INFORMATION SECURITY POLICIES FOR GOVERNMENTAL ORGANISATIONS, THE MINIMUM CRITERIA

SJ Ngobeni[1] & MM Grobler[2]

Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa

[1]sngobeni@csir.co.za, 012 841 4410

[2]mgrobler1@csir.co.za, 012 841 2838

ABSTRACT

Recent technology advancement has resulted in an era where many organisations become more and more comfortable to use computer systems to process their information. Intruders are making it their mission to break into these computer systems and access valuable information in an unauthorised way.

Information Security policies are seen as not only a counterproposal, but also a solution to Information Security effectiveness. However, a key issue impacting Information Security policies is what should be included in these policies. This study makes an attempt to design a Comprehensive Information Security Policy (CISP) to serve as basis for organisations when designing their own Information Security policies, based on a public survey on IT related governmental Information Security policies.

KEY WORDS

Information Security policies, standards, organisations

INFORMATION SECURITY POLICIES FOR GOVERNMENTAL ORGANISATION, THE MINIMUM CRITERIA

INTRODUCTION

Information can be regarded as a crucial business asset important for business continuity, and consequently needs to be protected. The protection of information is especially important due to the rapid increase of the interconnected business world, exposing information to a variety of threats and vulnerabilities. This information needs to be protected [1].

Information Security is seen as the process of protecting information and information systems from a range of threats and vulnerabilities to ensure business continuity, minimising business risks and maximising return on investments and business opportunities. This protection can be achieved by implementing suitable Information Security policies. These policies need to include relevant key issues impacting Information Security to enable this protection.

This study designs a Comprehensive Information Security Policy (CISP) to serve as basis for organisations when designing their own Information Security policies. This is achieved by first identifying and evaluating the Information Security policies of several IT related governmental organisations, and then formulating a theoretical framework for the evaluation of these policies. The results from the evaluation are then used to design the proposed CISP. The CISP can be adopted by any IT related governmental organisation as a guideline when designing or reviewing their Information Security policies. A literature survey was conducted to gain insight on Information Security policies and various South African IT governmental organisations were contacted to collect their policies.

The paper is structured as follows: Section 2 provides background knowledge on Information Security policies; Section 3 presents a theoretical framework for the evaluation of the policies; Section 4 presents

the evaluation and analysis of the policies and Section 5 presents the proposed CISP. Section 6 concludes this paper and discusses future work.

1 BACKGROUND

This section provides background information on Information Security policies. It presents an overview of Information Security policies and defines the boundaries of such a policy. Lastly, it presents a discussion on the key elements that an organisation needs to consider when designing an Information Security policy.

1.1 Overview

Information Security policies are the cornerstone of Information Security effectiveness. Public and private sector enterprises today are highly dependant on information systems to carry out their mission, vision and business functions [2]. Without a policy on which to base standards and procedures, decisions are likely to be inconsistent and security holes may be present, ready to be exploited by internal and external parties [3]. Accordingly, information must be protected to prevent the exploitation of valuable information, regardless of the information's format.

This study states that the protection of information and its systems can be achieved by employing Information Security policies within the government and the business organisation. Many governmental departments have adopted the use of these policies as the primary way to achieve their goals and business continuity. However, the exact framework of an all-inclusive Information Security policy is still to be decided. This study evaluates the Information Security policies of various IT related governmental organisations and further uses the results of this evaluation to design the CISP.

1.2 What are Information Security policies?

An Information Security policy can be defined as a document that outlines the rules, laws and practices for computer network access [4]. This document regulates how an organisation will manage, protect and distribute its sensitive information (both corporate and client information) and lays the framework for the computer-network-oriented security of the organisation.

Danchev [5] mentions a very important definition of Information Security policy: a plan that outlines the organisation's critical assets and

how the assets must (and can) be protected. The most important aspect of the Information Security policy is to provide security awareness within an organisation, engaging the employees to participate in protecting the organisation's valuable information. Danchev suggests a well designed policy addresses issues such as the acceptable use of the organisation's email system, the proper use of workstations and internet connectivity, how to respond to a security breach, the proper use of IDs and logging information, as well as handling of financial data.

1.3 The key Information Security policy elements

A well-written Information Security policy must satisfy the needs of the organisation, be practical and enforceable. This section discusses several essential elements that are necessary when designing an Information Security policy [6].

An Information Security policy should be:

- **Easy to understand**. The policy should be addressed in a manner that will meet the intended audience.
- **Applicable**. The policy must only contain security measures that are specific needs to the organisation.
- **Enforceable**. The policy should maintain a decent balance between being too defensive and too lenient.
- **Proactive**. The policy should state what is expected of employees instead of making pronouncements.
- **Doable**. The policy should be written in a way that will not restrict the objectives of the business.
- **Avoiding absolutes.** The policy should be written in a way that state things in a politically correct and in a diplomatic way.

2 A THEORETICAL FRAMEWORK FOR EVALUATING INFORMATION SECURITY POLICIES

Based on preliminary research and results retrieved from the public survey, the Information Security policies collected from IT related governmental organisations were reviewed based on the following characteristics:

1) **Access control.** The policy describes rights/permissions and to whom these rights/permissions can be granted with regards to accessing a particular resource within the organisation.
2) **Data classification and control.** Data need to be classified according to its level of sensitivity to assist the organisation in determining the extent security needed. Data can be classified as top secret, highly confidential, proprietary, internal use only or public use [7].
3) **Risk assessment.** The organisation's information systems need to be assessed to identify vulnerabilities that can affect the confidentiality, integrity and availability of the key information assets.
4) **Password and user ID management.** The policy should recommend rules for composing passwords, how to change and reuse passwords, and the need for keeping passwords.
5) **Encryption and digital signatures.** The policy need to address the need for encryption and digital signatures as means to achieve data security within the organisation.
6) **Instant messaging, PDAs and smart phones.** The policy must provide procedures and regulations regarding the use of Instant Messaging, PDAs and smart phones within the corporate environment [8].
7) **Security awareness and training.** The policy needs to facilitate compliance by employees regarding the organisation's stated rules and procedures [9]**.**
8) **Data privacy management for employees and customers.** The policy needs to address the privacy relationships between collection and dissemination of information [10].
9) **Corporate Governance.** The policy should discuss the procedures by which a business is operated, regulated and controlled. It should also discuss the internal factors defined by the officers, the constitution of the company and external forces such as consumer groups, clients and governmental regulations.

10) **Electronic mail, viruses, malicious code protection and social engineering attacks, including phishing scams.** The policy should describe methods of creating, transmitting or storing primary text-based human communications with digital communication systems. It must address the protection of the organisation's networks and information systems from being viruses and social engineering.
11) **Identity theft.** The policy needs to address the prevention of identity theft and related attacks.
12) **Network security.** The policy addresses the protection of the network and its services, unauthorised modification, destruction and disclosure of information, and assuring that the critical network functions correctly.
13) **Firewall.** The policy should address the use of firewalls to prevent unauthorised internet users from accessing the organisation's private networks connected to the internet.
14) **Communication security, including telephones and fax machine.** The policy should cover issues related to the security of telephone and fax equipment [11].
15) **Website and e-commerce security.** The policy should describe how to protect the organisation's website against security weaknesses such as SQL injections, Denial of Service attacks and spam relaying.
16) **Security in third party contracts, including outsourcing and off-shoring of IT project.** The policy should address security in its infrastructure and assets, whilst complying with regulations applicable to third party contracts [12].
17) **Document destruction, as well as retention of documents that may be used in courts cases.** The policy should clearly address the destruction and retention of documents.
18) **Incident response.** The policy discusses issues concerning how an organisation responds quickly and effectively to a system or network security breach [13].
19) **Contingency planning.** The policy needs to address contingency planning, or the disaster plan. This describes the organisation's immediate actions to respond to unexpected business interruptions or accidental disasters [14].
20) **Telecommuting and mobile computing.** The policy should address telecommuting as a means to replace work-related travel [15].
21) **Intrusion Detection Systems (IDSs).** The policy should describe methods to detect malicious network traffic and computer usage.

3 EVALUATION OF INFORMATION SECURITY POLICIES

Table 1 indicates the review of various Information Security policies for four IT related governmental organisations, as provided directly by the governmental organisations. Due to the strict regulations of these participating organisations, the Information Security policies used in this evaluation need to remain anonymous.

The characteristics column of Table 1 indicates what a good policy should contain. This list (identified in Section 3) is not all-inclusive, but based on the literature study done for this specific study. An organisational policy containing a characteristic that corresponds to any of the 21 characteristics identified in the theoretical framework is marked with an "X", and if it does not contain a corresponding characteristics it is marked with a "-".

Table 1: Review of Information Security used in this study

Characteristic	***Organisation A***	***Organisation B***	***Organisation C***	***Organisation D***
1. Access control	X	X	X	X
2. Data classification and control	_	X	X	X
3. Risk assessment	X	X	_	_
4. Password and user ID management	X	X	X	X
5. Encryption and digital signatures	X	_	X	X
6.Instant messaging, PDAs and smart phones	X	_	X	_
7. Security awareness and training	X	_	X	X
8. Data privacy management	X	_	X	X

Characteristic	***Organisation A***	***Organisation B***	***Organisation C***	***Organisation D***
9. Corporate governance	X	X	X	X
10. Electronic mail, viruses, malicious code protection, and social engineering	X	X	X	X
11. Identity theft	X	_	X	X
12. Network security	X	X	X	X
13. Firewall	X	X	X	X
14. Communication security	_	_	X	X
15. Website and e-commerce	X	_	X	X
16. Security in third party contract	X	_	X	_
17. Document destruction and retention	X	_	X	X
18. Incident response	X	X	X	X
19. Contingency planning	X	_	X	X
20. Telecommuting and mobile computing	_	_	X	_
21. Intrusion Detection Systems	X	X	X	X

From Table 1 it can be detained that not all existing Information Security policies are adequate. For example, Organisation A fails to address three of the identified elements and Organisation B fails to address eleven elements. Organisation C has a well formulated policy and addresses all the characteristics identified by the theoretical framework. Organisation D does not address four of the identified elements.

4 THE CISP

This section presents the proposed CISP. Figure 1 shows the proposed CISP on the next page.

5 CONCLUSION

The main goals of this study were to evaluate Information Security policies of various IT governmental organisations and design a resulting CISP. These goals were attained successfully.

The results of this study may not be optimal due to the limited number of Information Security policies that were evaluated. Various IT related governmental organisations were invited to participate in this survey, but had to decline due to organisational privacy requirements. The reviewed policies shows that most of the governmental organisations were found to omit the most significant issues that are supposed to be included in their Information Security policies (refer to Table 1).

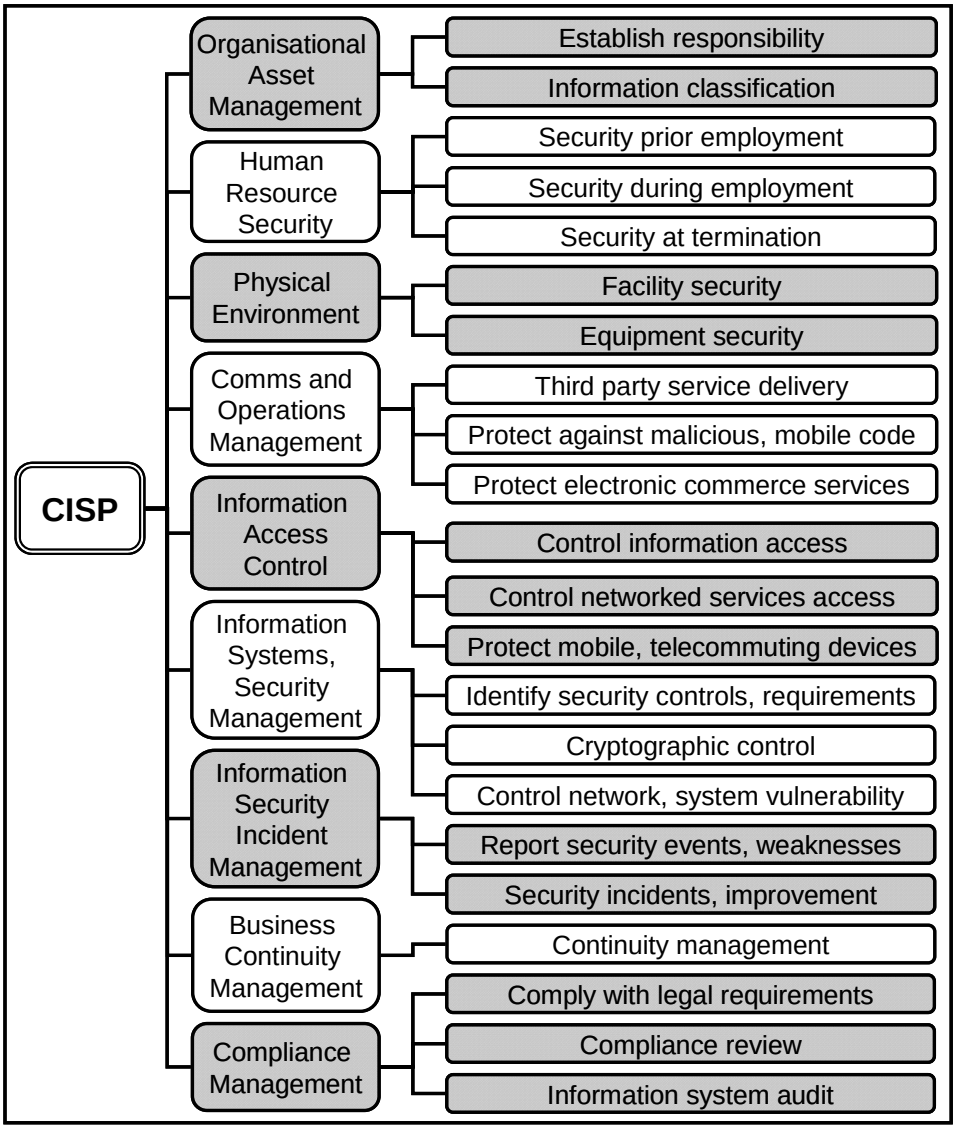

Figure 1: CISP

The proposed CISP provide organisations with a generic model to use when designing their own Information Security policies. Therefore, any IT governmental related organisation that needs to design or upgrade their Information Security policies may adopt the CISP. Consistent with the changing nature of technology, the Information Security policies will

be subject to change as well. Accordingly, the CISP may be valid for a set period due to technology improvements and will need to be upgraded.

REFERENCES

[1] Berk, DD. 2007. *How do you define Information Security*. Available from: http://www.linkedin.com/answers?viewQuestion=&questionID=56225&askerID=292188&goback=.hom.mid_138471153 (Accessed 2 April 2009).

[2] *Information Security: A Business Manager's Guide*. 2004. Department of Trade and Industry, Available from: http://www.berr.gov.uk/files/file9981.pdf . (Accessed 02 February 2009).

[3] Information Security. 2002. *Draft Position Paper on Information Security*. Available from: http://www.dpsa.gov.za/documents/acts&regulations/frameworks/e-commerce/POSITION%20PAPER%20ON%20INFORMATION %20SECURITY1.pdf (Accessed 2 September 2008).

[4] *Security policy*. 2008. Available from: http://www.webopedia.com/TERM/S/security_policy.html (Accessed 15 January 2009).

[5] Danchev, D. 2003. *Building and implementing a Successful Information Security Policy*. Windows Security resources for IT admin, Available from: http://www.windowsecurity.com/pages/security-policy.pdf (Accessed 9 October 2008).

[6] Piscitello, DM. 2009. *Guide to network security*. TechTarget. The IT Media ROI Experts. Available from: http://searchsecurity.imix.co.za/static/pdf/cisco/Eguide_NetworkSecurity.pdf (Accessed 07 April 2009)

[7] *Data classification.* 2007. Available from: http://searchdatamanagement.techtarget.com/sDefinition/0,,sid91_gci1152474,00.html (Accessed 14 December 2008)

[8] *7 things you should know about instant messaging.* 2005. Available from: http://connect.educause.edu/Library/ELI/7ThingsYouShouldKnowAbout/39385?time=1234488280. (Accessed 5 February 2009).

[9] Wilson, M. & Hash, J. 2003. *Building an Information Technology Security Awareness and Training program.* National Institute of Standards and Technology. Available from: http://csrc.nist.gov/publications/ nistpubs/800-50/NIST-SP800-50.pdf (Accessed 17 April 2009).

[10] *Privacy and Data Protection Draft Bill.* 2006. Available from: http://www.pmg.org.za/node/14653 (Accessed 18 February 2009).

[11] Rothke, B. 2008. *The lack of Security in Fax Machine and How to Secure it.* Available from: http://www.brighthub.com/computing/ enterprise-security/articles/8262.aspx (Accessed 13 January 2009).

[12] Framingham, DD. 2008. *Outsourcing and offshoring: A Security Expert's views, Beware of traps and pitfall.* Available from: http://computerworld.co.nz/news.nsf/spec/7DE10CD28E670122CC2575 070082D737 (Accessed 24 November 2008).

[13] *Incident Response*. 2002. Available from: http://www.redhat.com/ docs/manuals/linux/RHL-9-Manual/security-guide/ch-response.html (Accessed 02 February 2009).

[14] Herricott, L. 1997. *Disaster Recovery Journal.* Available from: http://www.drj.com/new2dr/w3_006.htm (Accessed 5 December 2008).

[15] *Telecommuting*. 2009. Available from: http://www.webopedia.com/ TERM/t/ telecommuting.html (Accessed 2 February 2009).