Addressing E-crime & Computer Security Issues in Homes & Small Organizations in South Africa

Dr. Michael Kyobe
University of the Free State, South Africa.

kyobeme@hotmail.com, +27 587185216

Abstract

While small organizations are encouraged to adopt e-commerce, the impact of e-crime and the growing negative attitude of these organisations towards good security practices have been ignored. This study investigated e-crime and computer security issues facing small organizations and home Internet users in South Africa. The purpose was to report on the current state of these issues as well as help raise the level of security awareness. The data was collected via a questionnaire developed using the NSTISSC security model.

Our findings show a strong association between lack of a security policy and occurrence of virus attacks. Many small organisations are more vulnerable than they realize. They operate vulnerable operating systems, rely on basic security mechanisms and possess little knowledge of cyber risks and security standards. Several recommendations oriented at inducing these organisations to adopt good security practices are provided in form of a security guideline.

Keywords:

Small organizations; Home Internet users; E-crime; Security awareness; Small business security guide.

Addressing E-crime & Computer Security Issues in Homes & Small Organizations in South Africa

1 INTRODUCTION

As small organizations adopt e-commerce to reach new markets, expand products and services and strengthen business relations, their systems increasingly become a point for vulnerability to their own business affairs and those of business partners. Despite the large number of attacks on these organizations, many are still complacent about these threats and shun good security practices (Zorz, 2003).

Very little has been done to assist these organizations. There are few scientific papers addressing the security aspects of small organizations (Masurel, 2004; SAITIS (2000) and most victim surveys on e-crime tend to capture only the experiences of knowledgeable large organizations such as banks and governmental institutions (Lombard, 2003). This has made small organizations believe that e-crime issues are not relevant to them and as such ignored the need for in-depth security.

This study investigates e-crime and computer security issues in homes and small sized organizations in South Africa. The purpose is to report on the current state of both computer crime and computer security and help raise the level of security awareness in these organizations. First, an overview of computer attacks is presented. Second, a model used in the investigation is introduced. Third, the results of this survey are examined and finally, a security guide oriented at inducing these organisations to adopt good security practices is presented.

2 AN OVERVIEW OF COMPUTER ATTACKS

2.1 Definition and short history

A computer attack or crime may be defined as unauthorized access or attempt to gain control over a computer or network system. Attacks on computers date back to early 1960s. The 1970s and early 1980s saw a number of seminal developments in US which laid the conceptual and practical foundation for future tools for computer crime. A series of laboratory experiments lead to the discovery of many tools, trapdoors, Trojans and viruses and subsequent attacks on private and government networks between 1980s and 1990s.

Today the world experiences large scale ever evolving attacks, which are blended and malicious in nature. These are committed by ego-driven *Script Kiddies*; disgruntled employees and hackers seeking challenge, status, financial or political gain. There are vast resources on software vulnerabilities, attack tools and tutorials distributed freely on the Internet and *social engineering* has become prevalent. With attacks becoming more aggressive, faster and multi-pronged, consistent assessment of security programs is necessary.

3 INFORMATION SYSTEMS (IS) SECURITY ASSESSMENT

While there are a number security assessment models, most are designed for the large business environment and only a few integrate the current aspects of security. For instance models based on ISO 17799 (www.IS17799.net) and COBIT (www.isaca.org)

are enterprise focused and need to be scaled down to capture security issues in small firms. Others like OCTAVE-s (www.cert.org/octave) have been adapted to small organizations but they are mainly asset-focused. Computational models are overly complex requiring enormous amount of historical data which is unavailable in small organisations.

In addition, while information confidentiality, integrity and availability have been emphasized in most models, the evolving nature of threats and technology makes use of these three concepts alone inadequate. More robust models integrating most of the current security aspects are needed to guide the appraisal of security programs. In this study we adopted the NSTISSC security model developed by the National Security Telecommunications and Information Systems Security Committee (McConnell, 1994). It illustrates various critical aspects of information systems security and their interdependencies. Its application is universal and is not constrained by organizational differences or technological changes. It can be used to identify vulnerabilities and security weaknesses and also in the development of comprehensive security policies, education and training.

This model comprises three dimensions (see Figure 1). Dimension Y reflects three critical aspects of information security: Confidentiality, Integrity and Availability (CIA). Confidentiality is the assurance that only authorized users have access to information. Integrity is the quality or state of being whole, complete or uncorrupted. Availability is the characteristic of information that enables users to access information without interference or obstruction. A key aspect of security is to preserve these three attributes. A loss of one affects the other two which leads to system threats and vulnerabilities.

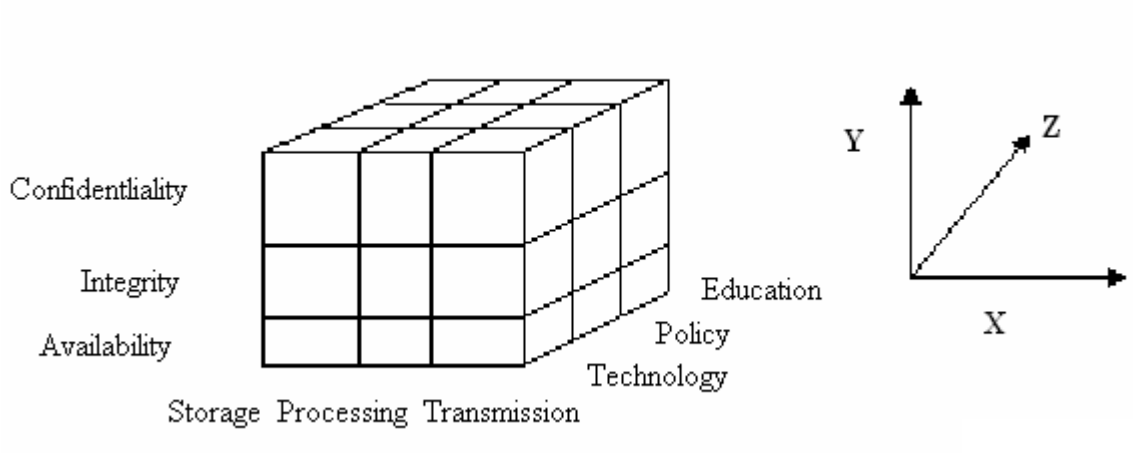

Figure 1: NSTISSC security model

Dimension X makes a distinction of the three states of information: storage, processing and transmission. This distinction is fundamental since it emphasizes the need to ensure security in all the states of information. In addition, it also indicates that as information changes states, specific security controls may be required.

Dimension Z reflects three security measures (Technology, Policy and Education), which must be implemented to maintain the critical characteristics of information (CIA). Technology plays a critical role in ensuring CIA and protecting information in all its states. However, use of technology must be guided by security policies. Furthermore, in order to ensure better

understanding of security principles and proper application and use of technology based on policies, it is essential to educate, train and create security awareness.

Once the information states within the system are identified, the evaluator then works down the vertical path of CIA analyzing threats and vulnerabilities. For each of the vulnerabilities discovered, the effectiveness of security measures is examined.

4 METHODOLOGY

The NSTISSC security model served as our framework for formulating pertinent questions for this survey. Section one of the questionnaire captured general information about the organization. In section 2, respondents identified the resources (hardware and software) used to store, process and transmit information. Using a five point Likert scale (1= strongly disagree; 5 strongly disagree), respondents were also requested to indicate their agreement/disagreement with statements that measured the threats and vulnerabilities in the systems; the awareness of current risks, standards and security protocols; and the effectiveness of measures used to ensure security in their organisations. Most of the survey items were adapted from recommended security practices and previous security studies (Internet Security Alliance, 2004; Straub, 1990; Thong, 1999).

The questionnaire was developed after several discussions with 2 Internet service providers, 4 small business owners, 6 Internet home users and three academic staff. It was then pre-tested for content validity, general format and readability with 8 small business owners and 6 home Internet users in the Free State province.

4.1 The Sample

The composition of the sample is shown in Figure 2. Respondents were selected from economic sectors that contributed substantially to the Gross Geographical Product (GGP) of the Free State province (Free State Provincial Government, 2001). This was important since attacks against the information systems in these sectors would have serious economic and social implications for the Free State economy. In addition, according to SAITIS (2000) the selected economic sectors represent the largest numbers of Internet-connected PCs in South Africa and their e-commerce transaction values were significant in the previous years, except for the Construction sector. The sample also included 22 home Internet users selected at random from the region. These were included in the sample because they have become common targets for hackers. It is also estimated that more than 60% of Internet users are home users (SAITIS, 2000).

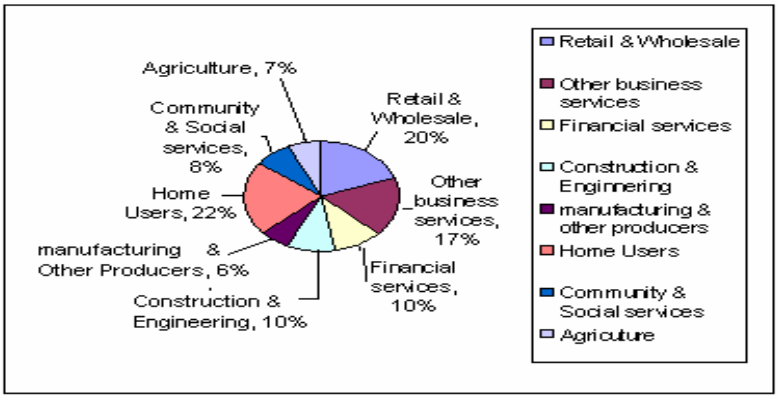

Figure 2: Respondents by industry sector

Only those engaged in e-commerce participated in this study. It was difficult to identify these respondents since there isn't a compiled list of such users in the province. Efforts to get information from some Internet Service providers were also futile since they could not disclose clients' details. We therefore decided to use the list of small-sized firms registered with the department of labour in the Free State province (all firms are required to register with this department in South Africa). First, those falling within the GGP sectors were identified and later during the survey, those engaged in e-commerce were then selected.

The survey questionnaire was completed in the presence of our research team. This enabled us to obtain responses quickly, clarify unclear questions and to verify the answers where possible. Initially, 142 organisations were selected from the labor list and across the GGP sectors. 36 were dropped of which 10 were not connected to the Internet, 14 were not engaged in e-commerce and 12 were no longer economically active. In addition, six responses were also rejected due to inconsistencies in the information provided. The total valid responses were therefore 100 collected from owner-managers, business assistants and business managers. In order to avoid any effect of small numbers, respondents involved in business activities such as computer services, transport and training were placed under "Other business services". Content validity was established by ensuring that most of the measures were adapted from prior studies as indicated above.

5 RESULTS AND DISCUSSION

Home Internet users and small organisations in South Africa are highly vulnerable to attacks than they realize. Many do not have a security plan. They use outdated hardware and software and heavily rely on technological measures which are never updated to match the rapid changes in threats and technology. The sections below discuss some important findings of this study.

5.1 Hardware and Operating Systems used

Figure 3 shows that many organisations still use old Pentium I and II computers. It is also surprising to find that there are more users of vulnerable operating systems such as Windows 98 (34%) than the more secure Windows XP (25%). 35% of the respondents use Windows 2000 and only a few use other operating systems such as Unix, Linux and Novell (6%). The need to upgrade to more secure software and hardware has not been taken seriously by these respondents. This is also confirmed in Figure 5 by the low proportion of respondents (20%) who installed current patches such as Windows XP service pack 2. We also found that respondents do not make use of on-line help services provided by vendors nor do they subscribe to vendor mailing lists. This is a serious weakness since it is mainly through such services that we learn about potential vulnerabilities, attacks and possible fixes. Some respondents however indicated that vendors do not permit independent verification of their privacy procedures nor do they cover potential data security breaches.

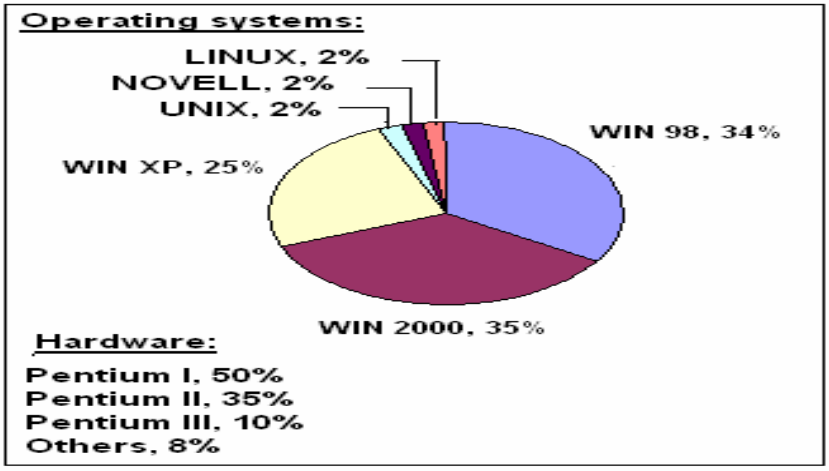

Figure 3: Hardware & Operating Systems used

5.2 Possession of a security policy

Figure 4 shows that majority of respondents (74%) do not possess a formal computer security policy. Guidelines addressing issues such as access rights, password standards and in some cases roles and responsibilities were not in place. In many instances we found that users had full-time access to the Internet and web browsing. Previous studies show that many small firms fail to plans and protect their IT resources (Kyobe, 2004). This could be explained by the general lack of awareness of security risks as revealed in Figure 5. Insufficient awareness of potential IT opportunities, IT risks and computing limitations are major factors inhibiting small organizations from engaging in IS planning and policy development (D'Amboise, 1990; Frieswick, 1996).

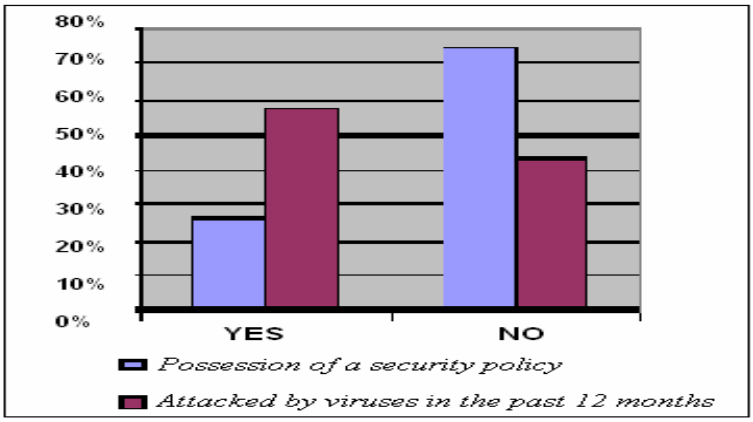

Figure 4: Possession of a security policy vs. Virus attacks

Furthermore, small organizations do not keep formal records of business objectives and IS requirements. This information is needed to guide the policy development process (D'Amboise, 1990; Raymond, 1993).

5.3 Attacked by virus in the last 12 months

Figure 4 also shows that (57%) of the respondents were victims of e-crime in the past 12 months and as indicated in Table I, approximately 89% of these did not possess a security policy. We conducted a Chi Square test to determine whether there is any association between lack of a security policy and occurrence of virus attacks. The Yates corrected Chi-square results were (14.68, p = 0.0001) suggesting that these two variables are associated.

Table I: Chi-Square Tests

	Attacked by Virus in past 12 months		
Possess a security Policy	**NO**	**YES**	Row Total
NO	23	51	74
YES	20	6	26
Column Total	43	57	100
Yates Corrected Chi-Square (df = 1)	14.68	p = 0.0001	

While 43% of the respondents claimed not to have been attacked (Figure 4), the spate of worms reported in South Africa (Sophos, 2004), the multiple vulnerabilities in Microsoft Internet Explorer (US-CERT, 2004), and the recent increase in variants of worms (Dunham, (2004) suggest that some of these organizations were either unwilling to admit to experiencing cyber attacks or were simply not aware of the attacks. With many computer attacks being surreptitious in nature these days, detecting them can be very difficult. Respondents that experienced attacks mainly identified Spyware, Code red, Blaster worm and Phishing.

5.4 Responsibility for security maintenance

32% of the respondents did not have any one to maintain their security systems, 36% outsource IT specialists and 40% in-source these services. Most of those that in-source security services often use people who are inadequately trained or qualified to handle technical and security aspects. Respondents were also concerned about the poor commitment of out-sourced IT specialists. In a previous study, the author found that firms providing IT services in the region are generally small in size, were established recently and operate with limited resources (Kyobe, 2004). There is a high possibility that such organizations could fold anytime without providing any warning to those customers who might have entrusted them with vital information. The department of trade and industry (DTI, 2002) has therefore recommended that more rigorous IT quality-control standards be introduced to ensure provision of appropriate services to small organizations.

5.5 Security Measures Implemented

5.5.1 Technology-based measures

It is indicated in Figure 5 that password protection (67%) and anti-virus software (68%) are the major security measures employed by small organizations and home users in the Free-state province. (24%) of the respondents possess firewalls, (3%) use Intrusion Detection Systems while (39 %) backup important files. Encryption and authentication technologies (1%) are the least used security mechanisms. These results are consistent with those in Figure 6 where few respondents were aware of security standards and protocols such as Pretty Good Privacy (PGP

1%), Secure Socket Layer (SSL 15%), Secure Hyper Text Transfer Protocol (HTTPS 21%) and S/Mime (9%). This suggests that many of these users enter the on-line trading arena with little or no knowledge of the potential cyber risks.

5.5.2 Non-technology based measures

The proportion of respondents that implemented non-technological measures such as Internet usage procedures (13%) security awareness training (7%) and incident reporting (21%) is also small (see Figure 5). File backup is however done by almost 40% of the respondents though backup copies are often made on floppies and left in the same premises.

5.5.2.1 Security education, training and awareness

Awareness training assists in the development of a strong security culture. It is a catalyst for proper application and use of technology and enhances communication of policies. Unfortunately, this is a low priority area for many organisations. Solms and Solms (2004) assert that the lack of awareness sin is still committed by many firms consequently users are unaware of the risks of using their IT infrastructure and the potential damage they can cause to it. It is also unfortunate that when budget crises occur, training and awareness are among the first areas in which the budget is slashed (Schultz, 2004).

There is therefore over reliance on technology-based measures (e.g. password protection and anti-virus software) which by themselves cannot prevent computer related crime. A combination of both technology and non-technology based measures is necessary.

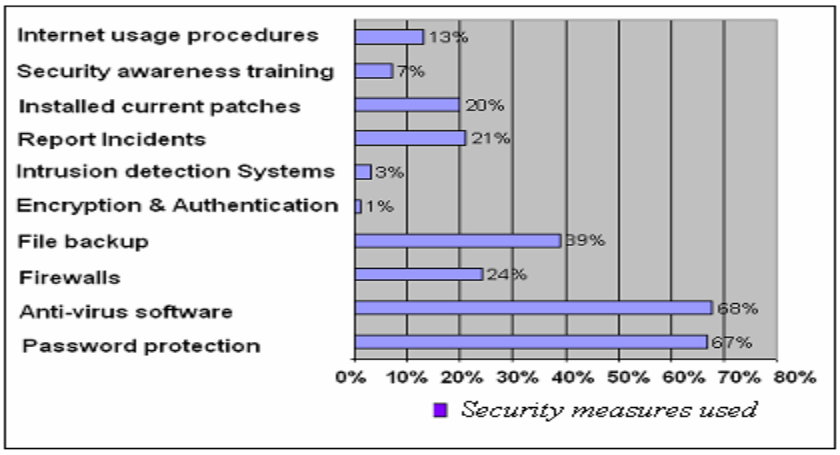

Figure 5: Security Measures used

5.5.2.2 Reporting of incidents

Only 21% of the respondents in Figure 5 reported security incidents to vendors, management and law enforcement agencies, the rest (79%) did not. Several reasons were provided during our discussions with these respondents. First, these users often do not have the technical competence to decide if an incident is malicious or not, a crime or a malfunction (technical faults). As indicated above, 36% lacked expertise to maintain their security.

A number of respondents simply fear losing business if customers or suppliers know they were attacked. Others indicated that if they reported these incidents to the Police, their equipments might be taken away as part of the investigations. Furthermore, some respondents were discouraged by the non-responses from vendors and law enforcement agencies and as such stopped bothering. There was also a general feeling that the law enforcement agencies were not pushing hard enough for companies to contact them when attacked. Schronen and Van der Merve (2002) blamed the escalating e-crime problem on the South African court system and inexperienced detectives who lack the necessary skills in handling e-crime cases. They reported that about 20% of the reported white-collar crimes reach the court and only 8.3% result in convictions. It is also alleged that South African laws are outdated and ineffective in addressing current e-crime problems (Levin, Esselaar and Davies, 2004).

5.5.3 Awareness of security legislations and standards

Figure 6 also shows that almost 50% of the respondents were not aware of important security protocols and standards. Only (22%) were aware of ISO17799, (15%) SSL and (21%) Secure HTTP. PGP (5%) and S/Mime (9%) were known by few respondents and only 10% knew others standards such as government IT security standards, Vendor and Industry specific standards. These results indicate respondents' limited understanding of the regulations and legislation surrounding their security systems and data transmission.

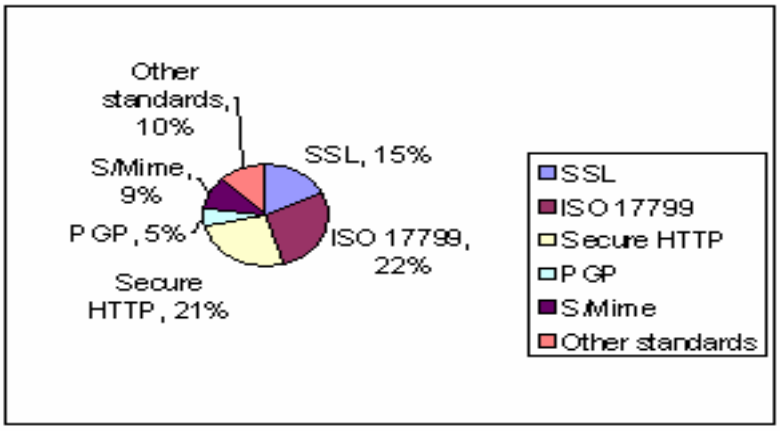

Figure 6: Awareness of security protocols & Standards

6 CONCLUSION

Small organizations and home Internet users in South Africa are more vulnerable than they realize in terms of security breaches. Since these organisations form a major source of employment and income generation in South Africa, and considering the much effort that has been made by banks and government to encourage small firms to adopt e-commerce, failure to attend to the current escalating security problems particularly in these organisations will result in dire social and economic consequences for the economy.

7 A SECURITY GUIDE FOR SMALL BUSINESS ORGANISATIONS

A security guide for small business organizations is provided in this section. This is based on a number of generally accepted principles and practices for securing Information Technology systems (NIST Special Publication 800-14; ISO 17799; US CERT; ISIZA; Internet Security Alliance, 2004). It consists of nine (9) straight forward best practices that would ensure better security in these organizations. For each security practice, the author identifies WHAT has to be done, the reasons for conducting the practice (WHY) and suggests how it should be done (HOW).

Practice 1

WHAT: Do not ignore security. Recognize its importance to your organization.
WHY: Any computer accessing the Internet is vulnerable. Resources such as bandwidth, disk space and information are ideal targets for attackers. It is also not uncommon for hackers to maliciously destroy a system when they find nothing of value in it.

HOW: Make security a business driver and prioritize it. Consider security to be an investment decision that has a direct impact on your survival and success. Always be aware of the legal, economic and social implications of e-crime.

Practice 2

WHAT: Implement a Security Policy and Procedures
WHY: An Internet user must possess a security policy that guides behaviour and security practices. It will provide protection to your organisation's assets and will be an effective tool in resolving security breaches.

HOW: Start by adopting available international best practices for security governance. ISO 17779 (available from www.iso.ch) provides a useful and internationally accepted framework on which to base an organisation's security policies and procedures. Professional bodies like ISIZA (www.isi-za.org) have also provided useful assessment tools. Your security policy should at a minimum include definitions of access and usage requirements, levels of protection, level of traffic through the system and security tools to be used.

Practice 3

WHAT: Keep current with security alerts and software updates.
WHY: Outdated or outmoded systems contain many vulnerabilities. Intruders read the same vendor mailing lists and notifications of vulnerabilities. We are moving to a 'zero-day' scenario whereby vulnerabilities are announced and exploited on the same day.

HOW: Always retire outdated systems. Download, scan and install patches as soon as they are released. Consider purchasing extended warranty support and subscribe to a vendor mailing list for notification of problems and fixes. Visit one or more of the following sites daily: CERT coordination Center (http://www.cert.org); Computer Incident Advisory Capability (http://www.ciac.org/).

WHAT: Ensure security awareness and training.
WHY: Your best security stewards of critical data and information assets are the employees. When properly trained, a security culture develops and many risks are mitigated.

HOW: Design, develop, implement a security awareness program. Measure its effectiveness and update it promptly. Communicate security requirements and risk management techniques to your staff. Ensure security in job descriptions and when hiring resources. Work towards ISIZA (2004), BSI, ISO 17779 or ISO9001:2000 certification. Such schemes provide a reputable means to measure your information security management against best practices.

Practice 5

WHAT: Employ competent people to manage your system security.
WHY: Maintenance of a secure system is a complex task. There should be some one in the organization fully responsible for identifying vulnerabilities, reporting security violations, directing policies and procedures designed to protect information resources (e.g. back-up) and develop security awareness programs.

HOW: Consider getting reliable technical expertise from other organizations if such knowledge does not exist already. Train one or more staff members to handle security problems. Back-up your data regularly.

Practice 6

WHAT: *Use 'strong' passwords*

WHY: Weak passwords weaken networks and systems. Attackers use automated tools to crack passwords and often social fraud (social engineering) to persuade users to divulge their passwords. The root cause of hundreds of corporate breaches, identity theft and financial fraud is the password. It is therefore recommended to use strong and unique passwords.

HOW: Do not use dictionary words or names of people (e.g., related to you), a combination of characters, numbers and punctuation marks may be appropriate. Password should always be encrypted during transmission. They should never be shared or kept in obvious places (e.g., under the keyboard, in drawers or on top of your screen). Change them regularly.
Practice 7

WHAT: Protect against viruses

WHY: Viruses are released on a zero-day basis. They are becoming complex, sophisticated and are a serious ever-evolving threat. They can jam your system resources, infect data and damage your hard disk.

HOW: Install and use recommended anti-virus software. Consider using trial versions of the program first. Determine if you can scan files and attachments and fix damages. Consider using email filtering programs e.g. *SpamAssassin* (http://spamassassin.org); *GFI Mail security* (http://www.mailessentials.com); and *Spam Tester* (http://www.dnsstuff.com).

Practice 8

WHAT: Install and use a firewall program and hardware.
WHY: A firewall protects your network from unwanted Internet traffic by permitting only appropriate messages. It is your first line of defense.

HOW: Decide the right amount of security without imposing unacceptable limitations on other users or undue management complexity. Ensure that your computer connects to reliable Internet locations and deny connections to suspicious locations.

Practice 9

WHAT: *Ensure that electronic transmissions are authenticated & encrypted.*.
WHY: Attackers often break into networks by listening to network traffic at strategic locations. Remote connections and all financial transactions must be secured.

HOW: Use products such as Private Key Identification (PKI) software. This provides strong customer identification, certificate authority and digital certificate issuance capabilities.

8 REFERENCES

D'Amboise, G. (1990). Strategic planning for small and medium-sized business: some proposed ways to go about it. *Southern African Journal for Entrepreneurship and Small Business* 2(1): 7-13.

DTI - Department of Trade and Industry (2002). *Implications of the Information Revolution for Economic Development in South Africa.* Project code: A.1.009, July 2002.

Dunham, K. (2004). Why SoBig Is Big. *Information Systems Security* 13(1): 2-7.
Free State Provincial government. (2001). *Free State Development Plan (2000-2005).* Retrieved December 12, 2005, from http://www.fs.gov.za/freestatedevplan/content/fsdp/final first draft report 01.09.31.doc.

Frieswick, K. (1996). Mixing progeny and profits. *Industrial Distribution* 85(4): 44-49.

ISIZA- Information Security Institute of South Africa (2004). *Resources and self assessment tool.*. Retrieved September 5, 2004, from http://www.isi-za.org.

Internet Security Alliance (2004, February). Common Sense Guide to cyber security for small Business. Retrieved October 22, 2004, from www.isalliance.org/resources%5Cpapres%5C31665_ISA_Small%20Bus%20Guid%20_LO-RES_web.pdf.

Kyobe, M. (2004). Investigating the Strategic Utilisation of IT resources in the small and medium-sized firms of the Eastern Free State province. *International Small Business Journal* 22(2): 131-158.

Levin, A., Esselaar, P., and Davies, S. (2004). Response to ICASA question document on ministerial determinations of 3 september 2004, *Governement Gazette 26763, notice 1924 of 2004. Internet Society of South Africa*. Retrieved October 14, 2004, from www.isoc.org.za.

Lombard, E. (2003). Hacker cleans out bank accounts. *Sunday Times News*. Retrieved October 22, 2004, from http://www.sundaytimes.co.za/2003/07/20/news01.asp.

Masurel, E. (2004). SMEs and Crime, Evidence from the Netherlands. *International Small Business Journal* 22(2): 197-205.

McConnell, J. (1994). National Training Standard for Information System Security. Retrieved October 10, 2004, from http://www.nstissc.gov/Assets/pdf/4011.pdf.

Raymond, L. (1993). Computerisation as a factor in the development of young entrepreneurs. *International Small business Journal* 11(1): 23-34.

SAITIS. (2000). A Survey of the IT Industry and Related Jobs and Skills in South Africa. *SAITIS BASELINE STUDIES*. Retrieved October 14, 2004, from http://www.saitis.co.za.

Schronen, J. and Van der Merwe, J. (2002). White-collar crime cleans up R40bn a year. *IOL SouthAfrica*. Retrieved October 15, 2004 from http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=ct20010319091018396L300510.

Schultz E. (2004). Security training and awareness – fitting a square peg in a round hole, *Computer and security* 23(004):1-2.

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

Sophos.com. (2004). South African government departments hit by Sasser. *Virusinfo*. Retrieved January 9, 2005, from http://www.sophos.com/virusinfo/articles/sasserza.html.

Straub, D.W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, 1(3), 255-276.

Thong, J.Y.L.(1999).An integrated model of information system adoption in small businesses. *Journal of Management Information System*, 15(4), 187-241.

US-CERT (2004). *US-CERT Technical Cyber Security Alert TA04-2939A 2004.* Retrieved December 12, 2004, from http://www.us-cert.gov/cas/techalerts/TA04-2939A.

Zorz, J.(2003, May 15). Small firms 'shun' PC security. *BBC NEWS*. Retrieved October 15, 2004, from http://www.net_security.org/news:php?id=2650.