A GENERAL METHODOLOGY FOR THE DEVELOPMENT OF AN EFFECTIVE INFORMATION SECURITY POLICY

Arvish Ramdeyal [1,*] and Mariki M. Eloff [2,]**

[1] Btech: Information Technology student, UNISA

[2] Associate Professor, Department of Computer Science and Information Systems, UNISA.

- P.O.Box 7646, Cumberwood, 3235

Tel: 0832339202 email: a_Ramdeyal@yahoo.com

[**] PO Box 392, Unisa, Pretoria, 0003 South Africa.
Tel.: +27 12 429-6336. email: eloffmm@unisa.ac.za

ABSTRACT

In today's hi-tech world, conventional physical security methods are simply insufficient for the protection of an organisation's information assets. This is because of the ever-increasing dependency on the use of electronic data in everyday business process activities. Since it is an information security policy that forms the basis for a security program, the importance of developing an effective policy is quite significant. Another phenomenon that has brought about a need for proper Information security policies is the fact that Information Technology is constantly evolving. As a result, new and changing security threats have to be constantly counter-acted. The intended objective of this paper is to provide a concise and generic methodology for the development, implementation and maintenance of a strategic information security policy. It must be noted that this project deals solely with policy development and it is therefore not indented to replace official and/or commercial security manuals. Policy development is quite a complicated task and developers will have to consult a number of information sources to successfully achieve their goal. This methodology should be used as the "primary information source" and will provide more than adequate general guidance on the development process of an effective information security policy

KEY WORDS

Information security, information security policy, policy failure, information technology, threat, countermeasure, policy development, policy maintenance

A GENERAL METHODOLOGY FOR THE DEVELOPMENT OF AN EFFECTIVE INFORMATION SECURITY POLICY

1. INTRODUCTION

As information technology develops, so does the need for the implementation of an information security policy. There are two factors that have contributed to this need i.e. (1) the increasing dependency of organizations on electronic information, and (2) the development of the World Wide Web and the increasing use of e-commerce.

Dhillon, (2001:1) explains how changing structures and the greater reliance of companies on information pose a number of challenges for good management practices. The following example from Doswell (1998:17) gives a clear indication of the increasing dependency of companies on information. In Manchester, a small printing company was broken into and cleaned out. The loss of machinery had proven to be far less than the loss of data, which had cost them their entire customer list.

In their article Vermeulen and Von Solms (2002:119) explain how a change in the way computers were used made mere physical security methods ineffective. The change referred to above is that of the ever-increasing use of networks and the Internet in every day business process activities, commonly referred to as e-commerce. Mason (2003:13) explains how the emergence of the Internet and e-mail has changed the type of security that is needed. He also explains that risks are poorly understood by end-users and stresses the importance of an effective security policy. "What many people don't realize is that the Web, as it has evolved, has serious security issues" (Geer, Ranum & Rubin, 1997:1).

The remainder of the paper is structured as follows:Section 2 stresses the importance of an effective information security policy by highlighting some of the threats. The 3rd section discuses some reasons why policies fail. The fourth section proposes the general methodology, followed by a conclusion.

2. THE IMPORTANCE OF AN EFFECTIVE POLICY

"If a threat exists and your business is vulnerable to it then there is a risk. If there is a risk then there must be an executive decision on the use of a countermeasure." Doswell (1998:25) The primary focus of an information security policy is to deal with threats that a particular company is vulnerable to.

Below are some of the major external threats to information security that have emerged with the constantly increasing popularity of e-commerce:

- Hackers - A hacker can be defined as a person who accesses a system that he/she is not authorized to. Hackers do what they do to learn and normally do not intend harm. It is the criminal hacker, also known as a cracker, who has malicious interests and may expect financial gain.
- Viruses - A virus is a program that is secretly implanted on a computer. A virus is designed to replicate itself until the entire machine and even any device connected to that machine is contaminated.
- Trojans - A Trojan horse is a program that is implanted on a system. The program may seem to be performing some normal function but is actually performing some malicious task and may be compromising information security.

- Worms - A worm is a Trojan that has the ability to replicate. They are used to attack local area networks and e-mail clients.
- Denial of service - A Denial of service attack is normally aimed at disrupting network activity. The aim is to deny a user from using a particular service by using various methods to flood the network of a particular company.

The employees of a particular organization are the primary contributing factor to inside threats. Jamon (2002:4) supports the argument that protecting from the inside is more important than protecting from the outside. Employees, meaning users of the system, sometimes tend to take advantage of certain Internet privileges. The use of e-mail, chat rooms and downloading provides a point of attack for a hacker. Also, although predominantly unintentional, it is normally the employee who is responsible for most information leaks.

The above threats are real and can lead to disaster as a result of a breech of information security. Considering these threats and the fact that new emerging threats are a reality, it is clear that there exists a definite necessity for any organization to implement an effective and evolving information security policy. The importance of this has been demonstrated by recent reports of a hacker having accessed the ABSA system and defrauding ABSA clients of more than One Million Rand. Another example is the recent attack by means of a worm, on the Microsoft operating system. This worm has been reported to be the fastest ever replicating Trojan horse.

Besides dealing with threat, a well-developed information security policy has added benefits. An information security policy reflects the goals of an organization. It also states acceptable use regulations and defines who does what, and how it should be done in order to maintain information security. (Jamon, 2002:1) explains how security policies can be used as a foundation when conducting audits or when trying to discover what went wrong after a breech of security.

3. WHY INFORMATION SECURITY POLICIES FAIL

An ineffective policy can generally be attributed to one or more of the following issues:

- Lack of employee support

One of the major contributing factors to policy failure is the lack of employee support. This involves the support of both management and employees. Although policy development is a management process, the maintenance of an information security policy requires the support of all employees by adhering to the rules in a policy. Furthermore, if management does not show support for a proposed information security policy, it is highly unlikely that the staff would. Elmy-Liddiard (2002:1) describes the support of employees as being "absolute top priority" for implementing an effective security policy.

- Legal and economic complications

An information security policy must adhere to government laws and principles. Policy rules should be clearly defined to avoid legal implications if a breech of security occurs. If a company opts for an off-the-shelf information security policy template, financial implications must be carefully considered. For example, the operational version of the RUSecure information security policies cost $595. RUSecure is quite comprehensive and would satisfy all the information security policy needs of any company. But its cost (R5000, at the time of writing) would not be feasible to facilitate the policy requirements of a small organization.

Furthermore, it is essential for a company to determine how much money is required to maintain adequate security. "If there is a sound business case for security, then there is a sound business case in making it happen" (Doswell, 1998:22). It makes no sense to document security measures in policy whilst it is subsequently discovered that these measures will be too expensive to implement.

- Employee disciplinary issues

Employee disciplinary issues should be clearly stipulated in a security policy and made clear to all employees. If an internal breech of security occurs, the documented disciplinary actions must be strictly followed. If these rules are not strictly adhered to, employees will become lax in terms of upholding information security and an information security policy will become just another document.

- Inadequate policy application/maintenance

Because of the nature of an information security policy, it is not possible for all companies to apply guidelines with the same severity or degree of intensity. "There is no 'out of the box' security response (nor attendant policy) that truly fits all organizations" (Aalberts et al., 2001:10).

Maintenance and constant policy review is an essential component of an effective information security policy. Constantly evolving information technology and the threats that accompany it support the above statement A policy that is not maintained will simply become worthless.

- Policy does not reflect the goals of the company.

Aalberts, Townsend & Whitman (2001:10) explain that no policy will succeed if the eventual policy requirements hamper an employee's ability to effectively perform his job Thus, an effective information security policy must properly reflect the goals of the company in order to maintain effective information security. If this reflection is not present, there will be much uncertainty with regards to (a) what information should be protected, (b) who has access to this information and (c) the degree of security intensity.

4. GENERAL METHODOLOGY FOR THE DEVELOPMENT OF AN INFORMATION SECURITY POLICY

4.1 Motivation

To avoid the problems such as generality of guidelines and unnecessary policy development costs, the obvious solution is for a company to develop its own information security policy. There are also added advantages that materialize when a company adopts this route to policy development. In his article Elmy-Liddiard (2002:2) explains how developing your own information security policy enhances your knowledge of the inner workings of the company.

It is important for the developer to know what he is doing and why he is doing it. A properly developed information security policy can be extremely beneficial to any given organization. The authors have thus chosen to include detailed explanatory notes in the proposed guideline. The guideline is also designed to educate and warn the developer of possible pitfalls during policy development that could lead to failure.

The proposed solution of an information security policy guideline will follow a life-cycle process for the development of an information security policy. It consists of four phases i.e.

- Security Assessment,
- Policy Construction,
- Policy Implementation and
- Policy Maintenance.

To minimise poor maintenance issues, the Policy Maintenance phase is designed as a continuous process, which starts when the policy is implemented. Also included is a link from the maintenance phase to the security assessment phase. This enforces a set procedure that must be followed if any changes to the policy are to be made after its implementation. Furthermore,

Employee support is indicated as an ongoing process in the development and maintenance of an information security policy.

4.2 Overview of guidelines

In the quest for the development of an effective information security policy, a thorough consultation of several different information sources is required. The purpose of this methodology is to serve as the "principal source" and will provide more than adequate general guidance for the development, implementation and maintenance of an effective and evolving information security policy. The methodology is divided into five phases i.e. Employee Support, Security Assessment, Policy Construction and Policy Maintenance. Within these phases, specific procedures and methods will guide the development team to reach the desired target of implementing an effective policy. Also, explanatory notes will be provided to help the developer successfully negotiate problem areas in the policy development process.

Before commencement of the actual policy development process, there are a few issues that need to be clear in the minds of the developers.

- What is an information security policy?

An information security policy, which is developed by management, deals primarily with threats to information security. It specifies what procedures will be adopted by a particular company in terms of (1) the prevention of a threat occurring, and (2) the reaction to the occurrence of a threat. It also states the general rules and regulations pertaining to use of electronic media.

- Why do I need an information security policy?

It is an information security policy that forms the basis for a comprehensive security program and the importance of developing an effective policy is therefore quite significant. In addition, Information Technology is constantly evolving and brings with it new and changing threats that must be accounted for.

Assuming that the developer has been given the 'go ahead' to develop an information security policy, the first task to be performed is a thorough risk analysis investigation of your company.

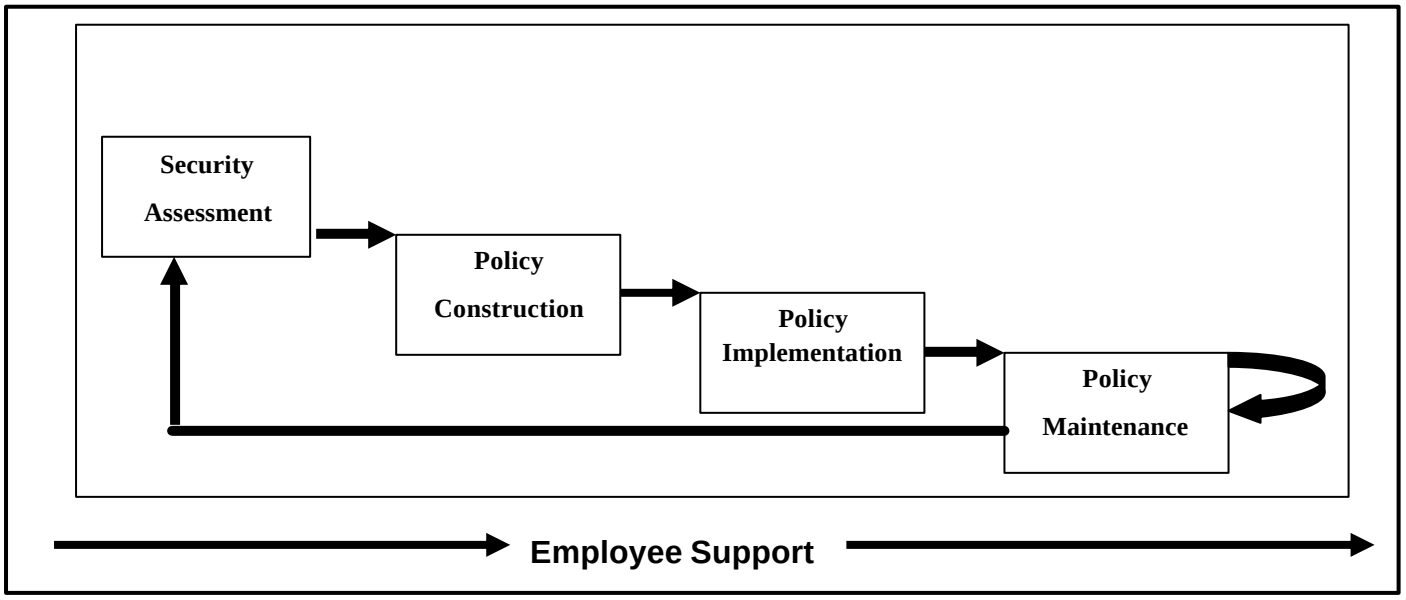

Figure 1: Information Security Policy Development Model

4.3. Security Assessment

The primary objective of this phase is to determine what threats your company's information is susceptible to. Once these threats are determined, the associated risk for each of these threats must be estimated. The risk of a threat occurring refers to the impact of this occurrence on the business. It would not be feasible to invest in a countermeasure for a threat that has a low risk factor.

4.3.1 Threat Identification

The developer should keep in mind that most threats attack one or more of the following aspects of information security.

- *Availability.* - Ensuring that defined services are always available to the authorized user.
- I*ntegrity* – ensuring that data is correct.
- *Confidentiality* – ensuring that unauthorized persons cannot access sensitive information
- Exclusivity - prohibiting a competitor from benefiting from any Information that may come into his possession

The types of threats that a particular company is susceptible to is obviously dependent on the type of company. It is also dependant on the way in which a company uses technology to perform its everyday business processes. For example a company could use stand-alone machines, a networked system or implement an e-commerce environment.

So before a risk assessment, it is imperative that the developer has a thorough understanding of how the current system works. Questions such as: What type of data is processed? What type of system is being used? Who can access the system? Who is responsible for what? Need to be answered.

Below is a table that contains (1) common information system threats, (2) the impact of these threats on a particular company, using a rating of 1 to 5.

Table 1: Example of Common Threats and Impact Rating

Threat	Impact
Hackers	3
Viruses	5
Software failure	5
Hardware failure	5
Denial of service	4
Internet Abuse	4
Employee trust	3

The above table is a simple example of determining which threats are of high risk to the company and need suitable countermeasures implemented. This process is however quite complex and requires a sound knowledge of risk analysis and management techniques.

4.3.2 Countermeasures

For information security purposes, there are various countermeasures that one could implement, but the choices are dependant on the threats identified. Some useful countermeasures include:

- Purchase and adopt suitable anti-virus

- Disaster recovery plans
- Password protection
- Data encryption
- Regular security audits
- Implementation of applicable laws and regulations
- Internet Use policies

When selecting countermeasures, economic implications must be considered. The objective of developing an information security policy will be lost if the developer underestimates the cost of countermeasures and later discovers that these cannot be implemented.

Ultimately, it is up to the development team to determine which threats the company is most vulnerable to, and in effect determine which threats require the implementation of a suitable countermeasure. Below is a checklist of processes that must be completed in the Security Assessment phase of this policy development methodology

Table 2: Security Assessment completion checklist

Process	**Completed**
Know the system	
Identify threats	
Estimate associated risk	
Document countermeasures for high risk threats	

Now that the threats that the company is vulnerable to are identified, and the countermeasures that have to be adopted, policy construction can commence.

4.4. Policy Construction

This phase deals with the development of the actual policy and focuses mainly on what a policy should contain. The information security policy document must be distributed to all employees or users of the system. Because of this, the diction used to describe technical procedures or laws should be adequately constructed to enable all users to properly understand the policy.

Below is a list of five broad topics that make up the general constituents of an information security policy. Also explored are the aspects that should be covered within each section. It is important to note that the policy should be developed in accordance with the goals the your company. You cannot institute rules, regulations and procedures that hinder an employee from effectively performing his job.

4.4.1. Overview and Policy Goals

The details of to whom, when and where your policy applies should be specified. Also, the general goals and intended outcomes of the policy document should be explained.

4.4.2. Description of the scope of the policy

This section should provide a detailed description of the scope of the policy. Aspects such as systems being used, system functionality, system architecture and hardware & software in use to be covered by the policy should be clearly defined.

4.4.3. Adopted Security Procedures

The purpose of this section is to stipulate (1) business vulnerabilities, (2) high impact threats that have been identified and (3) countermeasures that have been adopted. Issues such as backups and disaster recovery planning should also be discussed.

The intention of stipulating these issues in your policy should be to increase the security awareness of your employees. An information security policy document should be treated as highly sensitive information and, under no circumstances, should it be distributed to persons outside of your organization.

4.4.4. Employee Rules and Regulations

It should firstly be clearly defined who has access to the system. Also, authorization rights for specific employees must also be specified. Rules for the proper use of all electronic media must be clearly defined. If your employees have access to the Internet, regulations for Internet use must be specified. Also, in the case of an internal breech of security policy, disciplinary action should be clearly stated. Furthermore, the rules for distribution of your policy should be specified.

The employee rules and regulations must be carefully constructed. You must be able to implement rules while keeping the employee happy. Also, the severity of employee disciplinary actions need to be determined based on the type of offence committed. The disciplinary actions in the policy must be clearly documented and strictly followed. If not, employees will become lax in terms of upholding information security and the policy will become just another company document.

4.4.5. Management of Security

In this section, the way in which all employees (including management) should contribute towards the maintenance of information security must be explained. It must also be defined, who in the company, will be responsible for administering security.

The importance of security maintenance must be stressed. Employees must be made aware that, by adhering to the regulations in the policy, they are contributing to the maintenance of information security.

4.5. Policy Implementation

Before the policy is implemented and distributed to all employees, a thorough review of the policy must be conducted. This review should be aimed at trying to uncover any major loopholes in the policy. Ensure that the policy is clear, concise and consistent.

It is at this stage where the validity of the policy must be firmly established. The policy should adhere to government laws and principals to avoid legal implications. Also, if an employee who was dismissed decides to sue the company, a well-formed information security policy document will be the best aid in defence. The policy should also be checked for social and ethical implications.

4.6. Policy Maintenance

Technology, and the threats that come with it are constantly evolving. In order for a company to maintain a sufficient level of security, its information security policy should equally evolve. The adoption of constant review is a must.

This phase is probably the most significant with regards to the administration of an effective long-term information security policy. As depicted in the information security policy development model, the Maintenance phase is a continuous process and thus echoes continuous review.

Also, the maintenance phase is linked back to the Security Assessment phase. Hence, in the event of a required change to policy, the developers must follow a set procedure for the

implementation of these changes. This is to ensure that changes are instituted in the proper manner and will have no negative repercussions in terms of a poorly constructed policy.

Constant review refers to constantly checking and ensuring that any (1) changes in the company environment or (2) advances in technology, that impact on the security of information, are reflected and resolved in the information security policy. Maintenance is of extreme importance for the upkeep of an effective and long lasting policy. If a policy is not reviewed constantly, it will become insignificant.

4.7. Employee Support

All of the other phases in the policy development model are contained by the employee support phase. This is done to stress the importance of employee support. This involves the support of both management and employees. Although policy development is a management process, the maintenance of an information security policy requires the support of all employees by adhering to the rules in a policy

One of the major contributing factors to policy failure is the lack of employee support. It must be understood by all employees that information security is of vital significance for the purpose of running an effective and competitive business. Also, if management does not show support for a proposed information security policy, it is highly unlikely that the staff would. A lack of employee support will result in a worthless information security policy. This in effect leads to an extremely poor security program.

5. CONCLUSION

The development of an information security policy is more of a necessity than a requirement for an organization that depends on electronic information to run its everyday business processes. Policy development is a complicated process because of the many issues and implications that need to be considered and resolved. The authors propose a general methodology for the development of an effective information security policy. This proposed guideline is aimed at clarifying some of the development aspects. With the help of the proposed methodology in this guideline, many of the pitfalls in the policy development process can be alleviated. This guideline can "open the doors" to develop a solid and effective information security policy.

6. BIBLIOGRAPHY

Alberts, C.J., Allen, J.H. & Dorofee, A.J. 2001. OCTAVE Catalogue of practices. Version 2.

Aalberts, R.J., Townsend, A.M. & Whitman, M.E. 2001.Information systems security and the need for policy. Information Security Management: Global Challenges in the New Millennium. USA: Idea Group Publishing.

Dhillon, C. 2001.Challenges in managing information security in the new millennium. Information Security Management: Global Challenges in the New Millennium. USA: Idea Group Publishing.

Doswell, B. 1998. Managing Security – Achieving BS7799. Great Britain: Pitman Publishing.

Emly-Liddiard, M. 2002. Building and implementing an Information security policy. SANS Infosee Reading Room. URL: http://www.sans.org/rr/policy/building.php

Geer, D., Ranum, M.J. & Rubin, A.D. 1997. Web security sourcebook. A complete guide to web security. Threats and solutions. Canada: John Wiley& Sons, Inc.

Jamon, D. 2002. A preperation Guide to information security policies. SANS Infosee Reading Room. URL: http://www.sans.org/rr/policy/prep_guide.php

Mason, S. 2003. Electronic security is a continuous process. Computer Fraud and Security, (January), 13-16.

OECD Guidelines for the Security of Information Systems and Networks. Adopted as a recommendation of the OECD Council at its 1037 Session on 25 July 2002.

RUSecure - Information Security Policies. Evaluation Version 2.0. (2001). The evaluation copy was downloaded at: URL: http://www.information-security-policies.com/

SABS ISO/IEC 17799. 2000. Information technology – Code of practice for information security management. Edition 1.

Vermeulen, C. & Von Solms, R. 2002. The information security management toolbox-taking the pain out of security management. Information Management and Computer Security, 10(3) 119-125. URL:http://leporello.emeraldinsight.com/vl=1570653/cl=29/nw=1/fm=html/rpsv/cw/mcb/09685227/v10n3/s3/p119