ASSESSMENT OF INFORMATION SECURITY POLICIES

WITHIN THE POLOKWANE REGION: A CASE STUDY

SA Mlangeni and E. Biermann

Tshwane University of Technology

SA Mlangeni, Private Bag X 9496, Polokwane, 0700

MlangeniSA@tut.ac.za, 015 287 0733

Dr. E. Biermann, Faculty of Information and Communication Technology

Private Bag X680, Pretoria, 0001

biermanne@tut.ac.za, 012 318 5684

ABSTRACT

Computers as well as the networking environments in which they operate, have evolved into highly sophisticated and complex systems. The intricacy of these systems and especially the relationship between them forms the greatest area of vulnerabilities for organisations (Whitman & Mattord, 2004).

Information needs to be transmitted to and from the organisation, and thus may be vulnerable within certain stages along the communications line. If at any stage of the process, the information is compromised, it could have a negative impact on the entire organisation. Protective measures such as disaster recover plans, encryption / decryption, and information systems controls, can minimize or prevent the negative consequences. It is vital therefore that management of information systems take measures to protect their critical data and information from loss, damage, and misuse.

The process of minimising risks associated with information security includes the compilation of a detailed and standardised information security policy. Such a policy has to address issues such as threats and possible countermeasures as well as defining roles and responsibilities.

The aim of this study is to assess the status of information security policies compiled and implemented by different companies in the Polokwane region. During this study, the existence and format of the information security policy sets as well as the commitment of organisations to address security issues will be measured.

KEY WORDS

Information security policies, Information security models, Information security policy assessment.

ASSESSMENT OF INFORMATION SECURITY POLICIES

WITHIN THE POLOKWANE REGION: A CASE STUDY

1 INTRODUCTION

In recent years the computer industry has been revolutionised by the concept of communicating across networks. A large factor in this development has been the introduction of the Internet. The Internet was originally designed to help the Military establishment and researchers at different sites in the United States of America share computers and information (Leiner *et al.*, 1998).

Over the years the concept has changed and the domain is no longer limited to the academic and scientific community or to a single country. A person that has access to technology such as a personal computer, a modem and a telephone line can access the Internet. This huge increase in the connection of people and resources globally has introduced an array of problems in regards to the protection of sensitive information.

Security threats (and accordingly attacks) such as modification of information, masquerading or denial of service has increased dramatically in the past few years. Attacks are becoming increasingly more sophisticated as the field of computer and network technology evolves, for example new viruses and worms spread much faster and can potentially cause more damage than in the past. The level and quality of countermeasures to these threats depend on the quality of the security services and supporting procedures. The specific mix of these attributes is governed by the security policy of the organisation (Bishop, 2003).

According to Pfleeger & Pfleeger (2003) a security policy is a high-level management document that inform all users of the goals and constraints on using a system, and must answer three questions, namely *who* can access *which* resources in *what* manner. Procedure or guideline documents are created to define how the security policy translates into specific actions and controls.

The need for an information security policy in the strive towards the securing of information, has been established extensively in both the research and industry fields (see Von Solms & Eloff, 2001; Stefanek, 2002; Schneier, 2000; Whitman & Mattord, 2004). The question arises, however what is the firstly the existence and secondly the format status of information security policies within South African organisations.

2 INFORMATION SECURITY POLICY

Whitman & Mattord (2005) states that management from all communities of interest must consider security policies as the basis for all information security planning, design and deployment. The NIST 800-14 special publication stated that management must define three types of security policies, namely *general or security program policy, issue-specific security policy* and *systems-specific security policy.*

General security policy

According to Grobler & Von Solms (2004), a general policy is defined at a strategic management level of the organisation, and will set the strategic direction and scope of the security efforts within

the organisation. It typically defines the purpose, scope, constraints and applicability of a security program and further assigns responsibilities to various areas of security, such as systems administration, maintenance of policies and user education.

Issue-specific policy

Whitman & Mattord (2004) state that an issue-specific security policy provides detailed, targeted guidance to instruct all members of an organisation in the use of technology based systems. It articulates the organisation's expectations about how the technology-based systems should be used as well as documents how the technology-based systems are controlled. The processes and authorities that provide this control is also identified, and when implemented it can serve to indemnify the organisation against liability for an illegal use by an employee. Issue-specific policies may be drafted on topics such as electronic mail; Internet and use of photocopy equipment.

Systems-specific security policy

This type of information security policies are codified as standards and procedures to be used when configuring or maintaining systems. Standards are mandatory elements regarding the implementation of a policy while procedures are step-by-step instructions on how to implement policies within the organisation (Conklin *et al.*, 2004). Two general groups of systems-specific security policies are identified namely *access control lists* and *configuration rules*. Access control lists tables the rights and privileges of a particular user to a particular system, while configuration rules are specific configuration codes entered into security systems to guide the execution of the system as information is passing through it (Whitman & Mattord, 2005).

3 INFORMATION SECURITY POLICY MODELS

According to Chow & Mun (2000) standardisation within the information technology field is beneficial in that it provide for interoperability and ease of integrating components. A number of organisations and centres exist who aims to provide standards and regulations for information security policies, of which *NIST* and *ISO* is recognised worldwide as the leaders.

3.1 NIST

National Institute of Standards and Technology (NIST)[1] is a non-regulatory federal agency within the U.S.A. Its mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. In terms of computer security it provides principles and practices for securing information security systems. The NIST publications include a large number of documents developed to assist security specialists in designing security frameworks. These documents include for example the *SP 800-12: An Introduction to Computer Security*, which focuses on the management of information security and *SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems* provide best practices and security principles. Within the document SP 800-14, the first principle for securing information technology systems is the establishment of a sound security policy as the foundation of protecting a system.

3.2 ISO 17799

This security model entails a comprehensive set of controls comprising best practices in information security, and is internationally recognised as a generic information security standard. It consists of ten main sections, namely *security policy, system access control, computer & operations*

[1] See http://www.nist.gov for additional information

management, system development & maintenance, physical & environmental security, compliance, personnel security, security organisation, asset classification & control and *business continuity management.* Each section contains detailed statements and clauses that comprise the ISO 17799[2] standard itself as well as provide recommendations for information security management.

4 CASE STUDY: POLOKWANE REGION

In the process of assessing information security policies, preliminary research was conducted by means of performing a case study within the Polokwane region. Different types of organisations are based within the region and our focus was directed towards the government structures. Questionnaires were developed and interviews were conducted with the relative information technology managers within the different government organisations.

4.1 Interviews

In order to determine the status of information security policies within the Polokwane region, the process and specifications set by Grobler & Von Solms (2004) were adopted and partly implemented. These specifications consists of six steps, namely *obtaining the existing policy set of the organisation, determining the completeness of the policy, determining if the format of the existing policy is correct, determining if there are underlying standards and procedures supporting the existing policies, determining if a policy management program exists* and *determining the overall status of the policy.*

The first step outlined above (*obtaining the policy)* was integrated with an interview with the relative manager. During the interview questions relating to issues such as the current threats experienced by the organisation, existence of a security policy and the format of the policy were addressed and documented.

The second step (*determining the completeness of the policy)* was conducted by completing a checklist on the existence of specific policies, such as *asset classification, education and training, e-mail* and *intellectual property.*

Step three (*determining if the format of the existing policy is correct)* were assessed by determining whether aspects such as *objectives of policy, management's intent / commitment,* and *policy statement* are contained within the policy, as well as adequately described.

The fourth step (*determining the existence of supporting documentation)* included assessing only whether such documentation exists or whether it is lacking.

The fifth step (*determining if a policy management program exists)* as well as the sixth step (*determining the overall status of the policy)* did not form part of this preliminary research.

4.2 Step 1: Obtaining the policy

A number of problems were experienced during the process of obtaining the information security policies. As these problems effects the outcome of this study, we deem it necessary to not just outline the problems but also to provide a categorisation. The categories are summarised as follows:

Sensitivity

[2] See http://iso.org for additional information.

The sensitivity issue is multiple in the sense that firstly extensive physical security measures exist within the companies that make access to the information technology professionals difficult. Secondly the chain of gaining approval to access documentation is quite cumbersome and time consuming, meaning the assessment process were 80% of the time extensively delayed.

Physical access to security related documents were difficult, mainly due to existing company policies on the sharing of information. People are generally also not comfortable with entering into interviews in regards to the assessment of their organisations, and don't want to share information and statistics on threats and implemented countermeasures.

Knowledge

In many cases managers and directors have just been appointed in critical positions, which mean that they are not yet familiar with existing documentation and implemented procedures. Some of the managers also stated that they are not in a position to assure that a set of information security policies were in place and/or existed. This could also imply they do not have security polices at the moment.

An alarming number of managers also stated that they were in the process of developing information security policies from the procedures that are currently in use. This may confirm that the specific managers and also the company do not have sufficient knowledge and expertise in regards to the essence and creation of a policy to protect information systems. This was confirmed in the interviews with managers admitting they are not familiar with the subject.

Commitment

Staff dedicated to the creation and implementation of information security policies is scarce within the targeted organisations and this unfortunately has a direct influence on the status of the security system. Managers in charge of the security and information security policies are also difficult to get hold of, due to their tight schedule.

Apart from the problems experienced a total percentage of 56% of the targeted organisations did provide the available documentation in various degrees. The results presented within the next sections are provided within this percentage of received documentation.

4.3 Step 2: Completeness of policy

Figure 1 and Figure 2 provides detail in terms of the existence of the different policies within the policy set. Policies such as *access controls, information classification* and *remote access* did not exist as part of the policy set at any of the organisations. Policies on Internet usage received the highest percentage of 50%. A possible explanation can be organisations attempting to limit the time their workforce spent searching the Internet for non-work related information. Policies in regards to electronic mail are also amongst the highest (40%), which is also seen as a forced countermeasure implemented by the different sectors.

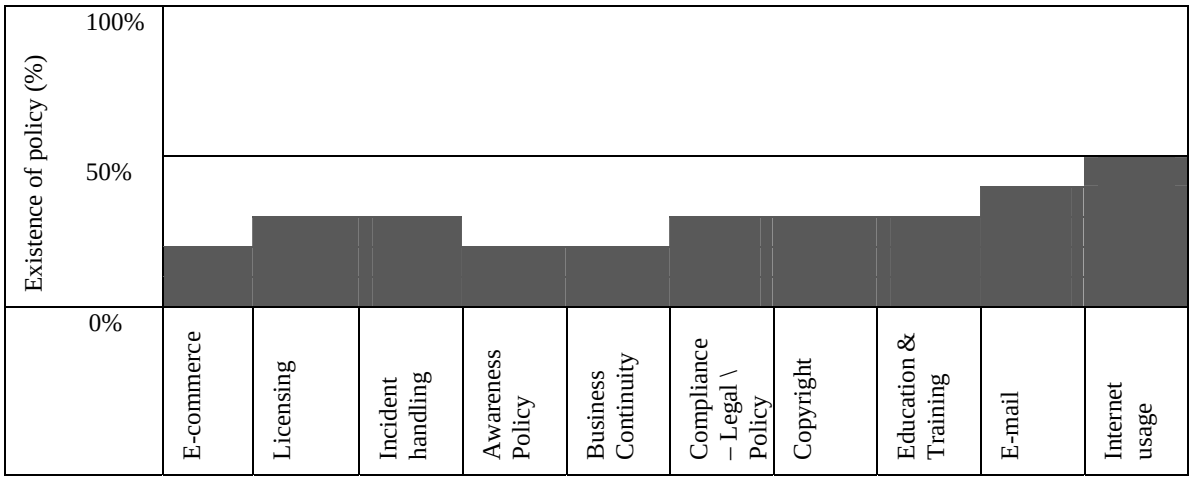

Figure 1: Policy completeness

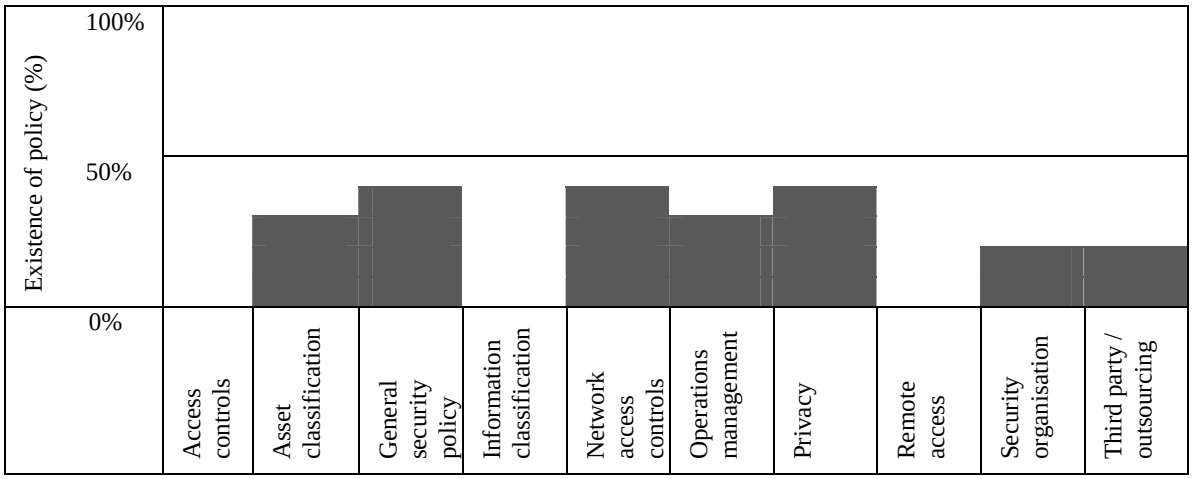

Figure 2: Policy completeness continued

The importance of the different policies as perceived by the organisations were also measured and the information is supplied in Figure 3 and Figure 4. The provided significance of the different policies is extremely low, which offers some explanation towards the lack of such policies within the targeted sectors. Importance of policies such as Internet and e-mail is however once again among the highest (40%). Threats from inside as well as outside the organisation doesn't seem to be perceived as an issue of high importance (example remote access and access controls), which is alarming.

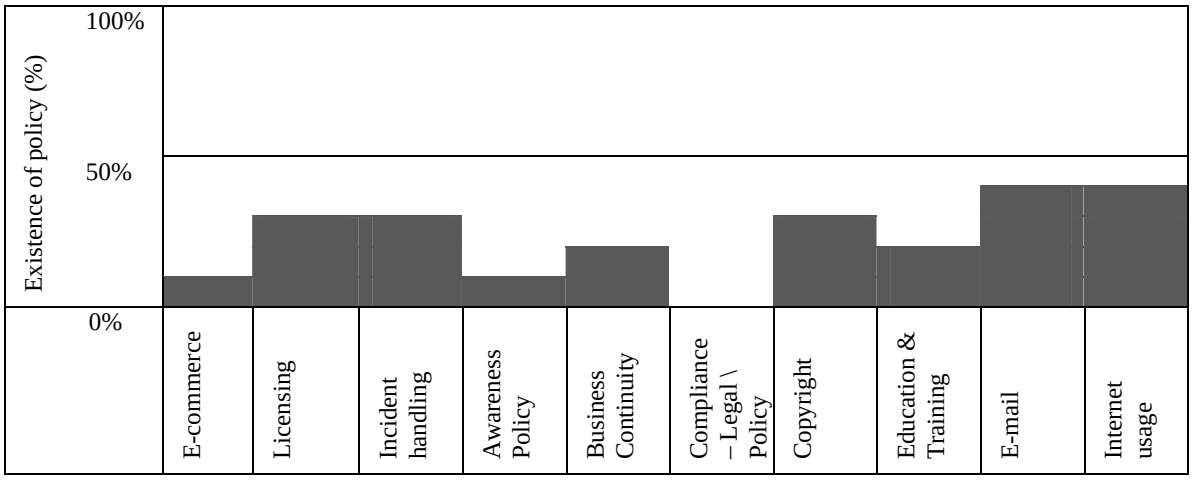

Figure 3: Perceived importance of policies

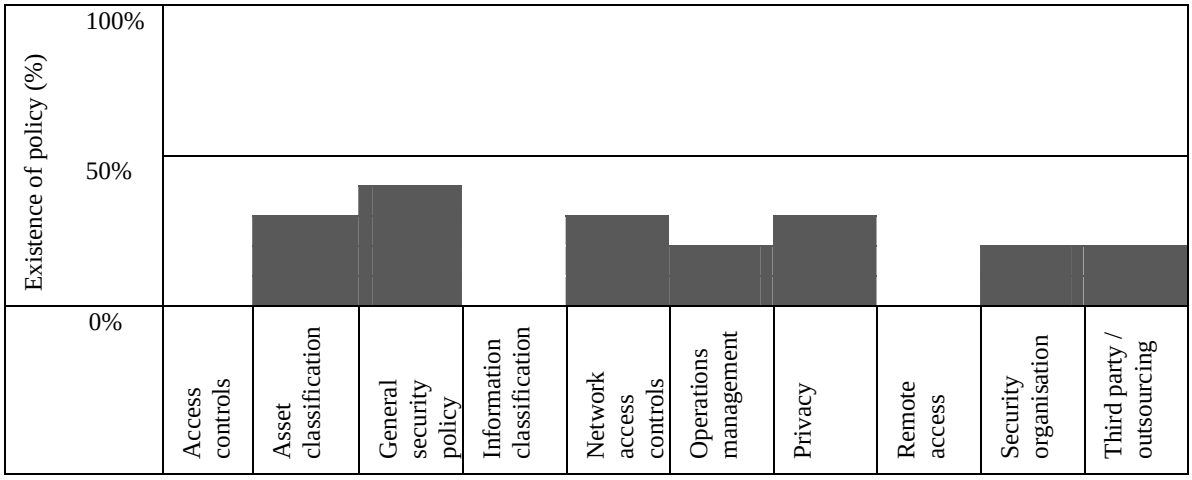

Figure 4: Perceived importance of policies continued.

4.4 Step 3: Format of policy

Figure 5 provide the information in terms of the assessment in regards to the format of the policy. The number of policies available for conducting a format assessment was quite low and has to be taken in consideration when interpreting the data represented in Figure 5.

The information contained within the different policies seems to be on a high standard (for example scope and objectives of policies are detailed extensively). Problems facing the industry are related to management not committed to the creation and implementation of a security policy, while incident handling does not exist (although risk management is covered to some extent). The non-existence of incident handling confirms the results in section 4.3 whereby the targeted organisations are not committed to handle issues such as possible threats within and outside of the company.

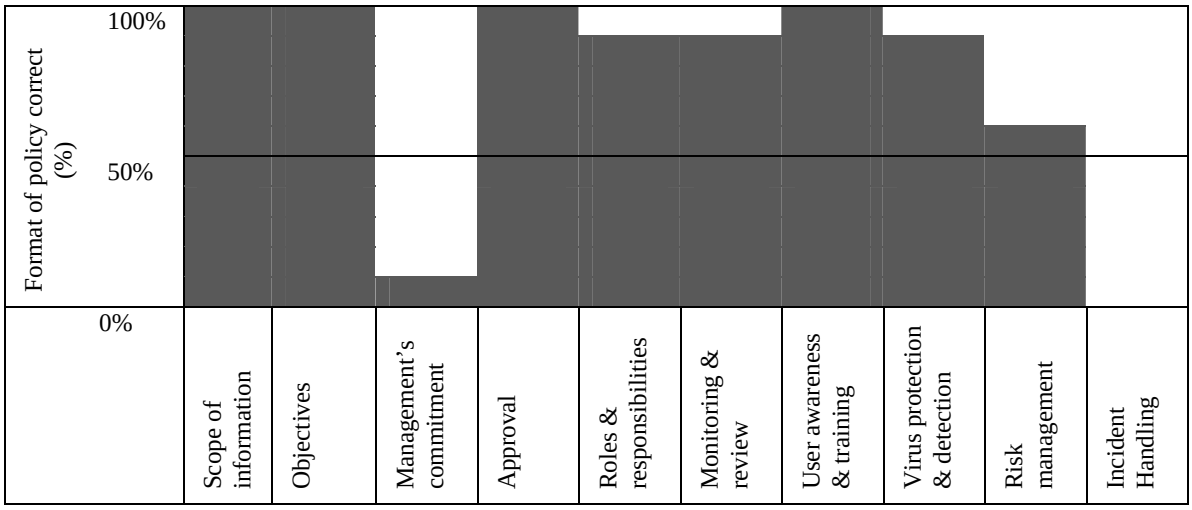

Figure 5: Format of policy

4.5 Step 4: Supporting documentation

In none of the responses were supporting documentation found. This can be due to some of the factors discussed in section 4.1, such as sensitivity of the documentation. A lack of such documentation seems however to be the main reason for absence.

5 CONCLUSION

Issues regarding computer security is increasing daily due to advances in technology as well as the global connection of people and resources. Organisations spent large amounts of money on securing their information in the quest to stay ahead. The first step in protecting an information system is the creation of an information security policy. Models and standards of information security policies are governed by organisations such as NIST and ISO, while industry and academia are playing a vital role in this domain.

We have conducted research on the status of such information security policies by targeting Government organisations in the Polokwane region. A number of concerns were raised during the study such as:

- People appointed in security managing positions seem to lack knowledge within the field.
- The number of security policy sets in existence is very low.
- Supporting documentation is non-existent.
- Management is not committed to the importance of the process.
- Government sectors are moving too slow in realising the importance of security policies.
- Dedicated computer security staff is scarce within the targeted organisations.
- Assessment by people from outside the organisation has a negative influence on the study. Internal research within the different government sectors may produce more detailed results.
- Computer security issues are regarded as a sensitive issue within organisations and requested information is difficult to obtain.

- The targeted organisations seem to implement policies on demands placed by staff members ineffectively using technologies such as Internet and e-mail.

Most of the managers interviewed during the study realised the shortcomings within their sections and departments and were quite willing with the necessary guidance to embark on a process of creating information security policies. They were also interested in building long-term relationships with researchers and academia in order to develop training and education possibilities.

Further research includes the expansion of the study to not only include organisations from the Government sector but also different types of industries.

6 REFERENCES

BISHOP, M. 2003. *Computer Security: Art and Science*. Boston: Addison Wesley. ISBN 0-201-44099-7.

CHOW K, M. & MUN, K.S. 2000, User awareness and adoption of security standards and technology. [Online]. Available from: http://www.itsc.org.sg/synthesis/2000/itsc-synthesis2000-mengchow-siewmun-it-security-stds.pdf

CONKLIN, W.A., WHITE, G.B., COTHREN, C., WILLIAMS, D. & DAVIS, R.L. 2004. *Principles of Computer Security: Security+ and beyond.* Illinois: McGrawHill Technology Education. ISBN 0-07-225509-9.

GROBLER, T. & VON SOLMS, S.H. 2004. Assessing the Policy Dimension. In: *Proceedings of the Fourth annual ISSA Information Security Conference, South Africa*.

LEINER, B.M., CERF, V.C., CLARK, D.V., KAHN, R.E., KLEINROCK, L., CYNCH, D.C., POSTEL, J., ROBBERTS, L.G. & WOLFF, S. 1998. *A brief history of the Internet.* [Online]. Available from http://www.isoc.org.

PFLEEGER, C.P. & PFLEEGER, S.L. 2003. *Security in Computing.* Third edition. New Jersey: Prentice Hall Professional Technical Reference. ISBN 0-13-035548-8.

SCHNEIER, B. 2000. Secrets and Lies: Digital security in a networked world. John Wiley & Sons Inc.

STEFANEK, G.L. 2002. Information Security Best Practices, 205 Basic Rules. Elsevier, USA,

VON SOLMS, H.S. & ELOFF, J.H. 2001. Information Security. First edition. Amabhuku publications (Pty) Ltd 2000/1/2, RAU, Republic Of South Africa.

WHITMAN, M.E. & MATTORD, H.J. 2004. Improving Information Security through Policy Implementation. In: *Proceedings of the 7th Annual Conference of the Southern Association for Information Systems.*

WHITMAN, M.E. & MATTORD, H.J. 2005. *Principles of Information Security.* Second Edition. Boston: Thomson Course Technology. ISBN 0-619-21625-5.