FIVE NON-TECHNICAL PILLARS OF NETWORK INFORMATION SECURITY MANAGEMENT

Elmarie Kritzinger[1] and Prof S.H. von Solms[2]
[1]*School of Computing, University of South Africa, SA.*
[2]*Department of Computer Science, Rand Afrikaans University, SA.*

Abstract: Securing information is vital for the survival of many organizations. Therefore, information must be proactively secured against harmful attacks. This securing of information becomes more complex when such information is transmitted over networks. This paper identifies five non-technical pillars (essentials) for network security management. For each pillar a number of specific actions are specified, resulting in a check list for a high level evaluation of the security status of these 5 pillars in a networked environment.

Key words: Information security; network security; non-technical aspects; information security management.

1. INTRODUCTION

In an increasingly competitive world, the company with the best information on which to base management decisions is the most likely to win and prosper [4]. Organizations must understand that information is a very valuable resource and must be protected and managed accordingly. Security must be considered as an integral part of whole IT governance environment, and must be dealt with in a proactive manner in order to be effective.

This means that information security is fundamental to the survival of any organization which uses electronic information resources. Information security is a discipline which can be divided into technical and non-technical

aspects. This division is also reflected in the following definition of Information Security Governance [17]:

'Information Security Governance consists of the leadership, organizational structures, policies, procedures, compliance enforcement mechanisms and technologies needed to ensure that the confidentiality, integrity and availability of the organization's electronic information assets are maintained at all times.'

Aspects like the leadership, organizational structures, policies, procedures and some of the compliance enforcement mechanisms can be seen as the non-technical aspects, while the specific technologies (firewalls, encryption, access control lists etc) can be seen as the technical aspects. The authors do agree that some of these aspects overlap, and therefore fall into the grey area of being technical as well as non-technical. Nevertheless, the major aspects can be categorized as technical or non-technical.

Real Information Security Governance therefore consists of ensuring that both these technical as well as the non-technical aspects are implemented and coordinated in a holistic way. Figure 1 below indicates where Information Security Governance fits into the wider Corporate Governance structure.

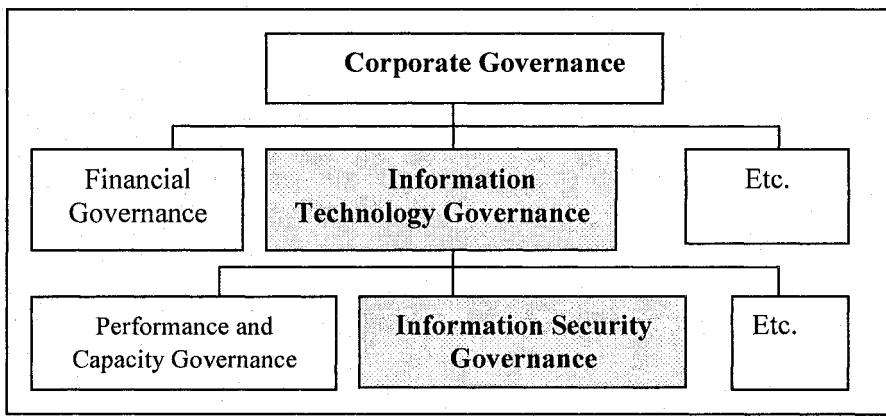

Figure 1. Corporate Governance Structure

Over the last 10 to 15 years, Information Technology in general has evolved from a centralized environment to a more decentralized environment, in which all types of networks (LANs, WANs, and Internet) are used daily to connect systems, work stations etc. to each other.

Managing the security of these networks, i.e. ensuring that the existence and use of all types of networks, do not impact on the confidentiality, integrity and availability of the organization's electronic assets, has become a pivotal part of more general information security governance. The more

recent security worries around wireless networks, emphasize the crucial importance of such network security management. Figure 2 below indicates where network security management fits into the Information Security Governance structure.

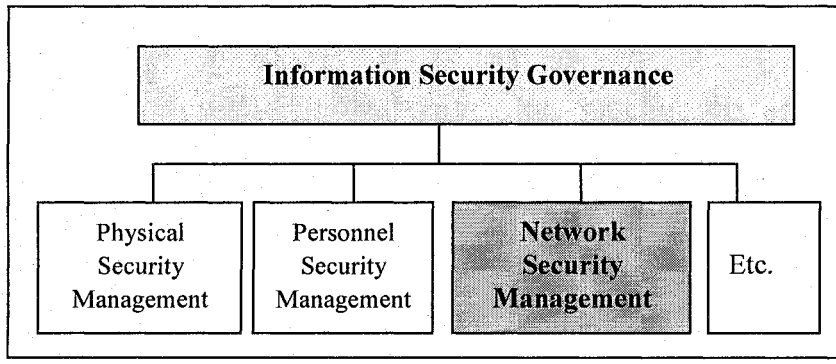

Figure 2. Network Security Management within the Information Security Governance structure

Because of the pivotal role of network security management, this paper zooms into this specific part of Information Security Governance, and defines 5 pillars (essentials) which must be in place to ensure proper network security management. These 5 pillars have to do with the more non-technical aspects of network security management, in line with the division made for Information Security Governance above.

Understanding the importance of these 5 pillars are vital to network security, as too often companies approach network security from a purely technical viewpoint, and do not realize that if the non-technical aspects (pillars) are not in place, huge risks will still exist as far as the use of their networks are concerned. Identifying and highlighting the importance of these 5 pillars are not necessarily a novel idea, as they are discussed and mentioned in most internationally accepted best practices for information and network security management. However, the purpose is to again stress their importance, and to provide a simple way for a network security manager to do a fast high level evaluation to determine the presence and level of implementation of these 5 pillars.

We start off by introducing and discussing each of these 5 (non-technical) pillars, and finish with a checklist that a network security manager can use to see whether the relevant 5 (non-technical) pillars are in place.

2. NETWORK SECURITY MANAGEMENT PILLARS

The five main pillars (building blocks) that the authors claim to be essential for network security management can be defined as:

- Having Top Management's commitment and buy-in for network security
- Having a proper Network Security Policy
- Having a proper Organizational structure for network security
- Having a proper User awareness program for network security
- Having a proper Compliance monitoring system for network security

Combined these five pillars will have a significant positive effect on implementing and maintaining a good network security management program.

Each of these five pillars will now be discussed briefly.

2.1 Having Top Management's commitment and buy-in for network security

In the last decade, boards of directors have experienced many new challenges and demands (such as rapid developments in technology and market conditions) [6]. The document referred to, goes on to state that information possessed by an organization is among its most valuable assets and is critical to its success. The board of directors, which is ultimately accountable for the organization's success, is therefore responsible for the protection of its information. The protection of this information can only be achieved through effective management and corporate governance.

According to Nicholas Durlacher [10], senior executives do not have to take responsibility for all the actions of their employees. However, organizations have the right to require senior executives to justify their conduct and competence formally in the event of any serious management failure that threatens the future of the firm. It is clear that senior managers in many large organizations are now expressing a much greater interest in Information Security than their counterparts of five to ten years ago.

Another author who has addressed the importance of senior management is Lewis [11]. Lewis states that the business should take responsibility for Information Security and appoint an officer whose key responsibility is the integrity of the organization's information. Given that the directors of the company are ultimately liable for business continuity, it is clear that the responsibility for Information Security cannot be removed from the boardroom.

This clearly shows that it is vital to involve top management in all Information Security management procedures and decisions within the

organization. The reason being, that they are ultimately responsible for the security of all information in the organization. Because of the increased risks in using networks, Top Management must specifically be aware of the increased risk exposure of the company by using such networks, based on the underlying risks of the Internet, remote dial-ins, wireless networks etc. Without such commitment and buy-in, proper corporate governance will be affected.

2.2 Having a proper Network Security Policy

A Corporate Information security policy may be defined as "compiled documentation of computer security decisions"[15]. These security decisions can be made with regard to hardware, software, networks and information. Such a Corporate Information Security policy must be a maximum of 2 to 3 pages, very generic, and non-technical, and must be signed by the most senior official in the company.

Because of the pivotal role of networks in most companies, and the increased risks arising from implementing and using such networks, a separate Network Security Policy, flowing from the Corporate Information Security policy, must exist. Such a policy must explain the reason why the company uses networks, the risks involved in using these networks, and the responsibilities of employees in limiting these risks whenever using such networks.

This can be a single policy document, but because of the growing importance and risks related to network usage, trying to cover all aspects related to network security in one document, results in a document which is too big and unwieldy. Increasingly companies are creating a set of policies related to network security, including:

- An Internet Usage Security Policy
- An Email Usage Security Policy
- An Encryption Policy
- A Wireless Network Security Policy
- A Malicious Software Security Policy
- Etc.

Such a Network Security Policy, or rather set of Network Security Policies, highlights the importance of security when using networks and makes it easier to enforce proper network security management.

2.3 Organization

According to the International Guidelines for Managing Risk of Information and Communications Statement #1 [8], one of the six major activities involved in Information Security is Roles and Responsibilities. This includes ensuring that individual roles, responsibilities and authority are clearly communicated and understood by all [7]. Therefore, all security responsibilities, roles and ownership must be defined and assigned to all the users in the organization who work with any information resource.

Again, because of the increased use of networks, a clear organizational structure, with a supporting set of roles and responsibilities must exist for network usage in all its forms. This structure must clearly indicate which organizational positions in the company can use which network services, for example, remote login from wired and wireless networks, home access, dial-in modems etc., and what their roles and responsibilities are.

2.4 Awareness

Information Security awareness is a widely publicized and talked-about issue in the business environment. The reason for this is that Information Security awareness is mainly a human-related issue. It is important to realize that "human issues" are the main cause of security breaches [11]. The most effective way to reduce Information Security risks in an organization is to make employees more Information Security aware. This awareness also means that employees must take responsibility for their own actions in the workplace.

Implementing an effective Information Security awareness programme helps all employees understand why they need to take Information Security seriously, what they will gain from its implementation and how it will assist them in completing their assigned tasks. An effective Information Security awareness programme could be the most cost-effective initiative a company can take to protect its critical information assets [16]. This protection can only be provided if there are effective programmes in place to make certain that employees are aware of their responsibilities.

It is the organization's responsibility to make employees aware of Information Security policies and issues in the organization. Without knowing the necessary security controls (and how to use them), users cannot be truly accountable for their actions [15]. Organizations that have implemented strong protection mechanisms and have educated their staff are in the best position to protect their information from unauthorized disclosure or modification.

According to the CCTA [2], the Information Security procedures must be integrated into normal everyday routine, and staff should come to recognize security as an enabler rather than a barrier. The NIST handbook [15] also stresses this "every day routine" by stating that Information Security is an ongoing process. This process of making employees Information Security aware must continue after a candidate has been hired, which includes keeping employees up to date with their IS duties and responsibilities.

Any general Information Security awareness program must, of course, include all aspects related to network usage security, which must not be hidden amongst a lot of other security issues. Again, because of the importance of networks, many companies are realizing that a network security awareness program, separate from the general Information Security awareness program, has significant value. This is enforce by Lewis [14] that states if one can make employees aware of the threats to the network and let them feel part of the network security team they may feel more inclined to help out and point out potential problems before they get out of hand. Greater success is achieved in this way, because employees are specifically exposed to the security risks related to the use of networks, and can therefore evaluate network security as an aspect in its own right.

2.5 Compliance Monitor (CM)

Compliance monitoring (measuring) is about finding out if procedures and processes that should be implemented in an organization are working as they should, and are being complied with. The objects that are monitored can differ from organization to organization; and include products, systems, processes, security program effectiveness and personal competence [9].

Network security in itself can be compromised if there are no mechanisms in place, apart from some annual audits, to ensure that it is enforced and complied with on a continuous basis. GMITS [5] states that Information Security compliance checking (which includes network security) has to occur on an annual basis. A setback with annual audits is that Information Security problems are only identified annually and the organization is open to security attacks daily. In today's business environment, organizations cannot afford to find out, 6 to 12 months later, that an employee has resigned from the organization but still has access to some of the servers. These problems can be avoided by continuously monitoring the network security in the organization.

A comprehensive compliance monitoring environment, to ensure compliance to the policies and procedures mentioned in 2.2 above, is therefore essential. Although many of these compliance measuring and

monitoring mechanisms will be technical, the results must be used to check compliance to policies, and to update aspects like the awareness programs. Therefore this pillar is handled as one of the non-technical pillars, as discussed in section 1.

The compliance measuring and monitoring must not only produce technical low level results for operational purposes, but must also be able to produce high level reports which can be used to inform top management, in an easily understandable way, about the risks related to the use of networks in the company.

Such compliance monitoring is essential, because 'you can only manage something if you can measure it'. This specifically holds true for computer networks.

3. THE '5 PILLARED' APPROACH

3.1 Network security management Processes

In the first part of this paper the 5 pillars for network security management were briefly introduced. Each of these pillars can be summarized into a few high level actions that will enforce the role of that pillar.

This section will use an incremental approach to illustrate how these actions can be used to implement (or evaluate the presence of) these pillars in a network security management environment.

Each of these pillars contains one ore more actions that is vital to that pillar. If there is compliance with an action one can move on to the next action. If compliance with one action within a pillar is not complied with, a counter action must be taken (indicated as a "No" in Figure 3). After a counter action is completed, the process starts again at the first action in the specified pillar (or block). If all the actions are complied with within the pillar, one can progress to the next pillar (block).

The order in which the pillars will be addressed is the same order as introduced in section 2. The order of the pillars is very important to follow, for example one cannot monitor a policy or procedures if such a policy or procedure does not exist in the first place. Therefore, the pillars must be kept in the correct order. The action and counter actions for each pillar can be depicted in Figure 3.

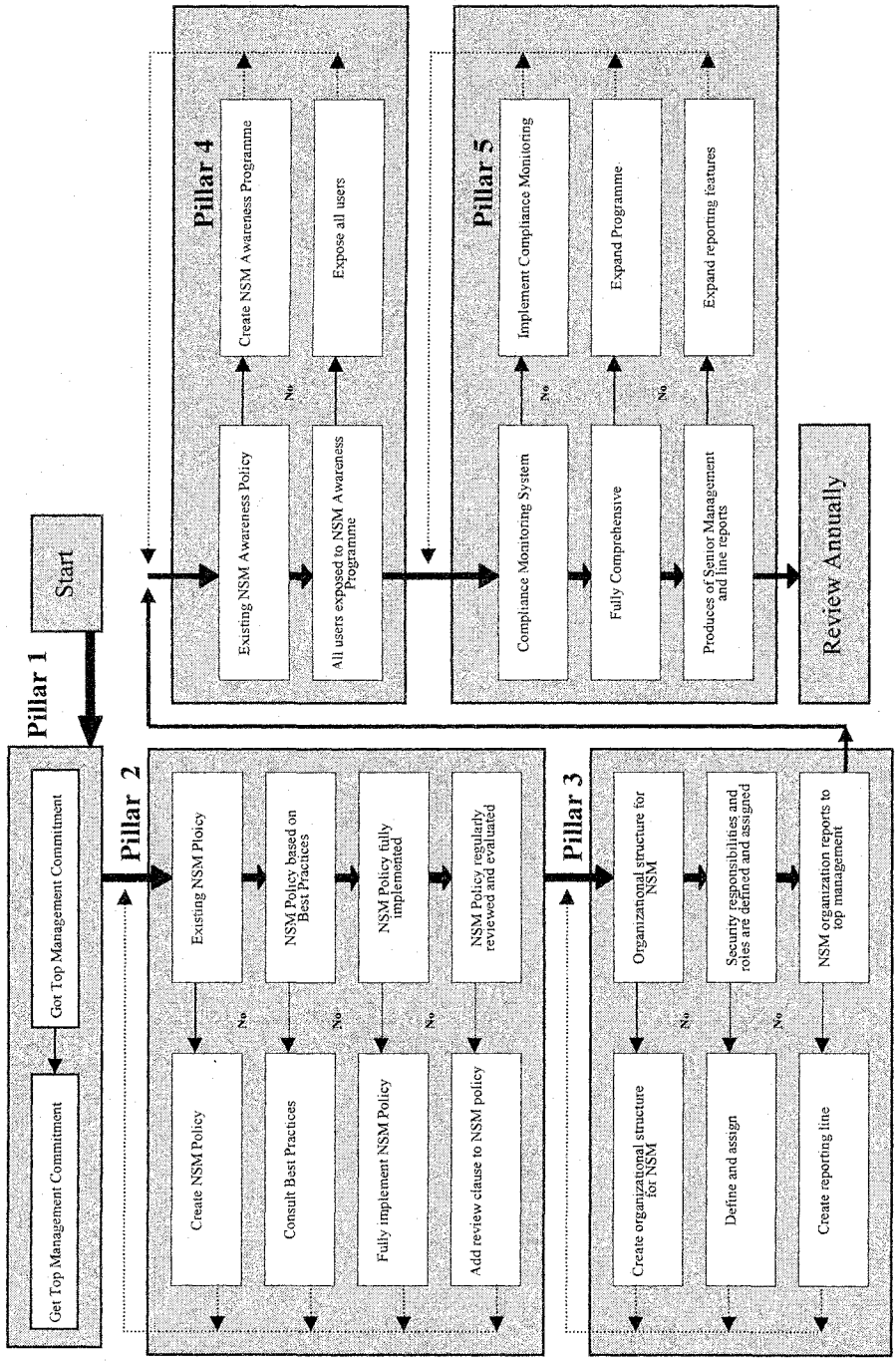

Figure 3. Network security Management (NSM) processes

3.2 Checklist

This section uses the actions and pillars depicted in Figure 3 to create a checklist for network security management. This checklist comprises each of the 13 decision questions from figure 3, and indicates the network security management approach for non-technical network aspects. Before starting to work through the checklist it is important to know that technical aspects such as firewalls protect an organization for outside attacks but leave the organization open to attacks from inside the organization. Insider threats are most often incidental in nature due to the fact that many employees do not know that they are compromising the confidentially, integrity or availability of information. With this check list in place an organization can try to minimize the "incidental" threats by employees.

4. CONCLUSION

This paper introduced the importance of the non-technical aspects of network security management. Five vital pillars were identified and briefly described. Different actions for each of these pillars were also identified. These five pillars, together with the individual actions can be depicted in a checklist with a preset order that must be followed. The importance of this checklist is to ensure that organizations are aware of the different non-technical aspects related to network security management and how to implement and monitor these in an organization.

5. REFERENCES

[1] CCH Enterprises Solutions 2000: *"Security is a management issue, not a technology issue."* Online: www.cch.za/es/news/articles/news59

[2] CCTA - Championing Electronic Government, 1999: Online: http://www.ccta.gov.uk/index.htm

[3] Department of trade and industry, 2000: *"Information Security Management Policy."* Online: http://www.dti.gov.uk

[4] Finne T., 2000: *"Information systems risk Management: Key concepts and business processes."* Computer & Security, 19 (3) 2000.

[5] Guidelines for Management of IT Security – GMITS, 2000 Online: http://www.cancert.ca/Pages/ISStandards.htm

[6] IIA, AICPA 2000: *"A call to action for corporate governance."*Online: http://www.nitc.state.ne.us/tp/workgroups/security.htm

[7] "Information Security Governance: Guide for Boards of Directors and Executive Management." IT Governance Institute

[8] International Federation of Accountants, 1998: *"Managing Security of Information."*

[9] Katzke S., 2001 : *"Security Metrics."*

Online: http://www.acsac.org/measurement/position-papers

[10]Kwok L. & Longley D., 1999: *"Information Security Management and Modeling."* Information Management & Computer Security. Vol 7, 1999.

[11]Lewis A., 2002: "Time to elevate IT security to the boardroom" E-Secure, Volume 1, Issue 1.

[14]Lewis R. 2003: *"The need for Establishing a Security Awareness Training Program."* As part of GIAC practial respository. SANS Institute

[15]National Institute of Standards and Technology 2000: *"An Introduction to Computer Security."* Online available: www.nist.gov

[16]Netigy 2001: *"Information security awareness program."* Online: http://www.netigy.com/solutions/security/sec_foundation/infosec_aware.htm Author unknown.

[17]Von Solms S.H., 2000: *"Information Security - The third wave?"* Computer and Security, Volume 19, Issue 7.