AN INVESTIGATION OF INFORMATION SECURITY IN SMALL AND MEDIUM ENTERPRISES (SME'S) IN THE EASTERN CAPE

C.T. Upfold and D.A. Sewry

Author's affiliation

C.T. Upfold: Department of Information Systems, Rhodes University

D.A. Sewry: Department of Information Systems, Rhodes University

C.T. Upfold

c.upfold@ru.ac.za

P.O. Box 94

Grahamstown

6140

046 603 8244

D.A. Sewry

d.sewry@ru.ac.za

P.O Box 94

Grahamstown

6140

046 603 8244

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, several "stripped-down" standards and guidelines are available 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.

1 INTRODUCTION

Much like any other business asset, information is an asset that needs to be strategically managed and protected. 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. Numerous internationally approved security frameworks and schemes may be implemented to safeguard an organisation against information loss and potential liability. As a result of these frameworks being complex, all embracing, and ultimately costly to implement, they are mostly adopted by large organisations.

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.

2 LITERATURE REVIEW

2.1 Information Systems in Small and Medium Enterprises (SME's)

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. Software, such as operating systems and custom applications, are installed on computers, but often not 'patched' or upgraded. This results in software errors or vulnerabilities which may lead to security threats. Although information systems may be robust, they cannot run continually without some form of maintenance. Access to good in-house or outsourced technical expertise is important. Whereas large organisations may have the capacity to hire-in expert IT staff, SME's usually do not, and often resort to outsourcing. (Geiger and Wegman, 2002). Outsourcing can present problems, however, and Ploskina (2001) in Geiger and Wegman (2002) warn that instability in service providers and a lack of service level agreements may render an SME vulnerable.

2.2 Outsourcing and Risk

Successfully managing systems implies that security risks are understood and the appropriate interventions introduced. Volonino and Robinson (2004: 63) suggest performing a risk analysis. Risk analysis is not a deliberate SME strategy and although SME management may consider the consequences of data loss, the risk assessment process is unlikely to occur. Security risks are classified as inadvertent or deliberate. Although deliberate attacks are often launched from outside an organisation, they may also be facilitated or conducted from within the organisation. Staff involvement and or negligence should never be ruled out. According to Klopper (2002), the four (4) worst mistakes committed by computer users are:

- 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.

Of increasing importance, is the liability organisations now face should private or sensitive information be compromised. Staff training is thought to be critical in this regard.

2.3 Regulatory Environment and Governance

Client confidential data that is stolen / leaked from a small organisation has the same legal implications for large organisations. According to Michalson (2003: 42), two Act's 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

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 management have to answer to shareholders and boards of directors. As SME's are established and seek to grow, however, it is essential, that management adopt good governance practices, as this is likely to provide vital assurance to potential funders, investors and partners. Good governance also means that policies are addressed, and these directly impact information security.

2.4 Personnel and Information Security

People constitute the least predictable and yet most critical component of any Information System. A badly negotiated and or 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 remains getting staff to support and participate in the implementation of security systems, policies and practices. Vroom and von Solms' (2003:29) suggest establishing a culture of employee co-operation and buy-in through the alignment of organisational and individual values and behaviour. It is imperative that SME management appraise and train staff so that they remain informed as to the impact their actions may have on their organisations security.

2.5 Standards, Frameworks and Models

Information security frameworks provide the basic structure on which an organisation can 'hang' its security initiatives. Many of the frameworks can be 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.

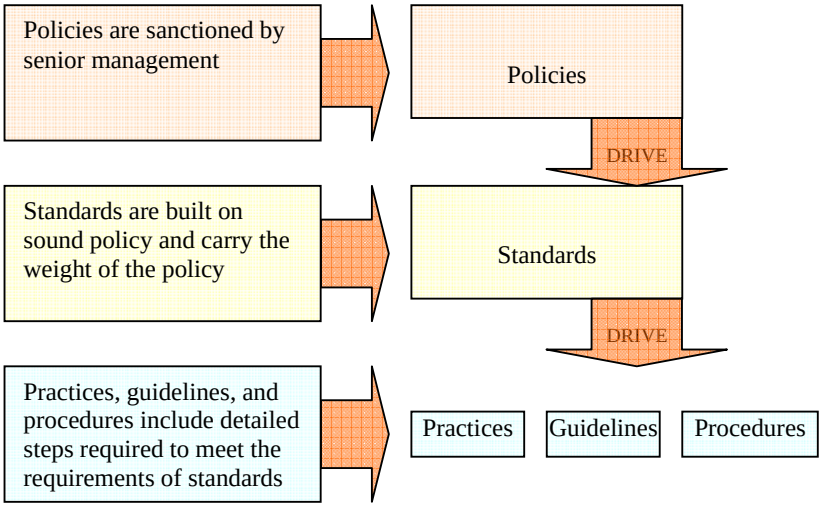

Figure 1. Policies, Standards, and Practices (Whitman and Mattord, 2003)

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, RFC2196, on Internet architecture and

Security is a framework for addressing computer security policies and procedures on the Internet. (Fraser 1997). While ISO/IEC 17799 together with BS7799-2:2002 constitute security standards, COBIT, (unknown, A. 1998), 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 those controls considered necessary and inadequately addressed 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, (unknown, B. 2005), 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 its 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 compliance is considered difficult for large, let alone SME's that may consider the process daunting and unachievable. The incremental model proposed by ISIZA, (von Solms and von Solms 2001: 308) 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.

3 RESEARCH OBJECTIVES

SME's are particularly vulnerable to security issues and concerns. A number of information security surveys, such as those mentioned below, 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 twenty nine (29) 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.

4 RESEARCH METHODOLOGY

4.1 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. These are:

- 2003 Special Report, Imation Small Business Survey (Imation Small Business Survey 2003).
- 2004 Ernst & Young Global Information Security Survey (Bennett 2004).
- 2001 Fujitsu Online information security Questionnaire (Fujitsu, 2001).
- 2004 PricewaterhouseCoopers information security breaches survey, technical report (PricewaterhouseCoopers information security breaches survey 2004).
- 2004 Department of Trade and Industry (DTI) Information Security Health check (DTI Healthcheck 2004).

Although some of these questionnaires are aimed at large enterprises, all of them contributed in some way towards the final research questionnaire.

4.2 Design of 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 feel inclined to complete the survey and not lose interest
- The questionnaire should be distributable to a large number of people

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. At the end of the survey, respondents are given the opportunity to enter contact details and to request feedback on research findings. (A copy of the questionnaire can be found in Appendix A.)

4.3 Administration of Questionnaire

The researcher administered the questionnaire over 3 months in Port Elizabeth, Grahamstown and East London. A dual approach was adopted whereby East London and Port Elizabeth respondents could complete the survey online. Once respondents had confirmed their willingness to participate, email was sent to them, explaining the purpose of the survey. A link was embedded in the email and when respondents picked on the link, they were automatically forwarded to a web server with the online questionnaire. Paper surveys were administered to Grahamstown respondents.

4.4 Population Sample

4.4.1 Grahamstown

Due to the small nature of Grahamstown and the proliferation of SME's, assembling the list was relatively easy. 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.

4.4.2 Port Elizabeth and East London

A large banking institution in the Eastern Cape 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 provided a list of clients, together with their company names, contact details and email addresses. All people on the list had been approached by their respective bank 'relationship managers' and had agreed up-front to participate in the process. 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, only 39 attempts were logged on the server. Despite 39 respondents logging on and commencing the

survey, only 34 respondents were recorded by the system as having completed the survey. These 34 completed on-line surveys were used for this research. The bank's assistance in pre-qualifying potential respondents was invaluable.

5 FINDINGS AND RECOMMENDATIONS

The overall impression gained throughout this research is:

- 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 to be irrelevant / unimportant to SME owners / managers may in fact, be critical given certain circumstances

Research findings considered to be most significant together with recommendations are discussed in the following section:

5.1 Security Policy

The security process starts with a general security policy which is designed to protect the overall assets of the organisation. The general policy serves as a basis for issue-specific policies. An overwhelming number of SME's have neither general nor issue-specific policies in place. (82%). Most respondents were dismissive of the need for policies, such as backup procedures or staff acceptable use guidelines. 57% of respondents do not provide any form of Information security education and training to staff. Critical functions such as data backups are erratic, untested and not stored correctly, on or off site. Despite this, it is alarming that many respondents are confident they have adequate Information security processes in place.

There is a strong indication that SME management view Information security policies as hard work, and expensive, requiring outside expertise and resulting in voluminous documentation.

Recommendation:

SME's should consider lightweight, living policy documents, 2-3 pages in length, that address specific issues such as backups, acceptable use of systems, and system and data security. 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. 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. The Joint Information Systems Committee is an example of this. (unknown, C. 2005)

5.2 Asset Classification and Control

An alarming 38% of respondents suggest staff are not aware of procedures for storage, usage, archiving, backup and destruction of data.

Recommendation:

While this is not surprising given the previous discussion on security policies, staff must be made aware of the legal / regulatory ramifications of information abuse / inadvertent or deliberate disclosure, as specified in the ECT Act 2002.

5.3 Personnel Security

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

unacceptable that 37% of respondents do not secure / 'lock' computer desktops when moving away from their computers. 55% of SME's denied having any form of prescribed disciplinary action for staff who ignore security processes.

Recommendation:

SME's must ensure that staff are properly trained and stay vigilant in respect of information security. Staff 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.

5.4 Communications and Operations Management

SME's are believed to be vulnerable when it comes to data recovery, knowing what to do and who to call in the event of a security incident. 47% of respondents reported not having any procedures that could be used to direct a recovery process while only 65% of respondents believe they have appropriate mechanisms in place to authenticate users logging onto their systems. Of major concern is the ad-hoc nature in which Information systems are upgraded and patched.

Software vendors frequently provide security upgrade patches. Due to insufficient system maintenance, however, these patches are not applied to systems rendering them vulnerable to security exploits. While outsourcing services may be beneficial to SME's that do not have in-house expertise, it may also leave them exposed, especially if their service provider lapses in quality of service (QOS).

Recommendation:

SME's must not assume their up-stream Service Providers are infallible when it comes to preventing viruses / hacking attempts. SME's must continually question security, and strongly consider the use of a firewall between themselves and any service provider / public network. Data backups, already discussed in 5.1, cannot be compromised. When all else fails, they present the business with a last ditch opportunity to recover critical data. Just as SME's now 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, some specifically for SME's, with the use of templates to allow for ease of administration.

5.5 Access Control

Only 52% of respondents confirmed the use of custom user accounts and passwords in their organisations. Considering that user accounts and passwords are the only way of enforcing controlled access to resources, this is alarming. 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, managers must restrict system 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.

Recommendation:

SME's must implement 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, system and data access 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.

5.6 Business Continuity Management

The majority of SME's participating in the survey, (59%), reported not having a business continuity plan. This is hardly surprising, given that over 50% of SME's interviewed do not have formal information security policies. Although no formal business continuity plan exists, 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.

Recommendation:

Business Continuity Management is a governance issue. 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 need to be addressed must include:

- 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?

6 CONCLUSION

Information systems and technology, originally considered to provide businesses, both small and large, 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. Several security standards and frameworks are available that 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.

7 ACKNOWLEDGEMENT

The authors would like to thank all participants in this study for the time given to interviews and discussions. Special thanks are conveyed to Prof R. von Solms who provided valuable feedback to the original thesis on which this paper is based.

8 REFERENCES

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
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
DTI healthcheck (2004)	The Department of Trade and Industry Healthcheck. Available [On-line]: http://www.dti-bestpractice-tools.org/healthcheck/
Fraser, B (1997)	The Site Security Handbook, RFC2196. Available [On-line]: http://www.rfc-archive.org/getrfc.php?rfc=2196
Fujitsu (2001)	*Fujitsu Online Information Security Questionnaire*. 2001. Available [On-line]: http://uk.fujitsu.com/services/itconsulting/security/questionnaire/
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_Special Report.pdf
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
Michalson, L (2003)	*Information security and the law: threats and how to manage them*. Convergence Volume 4, Issue 3, pp. 34-38.
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
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*
Unknown, A (1998)	COBIT and Related Products, Guidance Materials for IT Governance. Available [On-line]: http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT.pdf

Unknown, B (2005)	Pentana Checker for Information Security (PCIS). Available [On-line]: http://www.pentana.com/index.asp?menu=informationsecurity&pageid=23
Unknown, C (2005)	The Joint Information Systems Committee (JISC). Available [On-line]: http://www.jisc.ac.uk/index.cfm?name=pub_smbp_infosec
Volonino, L. & Robinson, S (2004)	*Principles and Practice of Information Security*, 1 edition, Anderson, Natalie E, New Jersey.
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.

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: _____
_____
_____
_____