the-shelf / outsourced vs. in-house developed systems

59 respondents, (89%), agree / strongly agree that their systems are bought in as off-the-shelf systems or custom built by external developers. 4 respondents, (6%), were unsure, and 3 respondents, (5%), disagree / strongly disagree with this statement.

Question 42:

We are aware that systems need to provide audit trails so that usage of the system and data input / changes can be audited

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
15	26	12	7	6

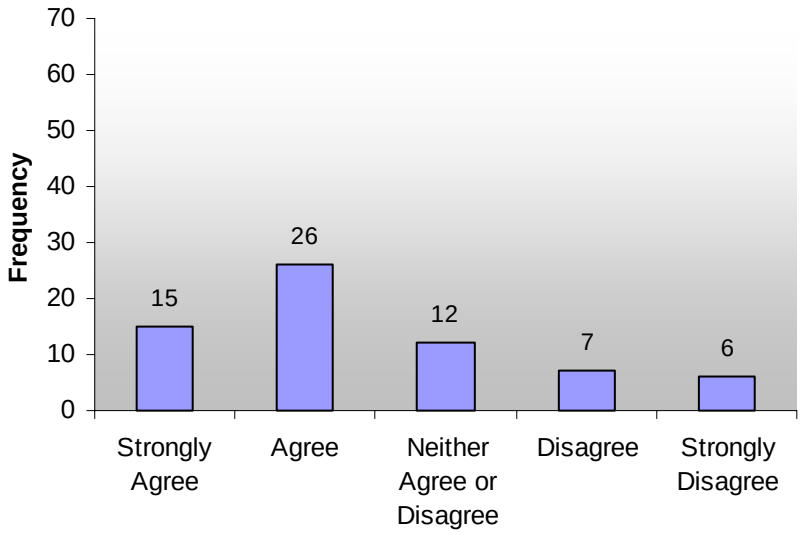


Figure 9.42 We are aware that systems need to provide audit trails

52 respondents, (79%), agree or strongly agree with the statement that systems require audit trails so that data input / changes can be audited. 12 respondents, (18%) are unsure, and the remaining 13 respondents, (20%), either disagree or strongly disagree with the statement.

9.4.9 Section I: Business Continuity Management

This section explores business continuity management process that is put in place to counteract business disruption / failure, in the event of a disaster or security failure (SABS ISO/IEC 17799:2000).

Question 43:

We have a business continuity plan which specifies who must take what action and what has to be done to ensure that the organisation can continue functioning in the event of a disaster such as a fire / flood.

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
6	13	7	30	9

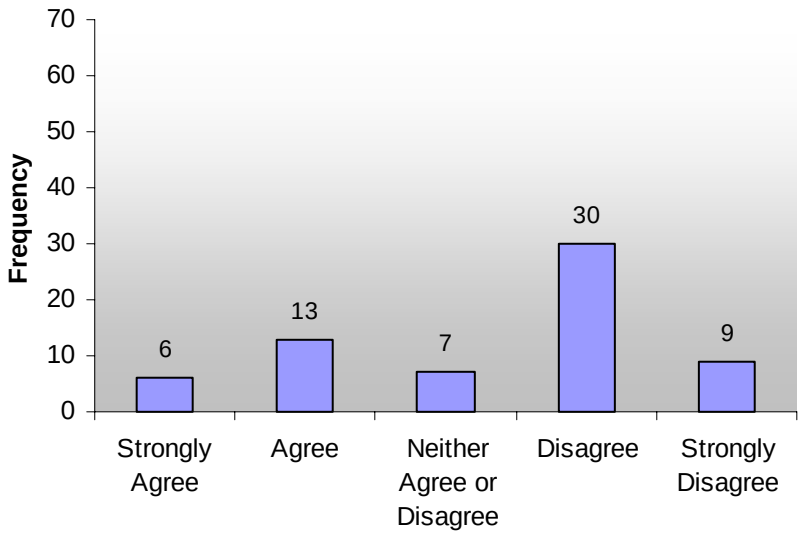


Figure 9.43 Presence of Business Continuity Plan

19 respondents, (29%), believe their organisation have a business continuity plan. 7 respondents, (11%), are unsure, and 39 respondents, (59%), suggest they do not have a business continuity plan.

Question 44:

There is a nominated person in our organisation that is responsible for managing the business continuity process

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
12	30	8	13	3

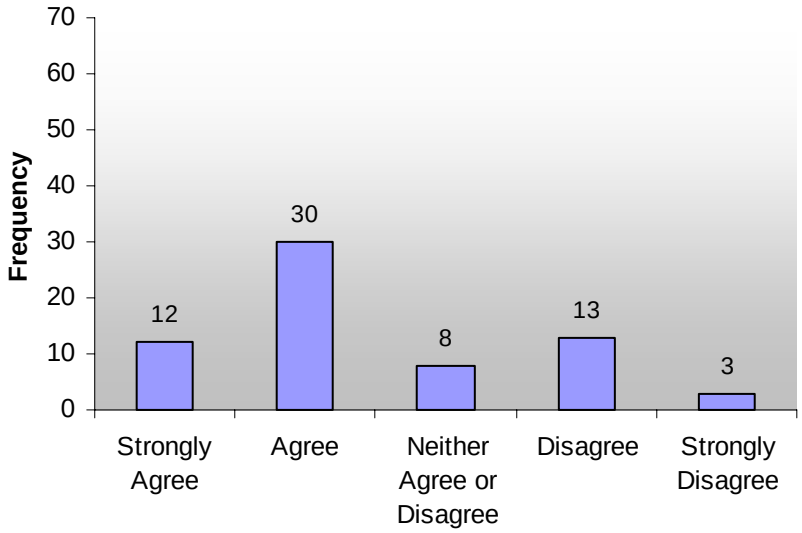


Figure 9.44 Person nominated to manage business continuity process

42 respondents, (64%), believe they have a nominated person to manage the business continuity process. 8 respondents, (12%), are not sure, and the remaining 16 respondents (24%) claim that they do not have a nominated person to manage the business continuity process.

Question 45:

Our security measures have been reviewed within the last year

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
11	16	4	29	5

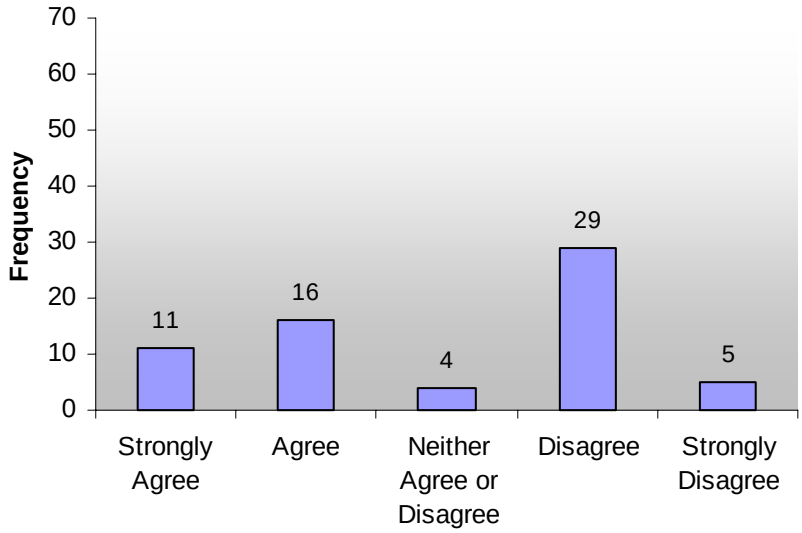


Figure 9.45 Security measures reviewed within last year

27 respondents, (41%), believe that their organisations security measures have been reviewed within the last year. 4 respondents, (6%) are unsure, and 34 respondents, (52%), do not believe their security measures have been reviewed within the last year.

9.4.10 Section J: Compliance

This section explores business compliance in terms of statutory, regulatory and contractual requirements that business must address when designing and implementing information systems and Security.

Question 46:

Prior to this survey, I was aware that there are established, International information security standards, available for organisations to adopt

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
6	15	10	14	20

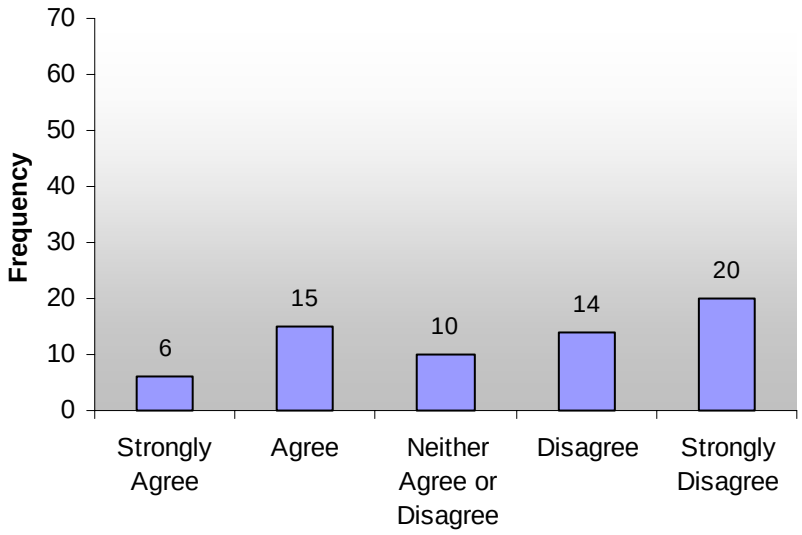


Figure 9.46 Awareness of International security standards

21 respondents, (32%), claim to have heard of International information security standards that are available for organisations to adopt. 10 respondents, (15%), are unsure and 34 respondents, (52%), claim not to have heard of International information security standards.

Question 47:

I have heard of the following information security standards:

Not aware of any standards	SABS ISO/IEC 17799 Part 1.	SABS 17799-2	NIST SP 800 Series	RFC 2196: Site Security Handbook	Other (please specify)
50	14	5	0	3	1

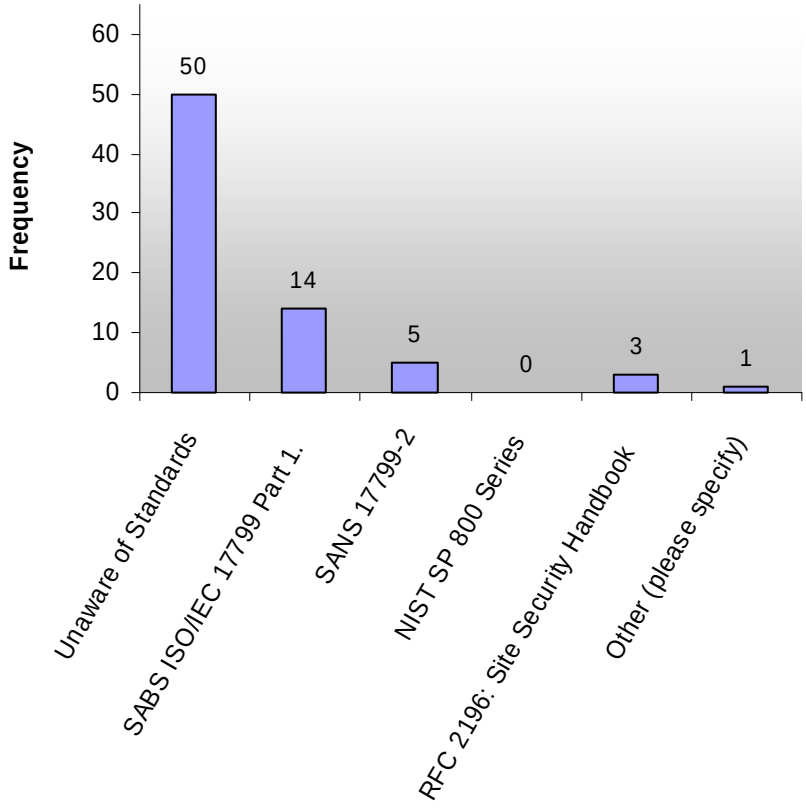


Figure 9.47 Awareness of specific security standards

50 respondents, (76%), have not heard of standards. 14 respondents, (21%), have heard of SABS ISO/IEC 17799 Part 1. 5 respondents, (8%), have heard of SABS 17799-2. No respondents knew of the NIST SP800 framework while 3 respondents, (5%), have heard of RFC 2196: Site Security Handbook and 1 respondent claimed to have a "security gentleman" who looks after their systems and follows all security standards.

Question 48:

Our organisation has suffered the following security breaches in the last 12 – 18 months.

No security breaches	Inadvertent breaches	Deliberate Attack	Asset theft	Equipment failure	Backup failure	Data theft	Site Disaster	Copyright infringement	Compliance	Other
32	22	2	5	23	4	2	0	2	0	2

Failures listed as other:
Viruses and Power Failure
Failure due to poor outside technical assistance

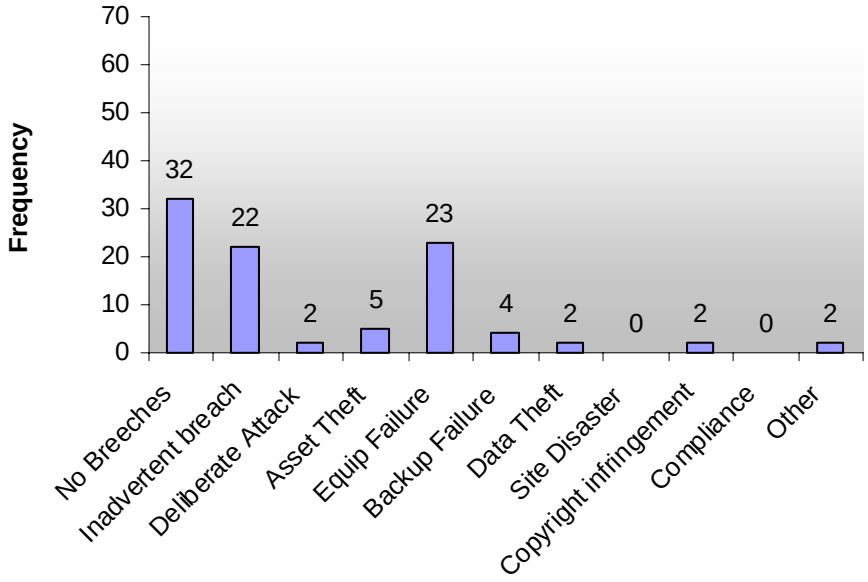


Figure 9.48 Security breaches suffered

32 respondents, (48%), reported suffering no security breaches while 22 respondents, (33%), reported having suffered from inadvertent breaches. Only 2 respondents, (3%), said they had experienced deliberate attacks and 5 respondents, (6%), said they had suffered from asset theft. Equipment failure such as a hard drive 'crashing' was

reported by 23 respondents, (34%). Only 4 respondents, (6%), reported having suffered backup failure while 2 respondents, (3%), said they had lost data through theft. A further 2 respondents reported infringing copyright. Finally 2 respondents, (3%), suggested they had suffered from viruses, power failures and poor outside technical assistance.

Question 49:

Information security is an issue that SME's should be concerned about

Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
33	30	3	0	0

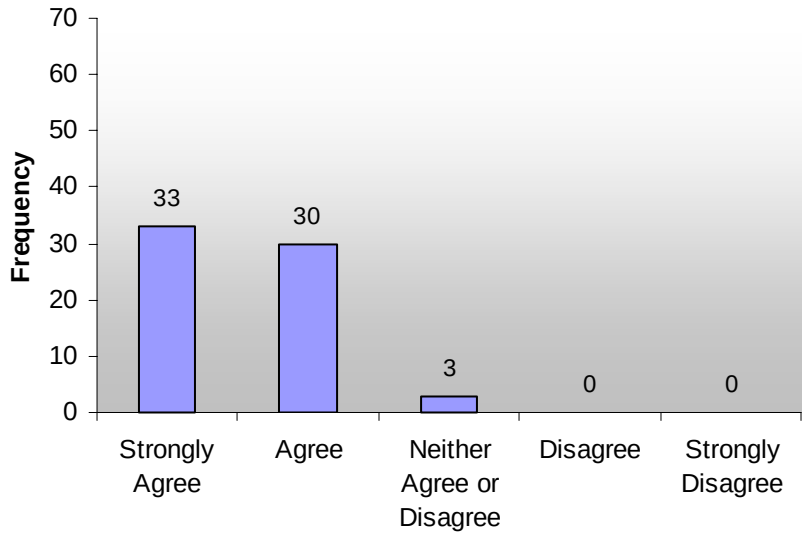


Figure 9.49 How SME's regard information security

33 Respondents, (50%), strongly believe that information security is an issue that SME's should be concerned about. A further 30 respondents, (45%), agree with this. 3 respondents, (5%), were indifferent.

9.5 Conclusion

The decision to administer the survey using both a web and paper based delivery system, worked well. The response rate to the paper based survey in Grahamstown was very good due to the researcher being able to meet personally with respondents,

and follow-up when necessary. The Web based delivery system worked well, especially being able to embed a link to the Perception server in email that was sent to respondents. (A copy of the email sent to respondents is in Appendix B). Of concern, was the number of respondents who started the Web survey, but never finished it? The Perception server logged several respondents who started the survey, some up to four (4) times, before finally completing it. The submit button was at the end of the questionnaire and this ensured that questionnaires were completed. Respondents were able to omit answering a particular question. This was not a concern in the Web survey, however, question 4, which explored annual turnover, received a poor response rate in Grahamstown. The researcher believes that certain questions may have a lower expectancy of being answered, but this should not detract from the question being asked if it is considered pertinent to the research.

Chapter 10: Analysis and Recommendations

Abstract

The previous chapter detailed the results of the survey. This chapter explores further the meaning and implication of the results obtained in Chapter 9. In addition, recommendations are made in terms of each of the ten (10) SABS ISO/IEC 17799 Security Domains in the context of information security in SME's.

10.1 Introduction

The approach taken for this chapter is to comment and make recommendations based on each of the 10 Control Domains which form the basis of SABS ISO /IEC 17799. Line graphs are used to indicate individual question responses to each of the Control Domains. Where there appears to be conflicting security practice in a Domain, this is indicated by a red column with arrows. (See figure 10.1)

Throughout this research, it is apparent that:

- Issues that SME owners / managers think are being addressed, quite often are not.
- Issues that are not being explicitly addressed, operationally / practically are to some extent, being addressed.
- Issues that may appear as irrelevant / unimportant to SME owners / managers may in fact, be critical, given certain circumstances.

10.2 Security Domains

10.2.1 Section A: Security Policy

SME owners / managers argue that their information security roles and responsibilities are well defined. SME's usually have a staff member who is responsible for performing tasks such as registering new users, supervising password changes, performing backup's and so on. Some respondents outsource these tasks. Only 18% of the respondents said they have policy documents, and over half the respondents, (54%), suggest staff are unaware of information security policies. 57% said that information security education and training is lacking. Despite a lack of staff training and no policy documents to serve as the basis for establishing guidelines, procedures and best practices, the majority of respondents believe their personnel are aware of what constitutes acceptable use of facilities and what does not.

More than one SME manager suggested staff are aware that Internet / email abuse is not tolerated or at least not acceptable.

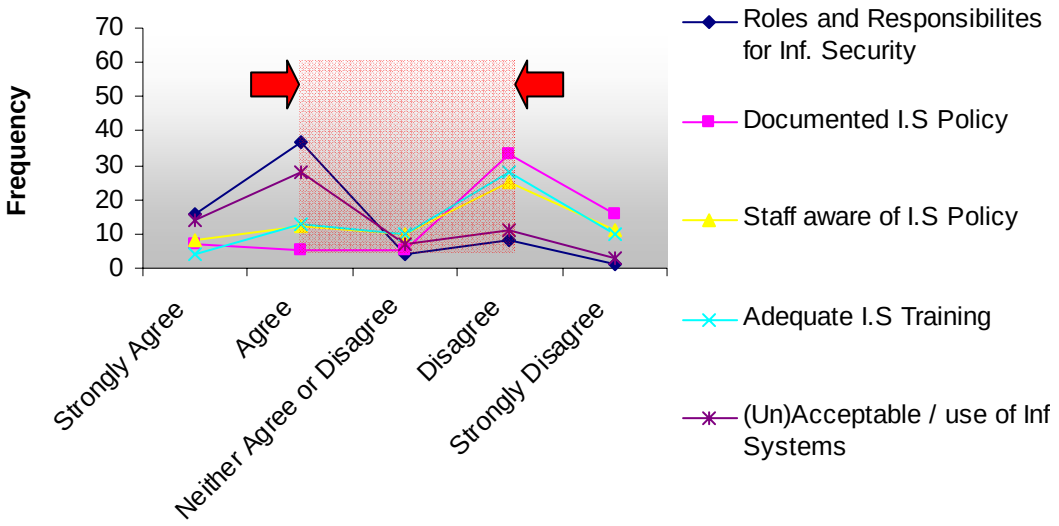


Figure 10.1 Gap between what is practiced and what is not.

Figure 10.1 indicates a gap that exists between what respondents consider to be addressed correctly, (roles and responsibilities for information security and acceptable use of information systems), and what is considered to be lacking, (information security training, information security policy documents and staff awareness of information security policies). This is indicated in Figure 10.1, (red column). The researcher found some SME managers dismissive of the need to formalise policies. Of concern, is the superficial nature in which various tasks are carried out, and assumptions made, and yet the high levels of information security confidence expressed by some SME managers.

SME owners / managers insist their organisations run regular backups. When probed on backup procedures, it became apparent that backups are not quite so regular and that no backup procedure policy is in place. Very few respondents could say that backups are taken off site or stored in a fire-proof safe, on-site. Some SME managers, surprisingly, are unsure of where their backups are stored. Having determined that one organisation had not backed up their systems for several months, the researcher asked the SME owner what he would do if his computer system failed or was stolen?

His reply was that he would sit on the pavement and cry. Another respondent, himself an accounting service provider in Grahamstown, told the researcher that he had given up trying to convince his clients, mostly SME's in Grahamstown, to keep their debtors information properly backed up, and preferably on a separate computer from the rest of their accounting systems.

Recommendations:

SME management have the perception that information security policies are hard work and expensive, requiring expertise from outside consultants, and resulting in an unwieldy, complex document. SME's must consider information security policies, which should be seen as lightweight, living documents, 2-3 pages, that address various issues pertinent to SME's. These policies are issue-specific policies and must be aligned to the overall corporate security policy which is the overriding higher level security policy governing the organisation. Examples of issue-specific policies are detailed below:

- Acceptable use policy:
  - personal email use
  - downloading of documents / images and multimedia files
  - installation of personal software
  - information ownership
- System and Data security policy:
  - Password selection, length and change frequency
  - Use of antivirus tools
  - Storage, dissemination and disposal of data
  - Transportation of data i.e. laptop usage
- Data Backups:
  - Person responsible for administering backups
  - Identification of data sets requiring backup
  - Methodology and frequency of backups, daily, weekly, monthly
  - Backup storage
  - Period of storage
  - Recovery testing

Security policies must be aligned to the business. By writing security policies, processes that are perhaps taken for granted, will be obviated, formalised and in some cases revised. Staff should be involved in the process of generating the policies. Many SME's outsource their information systems. Service Level Agreement, (SLA), are policy documents that provide SME's with recourse when a service provider fails to deliver / delivers a poor service.

Constructing information security policies must not be seen as insurmountable. There are numerous, freely available web sites that provide template documents, with explanations, specifically aimed at assisting small and medium business construct policy documents such as those mentioned.

10.2.2 Section B: Organisational Security

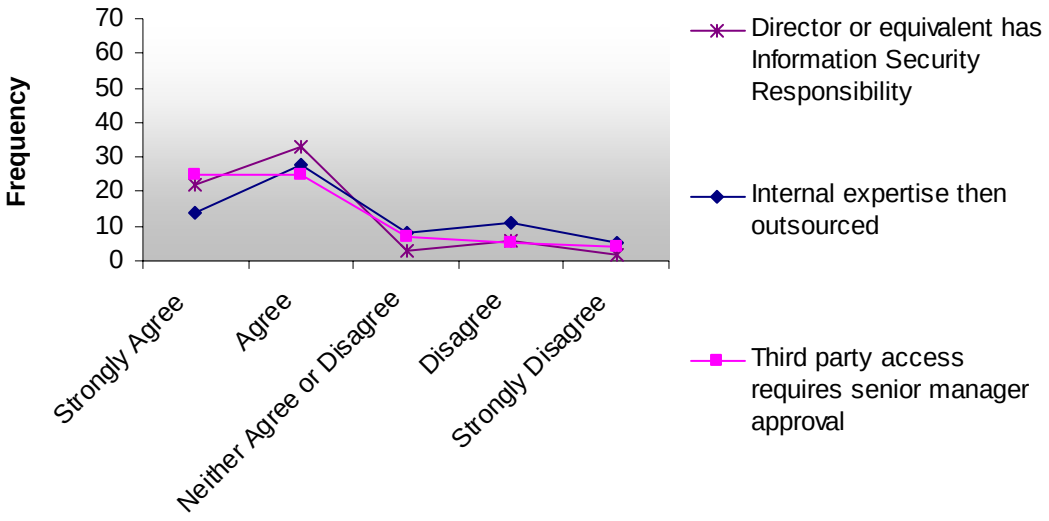


Figure 10.2 Overlay of Organisational Security Questions

Figure 10.2 indicates responses to three organisational security questions presented in the survey. Question 17 probed whether or not a director or person with similar status held responsibility for information security. An overwhelming 87% suggested that this was the case. Whereas a large business may delegate information security to a technical administrator, the nature of SME's generally means the owner / partner is involved in day to day operational decisions which include information systems and

security. Question 18, explored whether information security expertise was available internally and where not, external advice was sought. Respondents found this question confusing, and asked whether it should not be one or the other. Of those respondents who did not agree or strongly disagreed, it cannot be determined whether they meant:

- when the organisation runs out of internal expertise they do not call in outside assistance, or,
- the organisation does not have internal expertise and only uses outside expertise, or,
- the organisation does not have internal expertise and does not use outside expertise either.

This question should be revised if this survey is to be re-used.

Question 19, explored whether or not senior management would have the final say, in granting approval to a third party for access to their information systems. 75% of the respondents said this was the case. When respondents were asked about the nature of their computer transactions, 43% suggested they engage in Electronic Commerce, 35% specified selling services to customers via the Internet, and 18% suggested the use of Electronic Data Interchange (EDI). These responses are higher than anticipated, and respondents believe 3rd party access to information systems is well controlled.

Recommendations

The majority of SME's have information systems that are isolated from external 3rd party access, however, an increasing number of SME's are engaging in some form of E-Commerce / EDI. These SME's are collaborating and when necessary, outsourcing to service providers. 89% of respondents agree / strongly agree that their systems are bought in as off-the-shelf systems or are externally developed for them. The outsourcing of systems and technical expertise, does not absolve the responsibility that directors / senior managers have towards their organisations, however. When a senior manager / director grants information access to a 3rd party, irrespective of whether it is a small accounting firm "doing the books" or a third party developer

establishing an E-Commerce / E-Business site, he / she must follow up and ensure that:

- Information confidentiality agreements are signed
- Firewalls are in place and regularly updated
- Systems are correctly service patched to mitigate against vulnerabilities
- Some form of penetration testing is conducted by an independent party to ensure that appropriate security is in place
- Service Level Agreements (SLA's) are signed, and up to date

10.2.3 Section C: Asset Classification and Control

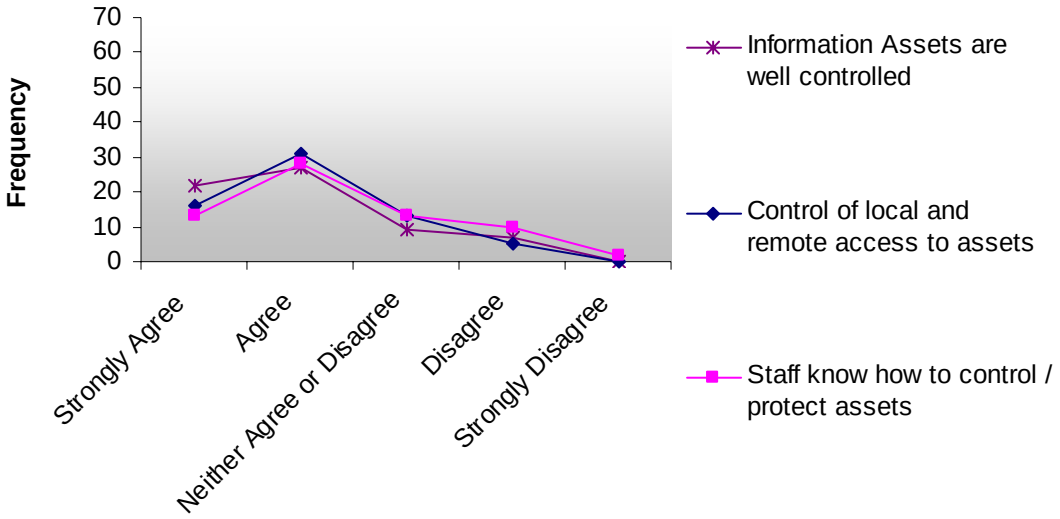


Figure 10.3 Overlay of Asset Classification and Control Questions

Given the size of the SME's surveyed, (33% employed between 11-25 staff followed by 28% employing between 0 - 10 staff), it is not surprising that all assets: hardware, software, staff and services can be located. Question 21, not dissimilar to Question 19 in Section B, explored the control of local and remote access to information assets. This question, received a favourable response. Question 22, explored whether respondents felt that staff know what to do when it comes to storage, usage, archiving, backup and destruction of information. Although 41 respondents, (62%) say that staff do know what to do, 12 respondents, (18%), argue that this is not the case. Given the responses to Section D, Questions 24 and 25, (Staff leaving computers open and

unattended and no disciplinary process for violating security processes), there is cause for concern. Surely, if access to information assets is correctly controlled, staff should be aware of the vulnerabilities facing the organisation. Again, surely this awareness would be raised by information security training and disciplinary repercussions for not following procedures within the organisation. According to the survey, both these areas are lacking.

Several of the SME's surveyed, were in the financial services sector. These included accounting firms as well as financial brokers. Both these types of business are audited by external bodies and have to demonstrate compliance with stringent regulations regarding information usage, security and control. It is not surprising that the control of information assets within these businesses is good.

Recommendations

As recommended in Section A, policies must stipulate staff conduct when it comes to working with information assets. Management must ensure that relevant issues in the ECT Act should be conveyed to employees through company rules and regulations. Staff must be aware of the legal ramifications of information abuse / inadvertent or deliberate disclosure.

10.2.4 Section D: Personnel Security

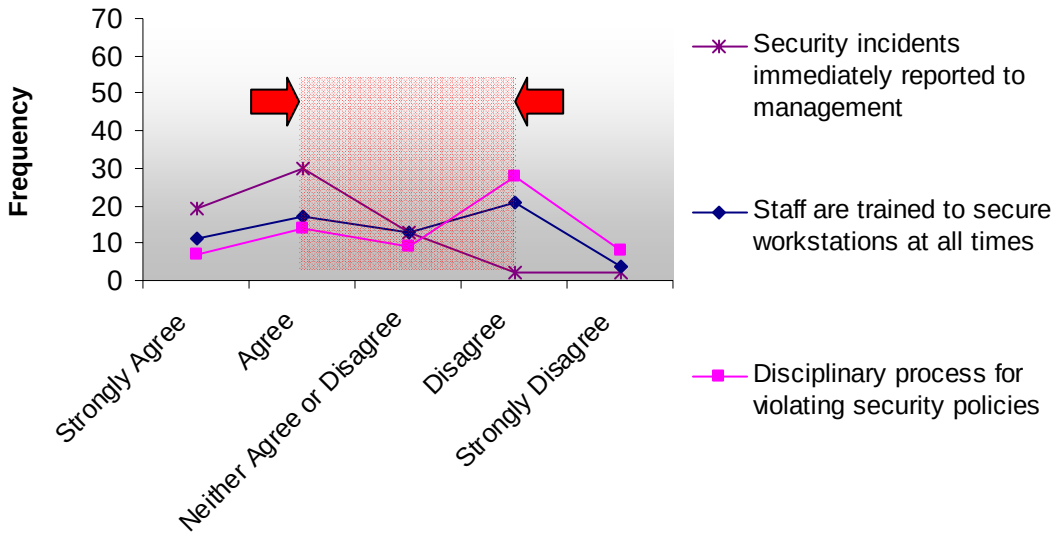


Figure 10.4 Security incidents, staff training and staff discipline

Figure 10.4 indicates a gap between what respondents say is being done and what is being neglected. 74% of the respondents say that staff immediately report security incidents to management. This is important, as in the case of an exploit being detected, time is of the essence. Security incidents need not only be hacking attempts or viruses. A high percentage of security incidents are brought about through social engineering. Again, a staff member being able to discern this is vitally important. Of concern are the 25 respondents (37%) who did not feel that staff secured their computers when moving away, and 36 respondents, (55%) who denied having any form of disciplinary process for staff that ignored security processes.

SME's generally operate with a small number of staff and a high level of co-operation. Although a culture of co-operation and teamwork must prevail within a SME, it is essential that staff understand the repercussions of lax discipline resulting in compromised security.

According to the PricewaterhouseCoopers DTI information security breaches survey (2004), companies that had recently connected their networks to the outside world, reported being scanned for vulnerabilities on a daily basis.

Recommendations

In the context of information security, personnel security starts with education / training and ensuring that personnel:

- Are conscious of visitors who may be peering over shoulders / eavesdropping to gain information illegitimately.
- Know that information left on a desk, on a printer, or data on a computer that has been sent in for repairs, could be critical to the organisation
- Understand that by creating a share on a computer, however temporary and urgent this may be, may provide a backdoor to someone scanning for an exploit opportunity
- Ensure that all work including work in progress is saved back on the server so that it can be backed up

- Ensure that backups are executed and tested according to a policy

Ultimately, SME's must ensure that staff are trained and stay vigilant when it comes to information security. Like staff in financial broking SME's, staff in other SME's must realise that information security is not a choice but a legal, ethical and operational requirement that could mean the difference between business continuance and failure.

10.2.5 Section E: Physical and Environmental Security

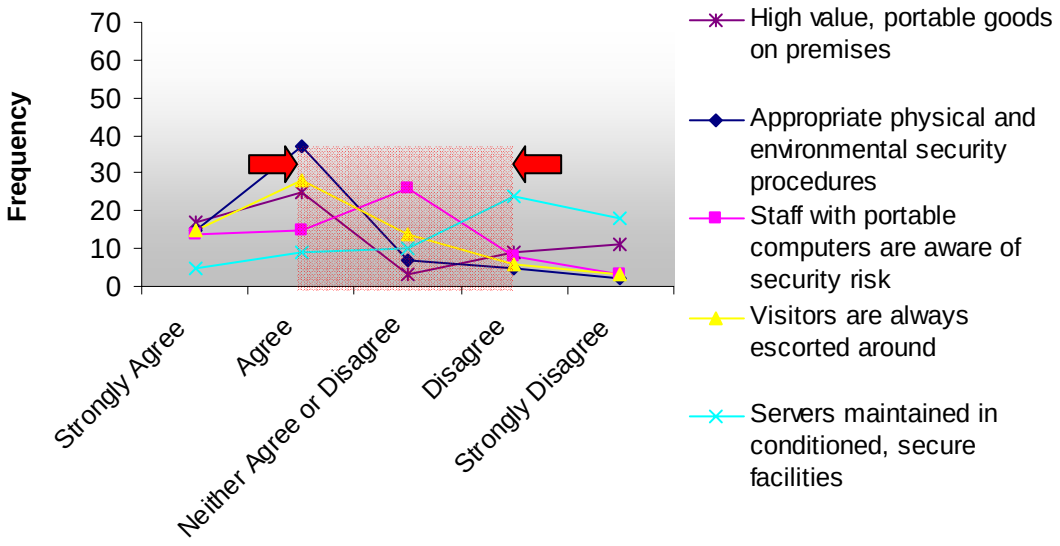


Figure 10.5 Physical and environmental security as reported in survey

64% of respondents believe their organisations have high value portable goods on the premises. 79% believe their organisations have appropriate physical and environmental security procedures in place to prevent interference with business premises and information systems. According to a FPI information security survey, laptop theft is one of the most common compromises of information security (Whitman and Mattord, 2003). It is interesting that only 11 respondents, (17%), believed this to be a problem. 29 respondents, (44%) believe staff are aware of the risk relating to laptop theft. A high percentage of respondents neither agreed nor disagreed. On investigation it became apparent that the majority of these respondents did not have laptops in their SME's. It is encouraging that 65% of the respondents

escort visitors around the building and do not let them wander around on their own. Finally, the majority of SME's do not have dedicated server facilities with conditioned power and air and restricted access.

Recommendations

As SME's develop their technical infrastructure, so will the need increase for appropriately equipped facilities. This not only includes servers, but also network equipment. Although not explored in the survey, environmental security also includes network security, irrespective of cabling type or wireless equipment being used. It is essential that SME's stay up to date with current state of security practice.

10.2.6 Section F: Communications and Operations Management

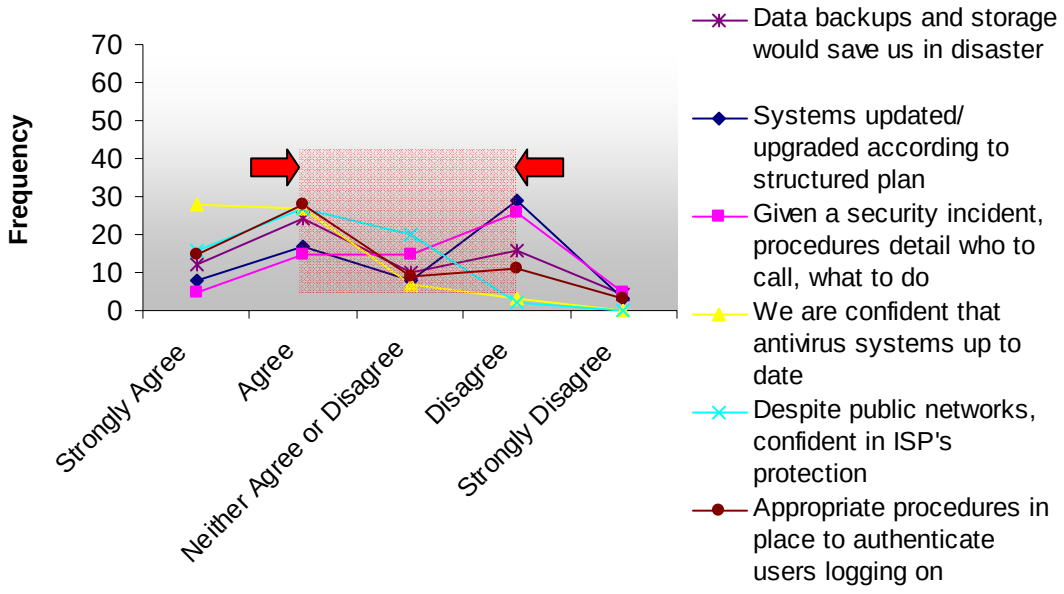


Figure 10.6 Communication and Operations security issues

83% of respondents say they have utmost confidence in their anti-virus systems. This is one of the most convincingly answered questions in the survey. Given widely publicised business disruption costs caused by viruses in recent years, it would seem that anti-virus software is a non-negotiable for SME's. Only 5% of SME's surveyed, felt unsure about their virus protection. SME's also believe that their Internet Service Providers (ISP's) are doing a good job of protecting their systems. With 54% of the respondents saying their backups would get them out of trouble, and 30% saying they

disagreed with that, the question on data backups, storage and retrieval confidence was not convincingly answered. It is encouraging that most SME's are doing backups but as mentioned previously anecdotal evidence would suggest backup processes are in many cases, superficial and untested. Only 38% of SME's plan their system upgrades. Given the ad-hoc infrastructure seen in many SME's as well as budget constraints, this result is not surprising. As SME's increase their investment in information systems and Technology, it is expected that budgeting processes will force a more structured maintenance and procurement plan. 47% of respondents said that in the event of a security incident, they do not have procedures that clearly define who to call for assistance.

A further 23% were not sure. This is interesting considering that 56% of the respondents in Question 12 reported that roles and responsibilities for information security are well defined. 65% of the respondents believe they have appropriate mechanisms in place to authenticate users logging onto systems. 21% of the respondents would disagree with this.

Recommendations

SME's must not assume that up-stream Service Providers are infallible when it comes to preventing viruses / hacking attempts. Outsourcing presents a real opportunity to SME's but may also leave them exposed, especially if their service provider lapses in quality of service (QOS). SME's must continually question security, and strongly consider the use of a firewall between themselves and any service providers / public networks. Data backups, as discussed in Section A, cannot be compromised. When all else fails, backups present the business with a last ditch opportunity to recover critical data. Just as SME's consider anti-virus solutions as non-negotiable, so they should, data backups. SME's must consider file server operating systems that provide centralised user accounts with password management and policy controls. These systems are increasingly simplified, with the use of templates to perform certain functions, and some of these products have been streamlined specifically for SME's.

10.2.7 Section G: Access Control

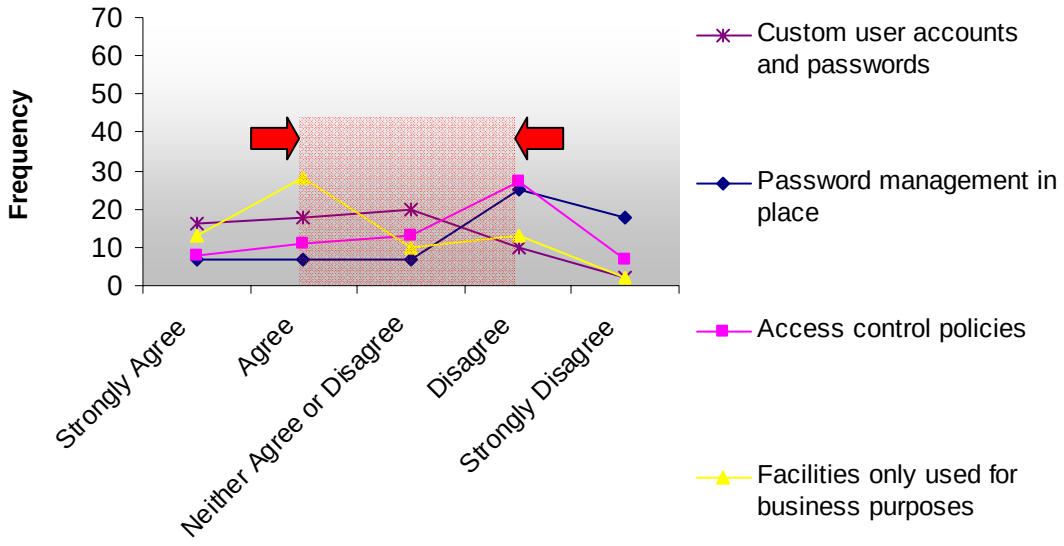


Figure 10.7 Access Control

52% of the respondents said user access to systems is restricted through own accounts and passwords. 18% disagreed with this and an alarming 30% were unsure. Throughout the survey, most questions had, a Neither Agree nor Disagree response rate of about 12%. The assumption is made, therefore, that an additional 12 respondents (18%) did not understand the question and probably do not use personal accounts and passwords to access their information systems. This assumption is enforced by the response to Question 38, which explores whether or not a password management system is in place. 86% of SME's said they do not use a password management system. The response to Question 39 is also poor with 52% of SME's not using access control policies to govern which users have access to what data. 41 respondents, (62%) said their information processing facilities are only used for authorised business purposes with 23% disagreeing with this.

Recommendations

At start-up, SME's are usually under-resourced, and to get the job done invariably end up with ad-hoc systems that have been crafted together. As SME's grow and take on additional staff, managers / owners must recognise the need to formalise their

systems, which includes tightening up on systems access. Attempting to control who has access to what resources without a centralised user management system, quickly becomes unmanageable. This results in staff ignoring basic security such as individual accounts logons and passwords. The recommendation is that SME's must procure a Network Server Operating System. As mentioned, most current state-of-practice network server operating systems, provide for centralised user accounts with password management and access control policies as standard offerings.
Once installed, access to information systems is not possible without valid user accounts and passwords. Password policies can be set, enforcing password changes frequency and password criteria, such as minimum length and special characters. Furthermore, most of these systems provide comprehensive auditing facilities whereby log files indicate: the identity and time that users have logged on and off, what directories and folders have been accessed and more importantly, what attempts have been made to access directories and folders that users do not have rights to.

10.2.8 Section H: Systems Development and Maintenance

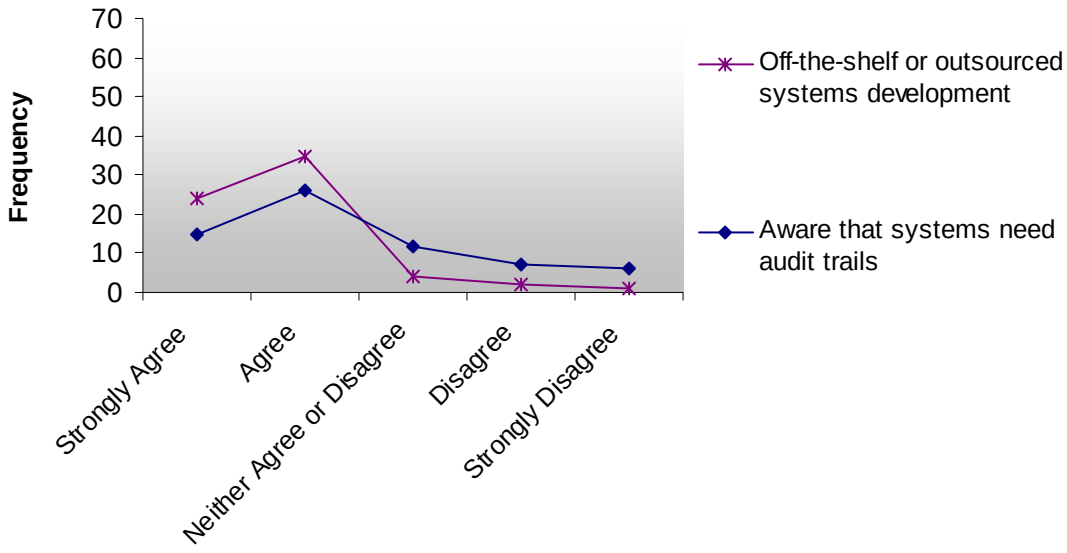


Figure 10.8 Access Control

With the exception of SME's that specifically provide IT solutions / systems development services, SME's generally do not have the resources and capacity to embark on systems development projects. Systems software tends to be bought in as

off-the-shelf products and or customised by consultants, to meet the needs of the SME. In this survey, 89% of respondents agree with this. Three of the sixty six respondents (6%) suggested they do in-house development. The demographics indicated six of the total population of sixty six SME's involved in the computer field. An encouraging 79% of SME's surveyed are aware of the need to provide audit trails with 20% disagreeing on this. 20% of SME's who say they are not aware of the need to provide audit trails, need to understand that without audit trails, it becomes very difficult if not impossible to monitor information security.

Question 42 asks whether respondents are aware of the need to provide audit trails and not whether they do provide audit trails. Audit trails can only be provided if there are unique user ID's and passwords. Failing this, audits are pointless because they cannot be traced back to an individual. Most commercial accounting systems, found in 88% of SME's surveyed, do make use of ID's and passwords and provide audit trails. It is the general computer systems found in SME's where there is a lack of Server Network Operating Systems, which results in a lack of centrally controlled User ID's and passwords.

Recommendations

As mentioned in the previous section, SME manager / owners must work towards a system of centralised user accounts so that access to any system or user resources, as well as other assets such as printers, can be controlled and audited.

10.2.9 Section I: Business Continuity Management

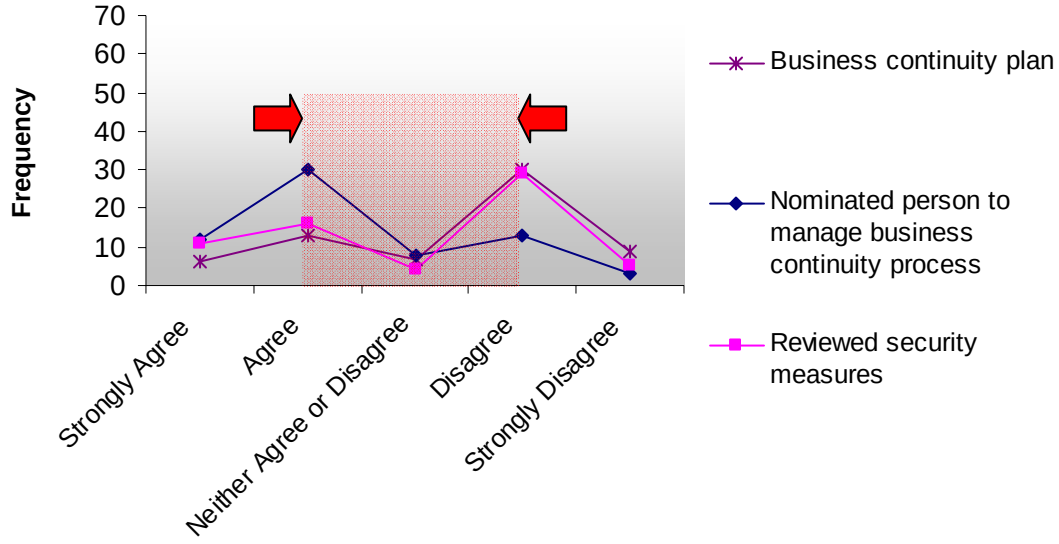


Figure 10.9 Business Continuity Management

The majority of SME's that participated in the survey, (59%), reported not having a business continuity plan. This is not surprising, given that over 50% of SME's interviewed do not have formal information security Policies. Although there is no formal business continuity plan, 42 respondents, (64%), say they have a nominated person who will manage the business continuity process. Again, over half the respondents say their security measures have not been reviewed within the last year although 41% would argue and say they have.

Recommendations

Business Continuity Management is a governance issue. Governance is currently receiving much attention. As SME's grow, they will increasingly need to demonstrate that Business Continuity Management is being addressed. It is not good enough to have someone nominated as responsible for managing the business continuity process. There must be a business continuity management plan, a living document that is revised annually. The complexity of this plan must be synchronised with the nature and size of the organisation and should be practical and realistic. Questions that should be addressed are:

- What happens when key personnel leave or are deceased?
- What about the potential loss of business data and systems?
- What about continuation of service or product support?
- What about business image / brand?
- What about the financial implications of a disaster?
- What about outsourcing risk, such as insurance?
- What about the legal implications of lost data

10.2.10 Section J: Compliance

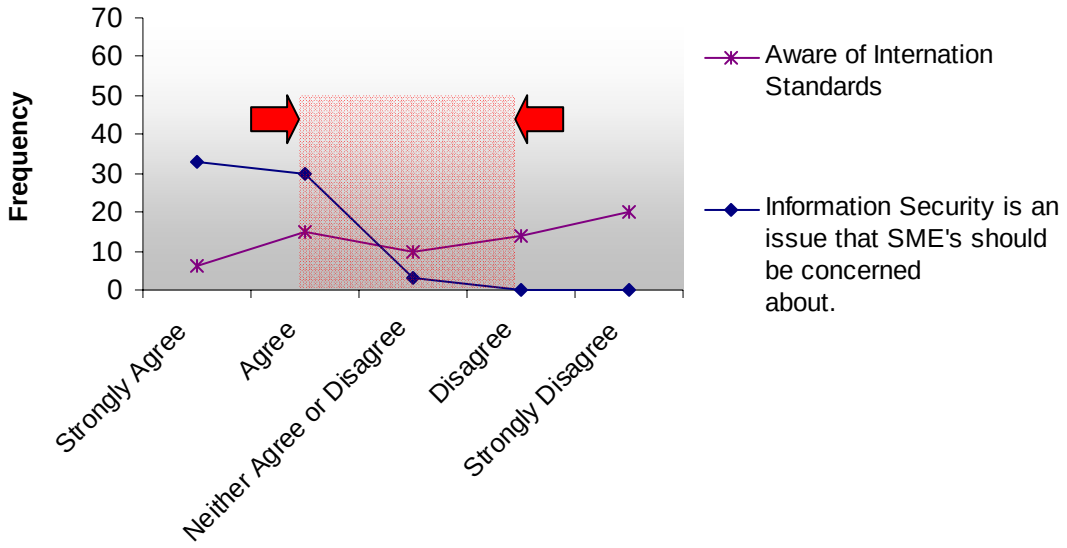


Figure 10.10 Compliance

52% of the respondents have not heard of International information security standards, which is alarming when other International standards such as ISO 9001 are widely known and embraced. Question 47 listed some of the more commonly known information security standards, asking respondents to indicate which standards they had heard of prior to the survey. This time, only 23% said they had not heard of standards. 21% of the respondents had heard of SABS ISO /IEC 17799. 8% had heard of SABS 17799-2. The only other standard, known by 5% of the respondents is RFC2196: Site Security handbook. When respondents were asked whether or not their organisations have suffered security breaches within the previous 12 – 18 months, 48% reported no breaches. Of those that suffered breaches, 35% were

equipment failure, and 33% were inadvertent breaches. Asset theft, (8%), backup failure, (6%), data theft, (3%) and copyright infringement (3%) were also presented as problems. Given that 48% of SME's reported not following any structured upgrade plan, this may explain the high percentage of SME's, (35%), that have suffered equipment failure. Anecdotal evidence would suggest a tendency by SME's to leave equipment and systems until they literally stop working. Part of the difficulty with this approach is old discontinued systems may no longer be supported. When break-downs occur, recovering 'legacy' systems or data within these systems, may be costly, if not impossible. Just as old worn plant and machinery must be maintained and ultimately written off and replaced in order to maintain a competitive production environment, information systems must be maintained and ultimately upgraded / replaced, in order to provide management with the tools to make competitive business decisions.

Considering that 57% of respondents said staff were given inadequate training, it was interesting to note that the second highest security breach suffered by SME's are inadvertent breaches (33%) that is a staff member accidentally deleting a file or table in data base or forgetting to backup data. The final question explores whether or not respondents think that information security is an issue that SME's should be concerned about? The overwhelming majority, (95%), say that information security is an issue that SME's should be concerned about, while 5% feel indifferent.

Recommendations

Information systems form an important part of SME's. It is important that those charged with the responsibility for information systems and Security:

- Keep abreast of the regulatory and legal implications for information systems and security
- Provide a maintenance / upgrade plan so that systems do not fall into disrepair
- Provide a staff training plan so that systems are used correctly and staff are aware of the risks surrounding the use and dissemination of information
- Keep abreast of information security literature, of which there is a proliferation
- Keep abreast of security standards and certification

10.3 Conclusion

In the services sector in the Eastern Cape, SME's abound. They provide a variety of services and embrace information systems and security at varying levels. Some SME's are well-resourced and boast up-to-date or even cutting edge information systems and technology, whilst some SME's survival is predicated on flexibility, adaptability and frugality with entrepreneurs crafting together information systems and technology on shoe string budgets. Both types of SME's were encountered during the survey. SME's are innovative, they seek out the obvious benefits derived from information systems and technology, extending these benefits to outside connectivity and convenience. Banking, tax returns and email are now common place in many SME's. Increasing use is made of online marketing and research and in some cases, even on-line business transacting. SME's do what is necessary to get the job done. Viruses threaten SME's and survey results suggest that these concerns have been taken seriously and solutions now appear to be in place to deal with this ongoing threat.

Of concern, are security issues, not as obvious as virus attacks, but so disruptive, they could have comparatively devastating consequence for SME's. Referring back to Figure 6.3, the majority of these concerns fall into: administrative and technical issues. SME's must take stock of their increasing dependence on information systems. Assumptions cannot be made regarding the integrity of data backups and recovery. These must be tested and correctly administered by a staff member who is trained and held accountable for data backups and recovery processes. If data backups and recovery are outsourced, a staff member must take on the responsibility of ensuring the service provider is competent and backups are current, secure, and recoverable. Staff, in general, must receive training and be held accountable for use of information systems. Service providers must be held accountable and contracted through Service Level Agreements. As information systems infrastructure and dependency grows, SME management must look at adopting current state of practice centralised user management operating systems. SME owners / managers must take a strategic view of information systems and Security by creating policies that guide their organisation through all of the above mentioned issues. Finally, SME owners / managers must understand that governance and business continuance are real

leadership issues. Ultimately the responsibility lies with the SME owner / manager to ensure that his / her business has in place the necessary processes to ensure that even through adversity, the business can continue operating.

Chapter 11: Conclusion

Abstract

The previous chapter analysed the results of the survey and provided recommendations that may benefit SME's in safeguarding their information systems. Chapter 11 concludes the research, lists contributions of the research and provides areas for future work.

11.1 Introduction

Small and medium enterprises provide employment for many millions of people throughout the world. While business environment and culture, as well as Government regulations and business ethics vary from country to country, common to most SME's are entrepreneurs who despite grappling with limited funding, limited access to expertise, and sometimes unfair restricted access to markets, manage to establish and build businesses. Information systems and technology, originally considered to provide businesses with decision support advantages, are now operational imperatives. The widespread adoption of Internet technologies is enabling SME's to connect to one another and to large business, both locally and globally. While on-line banking, Internet access and email are now commonplace in SME's, they are increasingly adopting Electronic Data Interchange (EDI), and Electronic Businesses (E-Business).

SME's are not currently addressing information security adequately. Although SME leadership are aware of the need for information security, in many cases, this awareness is superficial. Virus protection and data backups (untested) are common amongst many SME's, however security interventions in SME's are generally unplanned and ad-hoc. SME's must formalise information security by adopting a security standard. There are several security standards and frameworks available. Most of these standards are internationally developed, and are characterised as large, complex, all encompassing documents. The most widely adopted of these standards is BS 7799 or ISO/IEC 17799. The South African version of this standard is: SABS ISO/IEC 17799. Part of the difficulty for SME's wishing to implement a universal standard such as ISO/IEC 17799, is that the standard is complex and all embracing. SME's typically do not have the resources to embark on drawn-out implementations.

Following a survey of SME's whereby a scaled down, refined subset of SABS ISO/IEC controls were administered to select SME's in the services sector in the Eastern Cape, the thesis proposes that SME's seriously consider this approach to initialising the information security process.

11.2 General Contributions of the Research

- Information systems professionals are often enthusiastic and passionate about new technologies and software advances, whereas, entrepreneurs running SME's do not necessarily share this passion, are mystified by the intricacies of information systems, and prefer to view their systems as tools that can be used to run their businesses more efficiently.

- SME's are increasingly adopting information systems and technology. This includes ICT where many SME's are connecting to both public and private networks via permanent data lines and through service providers.

- SME management must understand that although an Information system may appear robust, it has to be maintained. Access to well trained in-house or outsourced technical expertise is important, as are trained disciplined personnel who use these systems.

- SME's do not appear to have processes in place to measure their service provider performance. Of concern, is that SME's do not appear to manage the outsource process. The research recommends the use of Service Level Agreements (SLA's) as a means to engage service providers contractually.

- SME's need access to impartial advice / governance on information security, so as to validate security initiatives and spend. This should include access to 3rd party experts who can test security initiatives via penetration testing and so on.

- While SME's view information assets as technology tools, they appear to overlook the knowledge contained by personnel in the organisation. The knowledge referred to, may be customer or supplier details or the knowledge

about operating a particular system. Human knowledge is one of the most valuable and volatile forms of assets found in an organisation. Goodwill is another asset, often overlooked. The more the organisation depends on technology to manage its knowledge and face its markets, the more vulnerable will be the organisations' goodwill to digital assault.

- Very small business may have modest application of information systems and are unlikely to engage in any formal risk analysis process. Management must, however, consider the implications of system and data loss due to malfunction or theft. They may choose to accept the risk or alternatively transfer the risk to a third party via insurance. Irrespective of the approach taken and the size of the business, SME management are ultimately responsible for ensuring their information assets are protected.

- There are a variety of information security standards available for adoption by enterprises. The majority of these are international standards and are well supported / documented. However, these standards are not particularly SME friendly as they tend to be complex and resource intensive to implement.

- While SME's may be convinced to formalise their information security processes by way of implementing security standards, many of these standards are prohibitively complex to roll-out and beyond the scope and expertise of SME personnel.

- As SME's grow and become increasingly dependent on information systems and technology, management must realise they have the added responsibility of managing the risk of potential loss of these systems. They have to engage in the process of protecting their information assets. This must start with deliberate policies that feed into operational processes. Although outsourcing may be an attractive option for SME's, the responsibility for information security planning must come from within the organisation.

- People are the least predictable "component" of an information system and personnel conduct directly impacts the well functioning of an information system. The ECT Act prescribes how information may be collected, stored, processed and then disposed of. Any business found in breach of the Act, may suffer severe consequences. Personnel must understand the implications for a business deemed guilty of non-compliance with the Act. Personnel training and awareness is very important irrespective of whether aspects of information systems management are outsourced or not. Policy documents should drive the process and must specify acceptable use of systems.

- Part of the leadership challenge is gaining staff buy-in. An enforced top down approach using performance appraisals and other auditing techniques is considered one option, the other, a bottom-up approach, achieved by creating an organisational culture where people feel personally willing and inclined to buy-into organisational values, which includes embracing security policies and practices. The latter of the two is considered more likely to succeed in SME's. Whatever the management style, personnel must be trained and act responsibly in using information systems.

- Several security blueprints / frameworks exist and are available for use by SME's. Associated with these blueprints / frameworks, are certification schemes that enable organisations to measure their security initiatives and gain certification, if they so wish. In general, SME's are not familiar with the various blueprints and certification standards. Certification schemes and auditing tools such as those available from the Information Security Institute of South Africa (ISIZA), are well designed, freely available, offering organisations a phased approach to implementing and assessing security. Despite this, respondents did not refer to ISIZA when asked to list security standards and frameworks they had heard of.

- While Governance may be viewed by SME's as a corporate issue, SME management should not forget that good governance provides a potential shareholder, financier, partner or potential employee, with some assurance that the

organisation is well managed. Good governance means policies and processes are addressed. Staff as well as contractors know where they stand and what is /not acceptable. Business continuity / disaster recovery plans are in place and considered working documents.

11.3 SABS ISO/IEC 17799 and Recommendations for SME's

BS7799 (SABS ISO/IEC 17799) is a comprehensive security standard, and boasts International / Universal acceptance. Most security frameworks explored in this research, make reference to BS7799. Numerous certification schemes based on BS7799 also exist.

SABS ISO/IEC 17799 provides a suitable framework for addressing SME information security concerns. The following section lists those security controls thought to be most pertinent for addressing information security in SME's.

- Security Policy

  The security process should start with high level planning that feeds into a security policy. Policy documents should be lightweight, living documents that include:

  - Acceptable use of information systems
  - System and data security
  - Data backup and recovery
  - Outsourcing / Service Level Agreements

  Staff must be made aware of these policies and they should be revisited periodically.

- Organisational Security

  Organisational security is about implementing security throughout the organisation:

  - A director / partner must take on information security as a portfolio.
  - All staff (permanent and contract) must be asked to sign Information confidentiality agreements.
  - Someone must be officially tasked with information security responsibilities irrespective of whether part of this function is outsourced

or not. If a part of information systems and security is outsourced, the relationship with the service provider must be managed and contractually formalised.

- Asset Classification and Control

  SME's must ensure that:

  - Software and licence agreements are stored safely.
  - Physical documents are stored and discarded of securely.
  - Sensitive documents are correctly stored.
  - Staff must be aware of the legal consequences of 'leaked' confidential information. As mentioned previously, SME's in the financial advisory / insurance sectors are governed by external bodies and these SME's were beyond reproach when it came to information classification, storage and disposal.

- Personnel Security
  - Staff must sign non-disclosure agreements. This should be non-negotiable.
  - Staff must be given basic awareness training so that they understand the consequences of an information security breach. Staff must think twice about opening email or attachments from an unknown source.
  - Staff must understand the risk in leaving computer terminals unlocked while not around, and the personal consequences for doing so as well.
  - Whoever has been tasked to look after backups must insist that staff comply and co-operate with the backup policy. This may mean that staff always save data onto the central server and not leave data on computer desktops.

- Physical and Environment Security
  - SME's must provide secure, conditioned storage for data processing and network equipment. A stable operating environment will mean that equipment remains reliable for longer.

- Conditioned / secure facilities will also mean that physical risk and tampering will be minimised.

- Communication and Operations Management

  SME's must ensure they have formal operational procedures such as:
  - A formal backup and recovery procedure as previously discussed.
  - An anti-virus policy with appropriate solutions in place.
  - A planned maintenance and upgrade policy.
  - Formal policies regarding email and Internet usage.

- Access Control

  SME's must implement a Network Server Operating System that addresses:
  - Centralised User accounts with managed password control.
  - Auditing facilities (usually part of Network Operating System).
  - Planned data structure so that documents are stored centrally and according to a predetermined directory structure. This will facilitate an efficient backup system.

- Systems Development and Maintenance

  SME's tend to outsource systems development and maintenance or purchase off-the-shelf products that are integrated into existing systems. SME's must:
  - Ensure that any contractors sign non-disclosure agreements.
  - Integrate new systems so that they provide for centralised user accounts and security.
  - Ensure that auditing is an option on all new systems.

- Business Continuity Management

A business continuity management plan must be produced and updated by an individual who is held responsible for business continuity management. Issues addressed in the plan must include:

- Loss of key personnel.
- Loss of business data and or systems.
- Business continuity, brand and image.

  - Financial implications of a disaster.
  - Outsourcing of risk such as insurance.
  - Legal implications of data loss / theft.
- Compliance
  - Keep abreast of regulatory and legal implications for information systems and security.
  - Ensure a maintenance plan is in place so that systems do not fall into disrepair, causing business disruption / data loss.
  - Again, staff MUST receive training, including information security awareness training.
  - Stay abreast of information security developments and certifications.

11.4 Future Work

The information security questionnaire was administered to SME leadership. All responses were from this leadership perspective. The researcher believes that administering the same survey to a section of SME personnel and comparing the results to those of the first questionnaire could prove to be an informative exercise.

The researcher found that talking to respondents in Grahamstown, prior to administering the questionnaire, was most revealing. The researcher believes that this anecdotal evidence assisted in the research. The researcher believes that conducting qualitative research, via a case study methodology, could result in very interesting and useful results and perspectives on information security.

A major challenge exists in heightening information security awareness amongst SME leaders. A methodology for achieving this should be sought.

11.4 In Closing

Numerous information security frameworks are available for business to adopt. However, the real concern should not be about which security standard to adopt or what auditing tool to use, but rather that SME management thoroughly engage in the information security process, adequately understanding and appreciating the need to address properly, information security, including the adoption of frameworks and high level planning, starting with information security policy documents.

List of References

Act No. 102 of 1996 — National Small Business Act, 1. *Act No. 102 of 1996: National Small Business Act, 1996*. Available [On-line]: http://www.polity.org.za/html/govdocs/legislation/1996/act96-102.html?rebookmark=1

Act No. 2 of 2000 — The Promotion of Access to Information Act 2 of 2000 (PROATIA) Available [On-line]: http://www.polity.org.za/html/govdocs/legislation/2000/act2.pdf

Act No. 25 of 2002 — *Electronic Communications and Transactions Act 2002* Available [On-line]: http://www.internet.org.za/ect_act.html

Barnard, L. & von Solms, R (2000) — "A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls", *Computers & Security*, vol. 19, no. 2, pp. 185-194.

Bennett, E (2004) — *Ernst &Young Global Information Security Survey 2004.* Available: [On-line]: http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf

Briney, A. & Prince, F (2002) — *Survey Overview "Does Size Matter?"* Information Security Magazine [September 2002]. 2002. Available [On-line]: http://infosecuritymag.techtarget.com/2002/sep/2002survey.pdf

Cowley, S (2002) — *Sept. 11 keeps disaster recovery in forefront*. Computerworld , 1-10. Available [On-line]: http://www.computerworld.com/databasetopics/data/story/0,10801,73956,00.html

Davies, C (2004) — *Governance and Small Business*. Available [On-line]: http://www.visa.ca/smallbusiness/article.cfm?cat=3&subcat=95&articleID=205

Dhillon, G. & Backhouse, J (2000) — *Technical Opinion: Information System Security Management in the New Millennium*. Communications of the ACM, ACM Portal 43[7], 125-128. Available [On-line]: http://portal.acm.org/results.cfm?coll=portal&dl=ACM&CFID=15093491&CFTOKEN=53643605

Eloff, M. & von Solms, S (2000) — *Information Security Management: A Hierarchial Framework for Various Approaches*. Computers & Security 19, 243-256. 2000.

Endorf, C (2004) — *Outsourcing Security, the Need, the Risks, the Providers and the Process*. Information Systems Security 12[6], 17-24. 2004. Available [On-line]: http://search.epnet.com/direct.asp?an=12244008&db=aph

Fujitsu (2001) — *Fujitsu Online Information Security Questionnaire*. 2001. Available [On-line]: http://uk.fujitsu.com/services/itconsulting/security/questionnaire/

Geiger, J. & Pendegraft, N (1999) — *Information Systems Security For Small Business.*

Geiger, J. & Wegman, J (2002)	*Small Business and E-Commerce: Strategic and Legal Concerns*. Available [On-line]: http://www.cbe.uidaho.edu/wegman/geiger-wegman%202002%20website.htm
Gordon, G (2003)	*Security and Risk Management: how to keep things under virtual lock and key*. Convergence 4[2], 60-67. 2003.
Hardy, G (2003)	*COBIT PowerPoint Presentation ITSMF, West Cape Meeting*, IT Service Management Forum Available [On-line]: http://www.itsmf.org.za/Presentations/Presentations2003/cobit%20%20itil.pps#451,1,CobiT & ITIL Gary Hardy
Information Security Healthcheck. (2004)	*Information Security Healthcheck.* Available [On-line]: http://www.ukonlineforbusiness.gov.uk/healthcheck/index.jsp
Information Security Self Assessment Instrument. (2004)	*Information Security Self Assessment Instrument.* Available [On-line]: http://www.isi-za.org/ http://jupiter.key.co.za/security2/default.asp
Information Systems Audit and Control Association. (2004)	*Information Systems Audit and Control Association*. 2004, *Standards, Guidelines and Procedures for IS Auditing*. 2004. Available [On-line]: http://www.isaca.org/template.cfm?section=Overview_and_History
Klopper, O (2002)	*How secure is your computer network* Available [On-line]: http://m1.mny.co.za/MBNews.nsf/0/C2256907002CDA624225692E005F3695?OpenDocument
Laudon, K. & Laudon, J (1995)	*Information Systems, A Problem-Solving Approach*, 3 edition, Elizabeth Widdicombe.
Leggat, H (2003)	*Damages Caused by Virus Infections - who is liable?* 2003. Available [On-line]: http://estrategy.co.za/article.asp?pklArticleid=2421&pklIssueID=326&pklCategoryID=131
Long, L (1994)	*Computers and Information Systems*, 4 edition, Prentice Hall.
Long, L. & Long, N (1996)	*Introduction to Computers and Information Systems*, 5 edn, Prentice Hall, Inc, New Jersey.
Michalson, L (2003)	*Information security and the law: threats and how to manage them*. Convergence Volume 4, Issue 3, pp. 34-38.
Michalson, L (2003)	*Under Virtual lock and key, Convergence*, vol. Volume 4, Issue 2, pp. 42-45.
Mostert, W (2003)	*Cry "Proatia" and Let Slip the Dogs of War?* 2003. Available [On-line]: http://www.deloitte.com/dtt/cda/doc/content/Without%20Prejudice%20July%2003.doc
NIST Special Publication SP 800-12 (2004)	*NIST Special Publication SP 800-12: An Introduction to Computer Security - The NIST Handbook.* Available [On-line]: http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter1.html

NIST Special Publication SP 800-14 (2004)	*NIST Special Publication SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems*. Available [On-line]: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
NIST Special Publication SP 800-18 (2004)	*NIST Special Publication SP 800-18: Guide for Developing Security Plans for Information Technology Systems*. Available [On-line]: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF
Panko, R (2004)	*Corporate Computer and Network Security*, International Edition, Prentice Hall, New Jersey.
Peltier, T (2001)	*Information Security Risk Analysis* Auerbach
Peltier, T (2002)	*Information Security Policies, Procedures, and Standards* Auerbach
Peltier, T (2003)	*Preparing for ISO 17799*. Information Systems Security Vol. 11, Issue 6, 21-28. Available [On-line]: http://search.epnet.com/direct.asp?an=8841317&db=aph
PricewaterhouseCoopers information security breaches survey (2004)	*PricewaterhouseCoopersDTI information security breaches survey 2004 technical report*. Available [On-line]: http://www.infosec.co.uk/files/DTI_Survey_Report.pdf
SABS ISO/IEC 17799: (2000)	South African National Standard (SABS IS0/IEC 17799) *Information technology - Code of practice for information security management*. [1].
SANS 17799-2: (2003)	South African National Standard Information security management systems *Part 2: Specification with guidance for use*
Schultheis, R. & Sumner, M (1995)	*Management Information Systems The Managers View*, 3 edition, Irwin,
Shaw, G (2002)	*Effective Security Risk Analysis*. Available [On-Line:] http://www.itsecurity.com/papers/insight2.htm
Silva, Z (2004)	*IT security critical for SME's*. ITWeb January 9, 2004. Available [On-Line:] http://www.itweb.co.za/sections/techforum/2004/0401090756.asp
Skoudis, E (2002)	*Infosec's Wost Nightmares*. Information Security Magazine [November 2002]. Available [On-Line:] http://infosecuritymag.techtarget.com/2002/nov/nightmares.shtml
Imation Small Business Survey. (2003)	*Special Report, Imation Small Business Survey*. Available [On-line]: http://www.imation.com/assets/NorthAmerica_Assets/AboutImation/PDF/IMN_SMB_SpecialReport.pdf
Swindle, O and Conner, B (2004)	*The Link Between Information Security and Corporate Governance* Computerworld , 2004. Available [On-line]: http://www.computerworld.com/securitytopics/security/story/0,10801,92915,00.html
Szymanski, R., Szymanski, D., & Pulschen, D (1995)	*Computers and Information Systems*. Prentice Hall Inc, 1995

Tiller, J (2003)	Tiller, J. *The Business of Security*. Information Systems Security 12[5], 2-5. 2003. Available [On-line]: http://search.epnet.com/direct.asp?an=11125482&db=aph
Unknown, (2001)	*What is BS7799 / ISO 17799*? Callio Technologies. Available [On-line]: http://www.callio.net/bs7799/id,6
Volonino, L. & Robinson, S (2004)	*Principles and Practice of Information Security*, 1 edition, Anderson, Natalie E, New Jersey.
von Solms, B (2001)	*Corporate Governance and Information Security*, Computers & Security.
von Solms, B. & von Solms, R (2001)	*Incremental Information Security Certification, Computers & Security*, vol. 20, no. 4, pp. 308-310.
Vroom, C. & von Solms, R (2004)	*Towards information security behavioural compliance*. Computers & Security 23, 191-198. 2004.
Whitman, M. & Mattord, H (2003)	*Principles of Information Security*, 1 edition, Thomson Learning, Course Technology, Boston, Massachusetts.
Whitman, M. & Mattord, H (2004)	*Management of Information Security*, 1 edition, Thompson Learning, Course Technology, Boston, Massachusetts.
Wylder, J (2003)	*Improving Security from the Ground Up*. Information Systems Security Volume 11[6], 29-35. 2003. Available [On-line]: http://search.epnet.com/direct.asp?an=8841319&db=aph

Appendix A

Paper Based Survey, Questions 1-7

MBA THESIS QUESTIONNAIRE - September 2004

Business Overview:

To establish the nature of service engaged in and that the business subscribes to the definition of small business as laid out in ACT 102 of 1996

1 What is the nature of your service business? (Cross (X) one only)

Consulting	1		Estate Agent	7	
Recruitment	2		Medical	8	
Vehicle Services	3		Equipment Leasing/Rental	9	
Cleaning	4		Computers	10	
Legal	5		Equipment Repairs	11	
Accounting	6		Other Professional Service	12	

2 How long has the business been in operation? _____ (years)

3 What are your current number of employees?

0 - 5	
6 - 10	
11 - 25	
26 - 35	
36 - 50	
51 upwards	

4 What is your average annual turnover in R '000?

0 - 150	
151 - 1000	
1001 - 1500	
1501 - 2000	
2001- 10000	
10001 upwards	

To establish the nature of your IT infrastructure

5 How many computers do you use in your business _____

6 How long have you been using computers in your business _____ (years)

7 What kind of hardware do you use ? (Cross (X) as many as is applicable)

Computers	1		Computer Networks	5	
Fax Machines	2		None of the above	6	
Printers	3		Other (please specify below)	7	
Modems	4				

Paper Based Survey, Questions 8-11

8 What kind of application software do you use ? (Cross (X) as many as are applicable)

Word Processing	1		Spreadsheets	6	
Database	2		Communications	7	
CAD/CAM	3		Integrated Packages	8	
Accounts	4		None of the above	9	
Desktop publishing	5		Other (please specify below)	10	

9 Please indicate which of the following you make use of:(Cross (X) as many as are applicable)

Internet	1		Electronic Commerce	4	
Email	2		EDI	5	
Intranets	3		None of the above	6	

10 The Internet is used for the following business issues: (Cross (X) as many as are applicable)

Gathering Information on customers	1	
Gathering information on competitors	2	
Establishing a business presence (e.g. website)	3	
Routine communications with customers	4	
Routine communications with suppliers	5	
Providing service/support to customers	6	
Selling services to customers	7	
Other (please specify below)	8	

11 Please indicate what type of access you have to the Internet:

Full time connection, (ADSL, DIGINET, LEASED LINE)	1	
Dial-up connection, (Modem, ISDN)	2	

(Please continue overleaf)

Paper Based Survey, Questions 12-22

	Please evaluate the following statements by placing an (X) in the appropriate column	Strongly Agree	Agree	Undecided	Disagree	Strongly Disagree
Section A: Security Policy						
12	Roles and Responsibilities for Information Security in our organisation are well defined, e.g. someone is responsibe for backups, registering users on the system, planning against a site disaster, liasing with Service Providers	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
13	We have a documented Information Security Policy.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
14	Staff are aware of our Information Security Policy.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
15	All staff are given adequate and appropriate Information Security Education and Training.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
16	Staff are well informed as to what is considered to be acceptable and unnaceptable usage of our Information Systems e.g Email and Internet conduct.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
Section B: Organisational Security						
17	A Director (or equivalent) member of our staff has responsibility for information security.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
18	Expertise on information security is available internally, and where not, external advice is sought.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
19	Third party (outsider) access to our information systems requires approval by a senior manager.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
Section C: Asset Classification and Control						
20	We can identify and locate all Assets (including software, hardware, staff and services) used for information handling.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
21	We control Local and Remote Access to our information assets adequately.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
22	Our staff know what to do with information with regard to its storage, usage archiving, backup and destruction.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯

Paper Based Survey, Questions 23-33

Section D: Personnel Security						
23	Staff are aware that security incidents must be reported to management immediately.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
24	Staff have been trained to secure their computers at all times, when moving away from their work stations. e.g. locking or logging off their computers when going for a tea break or out to lunch.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
25	There is a formal disciplinary process for employees who have violated our security policies and processes.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
Section E: Physical and Environmental Security						
26	Our organisation contains high value, portable goods or stock items on the premises.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
27	We have appropriate Physical and Environmental secruity procedures in place to prevent interference with business premises and information systems.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
28	Staff who travel with portable computers, are aware of the risk relating to theft and the potential liability through compromised data.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
29	Visitors to our organisation are always escorted around the building and are never left to wander around on their own.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
30	Our servers are maintained in airconditioned, fire-retardant, power conditioned secure facilities.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
Section F: Communications and Operations Management						
31	We are confident, that in the event of equipment failure, theft or a site disaster, our data backups and storage would enable us to retrieve our information with minimal business interruption.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
32	Our systems are updated / upgraded according to a structured plan and not in an ad-hoc fashion.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
33	In the event of a security incident, procedures clearly define what to do and who to call for assistance.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯

Paper Based Survey, Questions 34-45

34	We are confident that our anti-virus systems are up to date, and in the event of a virus outbreak, we should be able to protect our systems as best as possible.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
35	Desite being connected to public networks, we are confident that our systems are adequately protected by our Internet Service Provider's (ISP's) security and / or our own Firewalling systems.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
36	Appropriate mechanisms are in place to authenticate users logging onto our systems.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
Section G: Access Control						
37	Users may not logon / gain access to our systems without being formerly registered with their own user account.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
38	A password management system is in place which specifies the frequency of password changes as well as the minimum password complexity e.g. password must be changed every two weeks and be at least X characters long	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
39	Our organisation controls access to information via an access control policy which specifies which users have access to what data.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
40	We ensure that information processing facilities are only used for authorised business purposes.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
Section H: Systems Develoment and Maintenance						
41	Our systems tend to be bought in, either as off-the-shelf software products or customised systems, outsourced from developers.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
42	We are aware that systems need to provide audit trails so that usage of the system and data input / changes can be audited.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
Section I: Business Continuity Management						
43	We have a business continuity plan which specifies who must take what action and what has to be done to ensure that the organisation can continue functioning in the event of a disaster such as a fire / flood.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
44	There is a nominated person in our organisation who is responsible for managing the business continuity process.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯
45	Our Security measures have been reviewed within the last year.	1 ◯	2 ◯	3 ◯	4 ◯	5 ◯

Paper Based Survey, Questions 46-49

Section J: Compliance

46 Prior to this survey, I was aware that there are established, international information security standards, available for organisations to adopt.

1	2	3	4	5
○	○	○	○	○

47 I have heard of the following Information Security Standards: (Cross (X) as many as is applicable)

Not aware of any standards	1	
SABS ISO /IEC 17799 (Part 1)	2	
SABS 7799 (Part 2)	3	
NIST SP 800 Series	4	
RFC 2196: Site Security Handbook	5	
Other (please specify below)	6	

48 Our organisation has suffered the following security breeches in the last 12 - 18 months:

No information security breeches	1	
Inadvertent breech, (e.g. user accidentally deleted files or changed computer configuration)	2	
Deliberate attack (e.g. hacker / disgruntled staff gained access, deleting or stealing data)	3	
Asset theft (e.g. software application misplaced causing re-installation delay / costs)	4	
Equipment failure (e.g. hard drive crashed causing lost data and business disruption)	5	
Backup failure (e.g. system restore failure due to corrupt / inadequate backups)	6	
Data theft (e.g. espionage which resulted in data loss and possible legal exposure)	7	
Site disaster (e.g. fire or flood causing damage to systems and business disruption)	8	
Copyright infringement (e.g. staff loading pirated software, legally exposing the organisation)	9	
Compliance (e.g. passing on confidential information, legally exposing the organisation)	10	
Other (Please specify below)	11	

49 Information Security is an issue that SME's should be concerned about.

1	2	3	4	5
○	○	○	○	○

Thank you for completing this survey. If you would like a copy of the research findings, please enter your email and postal details below:

Name: _____
Email Address: _____
Postal Address: _____
_____
_____
_____

Appendix B

Web Survey Introduction / Front Matter

Rhodes University

Department of Information Systems

RHODES UNIVERSITY

Grahamstown • 6140 • South Africa

Dear Respondent,

The following questionnaire is part of an MBA research dissertation on Information security in small businesses, in the services sector in the Eastern Cape. It would be appreciated if the owner-manager of the business would complete and answer the questions as thoroughly as possible.

All information will be treated as **Strictly Confidential** and will only be used for academic purposes. If you have any queries concerning the questionnaire, please contact the researcher whose contact details are set out below.

If you would like a copy of the research findings, please full out your details at the end of questionnaire.

Your participation is much appreciated.

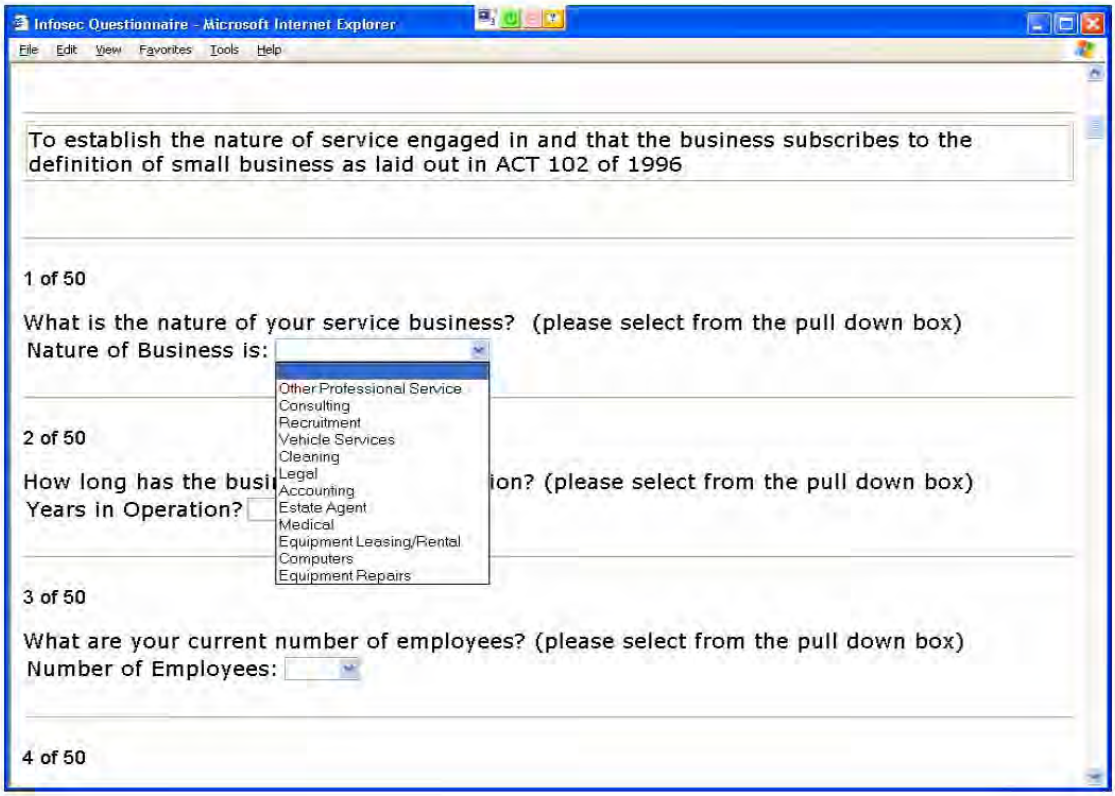
Researcher: Chris Upfold
Tel: (046) 603 8244
Fax (046-636 1915)
Email: C.Upfold@ru.ac.za

Instructions for completion:

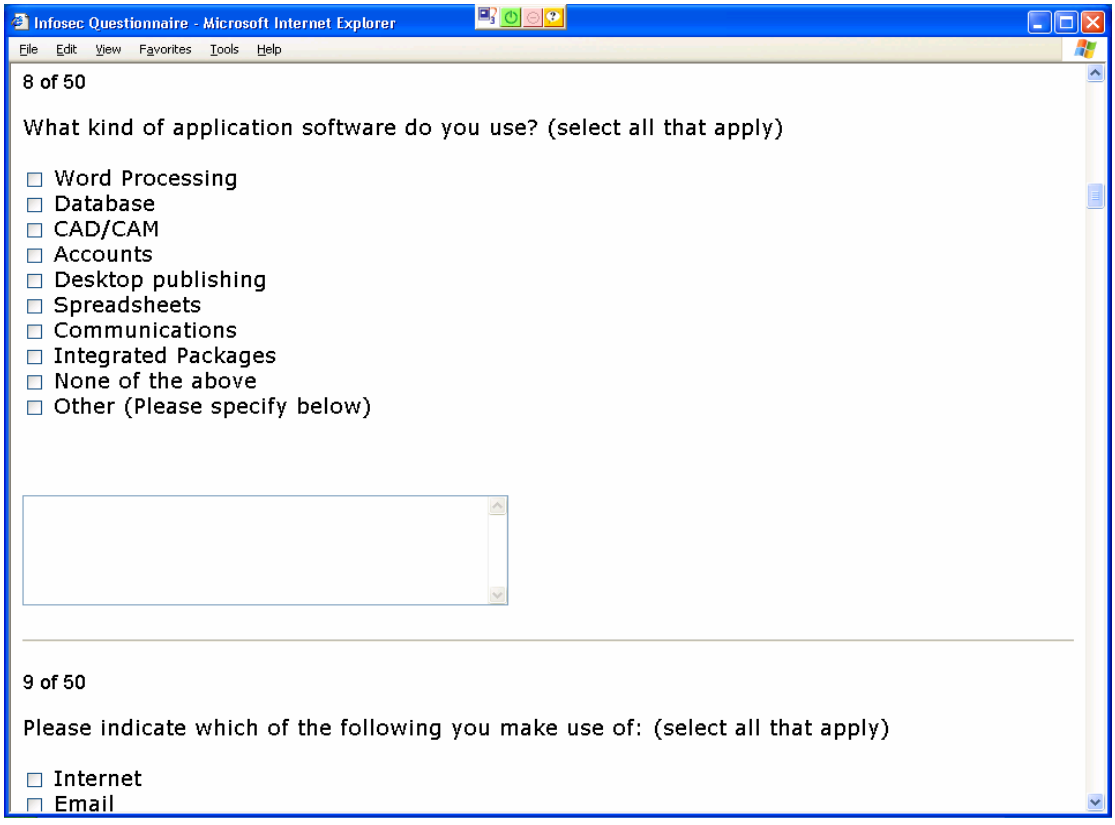
1. Please answer the questions as objectively and honestly as possible according to the instructions contained in the body of the questionnaire.
2. Please answer all the questions to allow an accurate analysis and interpretation of the data.
3. Once you have completed the questionnaire, please simply click on the button labelled SUBMIT at the end of the questionnaire.

Appendix C

Select Questions, Web based Survey

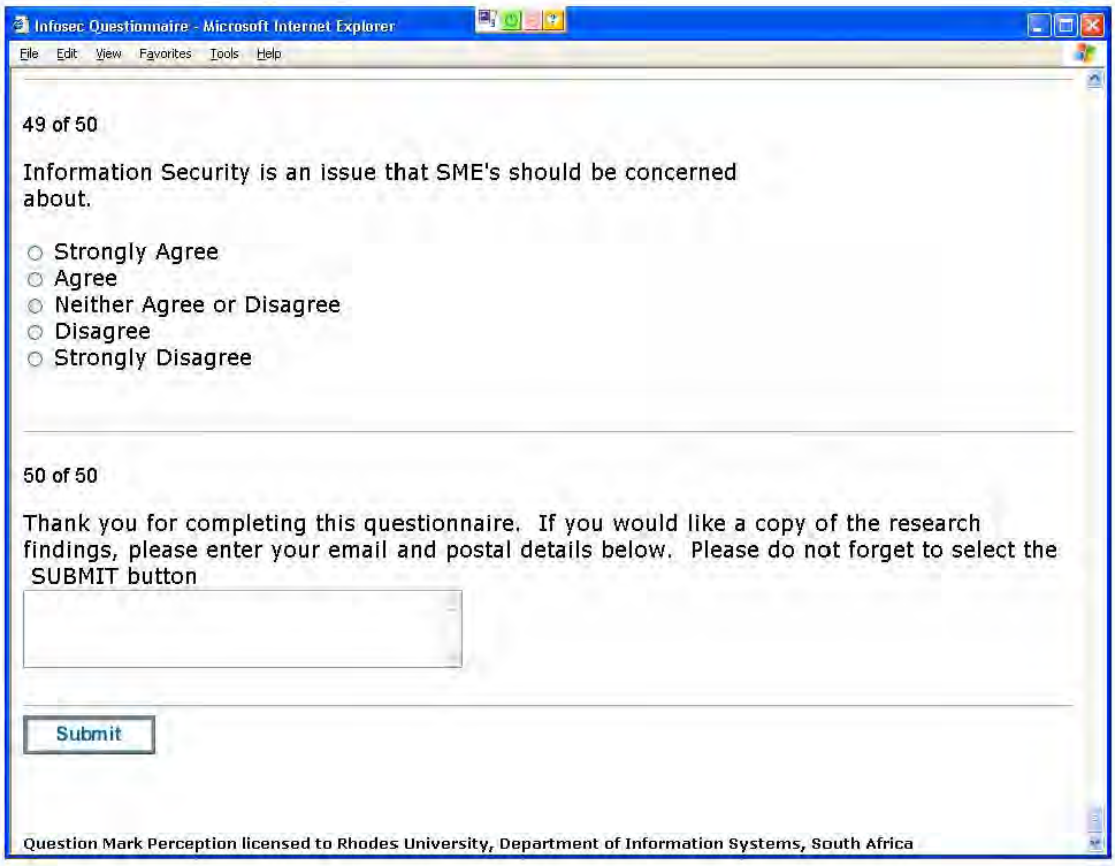


Select Questions, Web based Survey




Infosec Questionnaire - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Internet Connectivity
Please evaluate the following statements:
Section A: Security Policy
12 of 50
Roles and Responsibilities for Information Security in our organisation are well defined i.e. someone is responsible for backups, registering users on the system, planning against a site disaster, liasing with Service providers.
Strongly Agree
Agree
Neither Agree or Disagree
Disagree
Strongly Disagree
13 of 50
We have a documented Information Security Policy.
Strongly Agree
Agree

Final Question Page, Web Questionnaire



Appendix D

Survey initialisation email