INFORMATION SECURITY HEALTH CHECK

Raising information security awareness by diagnosing an organization's current security situation, considering the importance of their specific security concerns

PETRUNEL GERBER, petrunel@xsinet.co.za;

MARIANA GERBER, mariana@petech.ac.za
Port Elizabeth Technikon

Key words: information security, management, security concerns, preparedness, easy to use, effective tool

Abstract: Organization's dependency on information systems and the related resources has led to an increased vulnerability to computer crime and abuse. It is therefore of the utmost importance that senior management are aware of the importance of information security because they are ultimately accountable for the organization's success. Unfortunately, no effective, easy to use tool is available to diagnose an organization's current information security situation. This paper will therefore aim to propose the "Information Security Health Check" as an effective, easy to use tool to get senior management's commitment and to determine the current status of information security, considering the importance of their specific security concerns.

1. Introduction

Information security can be defined as the process of protecting information from a wide range of threats in order to ensure business continuity, minimize business damage and maximise return on investments and business opportunities by preserving confidentiality, integrity and availability of information (British Standards Institution, 1999, p.1). Information security management could therefore be very vital in maintaining an organization's profitability, competitive edge, cash flow, legal compliance and respected organization (British Standards Institution, 1999, p.1). It is therefore clear that information security is a business responsibility shared by all members of the management team (British Standards Institution, 1999, p.4). However, it is very important that an enterprise must realize that they can spend millions on technology, but if their users/employees are not information security aware, their technology will not protect them (von Solms, 2001). Therefore information security requires a whole-hearted organizational commitment of resources (financial, human, and technological) to an enterprise-wide program designed to evolve and adapt to new dangers (Power, 2002, p.3).

In order to whole-heartedly commit an organization to information security, an organization needs to be able to analyse their current security situation to see whether they are adequately protected or not. Unfortunately, no effective and easy to use tool is available to firstly diagnose an organisation's current security situation and secondly draw management's attention to the situation.

The primary objective of this paper will be to develop an "Information Security Health Check" that will serve as an easy to use and effective tool in the information security management process. By developing such a tool, the secondary objectives would be met, namely to:

- Raise senior management's information security awareness
- Determine an organization's preparedness for security

In order to justify the need for the Information Security Health Check (ISHC), this paper will firstly study the importance of senior management's awareness and commitment to information security as well as the importance of an organization's preparedness for security as a whole. The current situation of senior management's awareness and commitment as well as the organization's preparedness for security will be determined by studying various security statistics. Secondly, this paper will look at risk analysis as a possible solution, motivate why risk analysis does not meet the objectives of this paper and finally propose the Information Security Health Check (ISHC) as the best possible solution with the following functionality:

- Determining senior management's information security awareness and commitment
- Determining requirements for security concerns
- Determining an organization's current preparedness for security
- Graphically reporting the current protection against required protection, considering the importance of their specific security concerns.

2. Why information security is needed

In this section the need for senior management's commitment and the need for organizations to be prepared for security will be addressed. This section with its subsections, will aim to convince the reader by means of various statistics that information security's need is still understated today because most organizations' senior management are not whole-heartedly committed to information security and most organizations are not prepared enough for information security.

2.1 Senior management's commitment to information security

This subsection will firstly look at the need for senior management's commitment to information security and secondly depict the situation today by looking at some statistics.

An organization's information is among its most valuable assets and is critical to its success and therefore information security is a direct corporate governance responsibility and lies squarely on the shoulders of the Board of the company (von Solms, SH, 2001). Furthermore, organizations must adhere to legal and regulatory requirements like the Financial Services Act (Gramm-Leach-Bliley Act of 1999, 2002), and the Data Protection Act in the U.K. (Information Commisioner, 2002) the Promotion of Access to Information Act and the Promotion of Administrative Justice Act in South Africa (South Africa Government Online, 2002).

Professor Basie von Solms stated that information security is a multidimensional discipline and also added that the following dimensions must be taken into consideration:

- External commands like clients and suppliers could require an organization to ensure that all their information security bases are covered in order to ensure security of the business link
- Insurance companies may use information security certification as a basis on which to base premiums
- The existence of a proper organizational structure, a Corporate Information Security Policy and information security awareness among users, allows management to create an ordered and disciplined environment within their company
- Information security certification is gaining ground all over the world and can increase customer confidence and trust
- The technical as well as the non-technical aspects of information security must be managed, measured and monitored effectively in order to be successful

- The good reputation of a company leads to its acceptability in society, which in turn leads to success (Von Solms, 2001, p.504-508).

Although the importance of senior management's commitment to information security is clear, it seems like the message has been lost somewhere along the line. Various statistics show the real picture in contrast with the above-mentioned.

According to the 2001 Information Security Industry Survey, budget constraints and a lack of end user awareness continued to top the list of obstacles to adequate security. While lack of management support was third in the ranking, many would cite it as the source or cause of most other obstacles to security (Briney, 2001, p.46).

The 2002 CSI/FBI Computer Security Survey reported that most organizations still have only one information security professional for every thousand users and most organizations do not spend more than 1-3% or 3-5% of their total IT budget on security (Power, 2002, p.17).

The real picture reflects that most organization's senior managements are not whole-heartedly committed to information security.

2.2 Organizations' preparedness for security

This subsection will firstly look at some of the needs for an organization's preparedness for security as stated by the British Standards Institution where after the current situation will be depicted by means of quoting statistic resources.

- Increasingly, organizations, their information systems and networks are faced with security threats while attacks have become more common, more ambitious and increasingly sophisticated (British Standards Institution, 1999, p.2).

The findings of the 2002 CSI/FBI Computer Crime and Security Survey once again confirmed this by showing that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting (Power, 2002, p.1). According to the CERT/CC the number of reported incidents drastically increased with 21,756 documented in 2000 to 52,658 reported in 2002 (Security Stats.com, 2002).

- Organizations have become increasingly dependent on information systems and services and this means that organizations are even more vulnerable to security threats (British Standards Institution, 1999, p.1).

This is confirmed by the 2002 CSI/FBI Computer Crime and Security Survey which stated that the types of incidents reported as well as the trends that the seven-year life of the survey confirm, have the potential to do serious damage to U.S. economic competitiveness (Power, 2002, p.2). According to the CERT/CC computer security vulnerabilities more than doubled in the previous year, with 1,090 separate holes reported in 2000, and 2,437 reported in 2001 (Security Stats.com, 2002).

- The effectiveness of central, specialist control has weakened because of the interconnecting of public and private networks as well as the sharing of information resources (British Standards Institution, 1999, p.2).

The 2001 Information Security Industry Survey stated that ubiquitous connectivity, complex systems and networks, the push for point-and-click commerce and the proliferation of easy-to abuse attack tools have created an environment of ever-increasing risk (Briney, 2001, p.35).

- Many information systems have not been designed to be secure and it is important to remember that the security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures (British Standards Institution, 1999, p.1).

American Hospital Association (AHA) estimated that implementing information technology and management solutions to ensure **minimum** compliance with the Health Insurance Portability and Accountability Act (HIPPA) regulations, could cost hospitals up to US $22.5 billion, over the next 5 years (Security Stats.com, 2002).

In November 2001, Software and Information Industry Alliance (SIIA) and KPMG LLP reported that of 1004 business people they surveyed, more than half of the business users said they are unaware of corporate policies governing intellectual property that maybe in place (Power, 2002, p.17).

The real picture reflects that most organizations are still ill prepared for information security. From these statistics one can conclude that senior management is not committed to information security and that most organizations are still ill prepared for information security.

3. An effective, easy to use Tool?

The primary objective of this section is to propose an effective and easy to use tool to firstly raise senior management awareness and secondly to determine an organization's current preparedness for security.

3.1 Risk Analysis

This section will take a closer look at risk analysis and why it does not meet the objectives of this paper.

Risk analysis is a well-known planning tool to determine the exposures and their potential harm (Pfleeger, 1997, p.462). This tool is an orderly process adapted from practices in management that improves awareness, identify assets, vulnerabilities and controls, improve basis for decisions, and justify expenditures for security (Pfleeger, 1997, p.463). To see whether or not risk analysis meets the primary objective of this paper, a few critical resources have been consulted.

According to Pfleeger the results of risk analysis are no more precise than the figures used in the analysis, which are often mere guesses (Pfleeger, 1997, p.471). Pfleefer also noted that risk analysis is immutable because it has the tendency to be filed and promptly forgotten and that it should be updated annually (Pfleeger, 1997, p.470).

Jacobson described risk analysis as a tedious process because there are many decisions to make and lots of data to collect. He further described risk analysis as pain full because each risk analysis starts from scratch again and it is difficult for risk analysis to focus on support of management (Jacobson, 1996, p.1-2).

Although risk analysis definitely has its place in information security management, it does not meet the primary objective of this paper. It is not an easy to use and effective tool to determine an organization's current security situation.

3.2 Information Security Health Check (ISHC)

This section will aim to propose the ISHC as an effective and easy to use tool to raise senior management's awareness and to determine an organization's preparedness for security. The ISHC model will be briefly explained as well as the reason why the ISHC is so effective in solving the identified problem.

The first process (see Figure 1) is the actual gathering of information, which will provide the ISHC with the necessary data that is needed to accurately assess the security within the organization. This data will provide various information about the current security requirements as well as the current protection of information within the organization.

The ISHC firstly determines senior management's commitment by asking various questions to determine current management commitment and graphically report the current commitment against the ideal level of commitment. Thereafter, the ISHC determines the organization's preparedness for security by asking various carefully drafted questions to:

- Determine the required preparedness of an organization for security relating to the importance of the three security concerns, namely confidentiality, integrity and availability.
- Determine the current preparedness for security, considering the indicated importance of the security concerns.

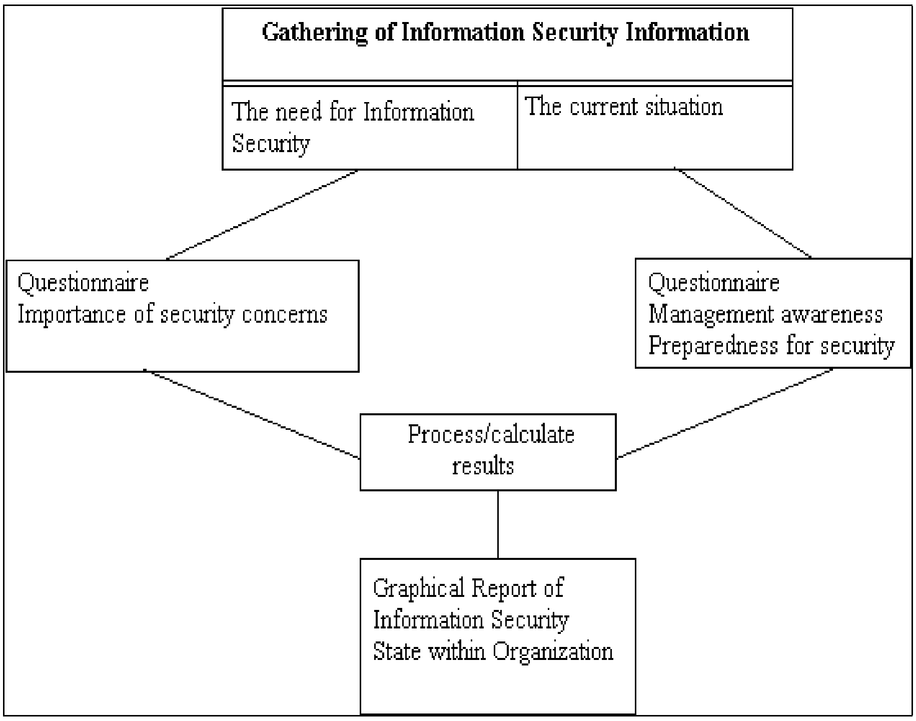
Gathering of Information Security Information
The need for Information Security
The current situation
Questionnaire
Importance of security concerns
Questionnaire
Management awareness
Preparedness for security
Process/calculate results
Graphical Report of Information Security State within Organization

Figure 1. The Information Security Health Check Model

With the above information, the ISHC can graphically compare and present the difference between the security preparedness that the organization requires and what they are currently prepared for.

These results can then be displayed on the final report (as seen in Figure 2), which will highlight the shortcomings, if any, of the current information security preparedness.

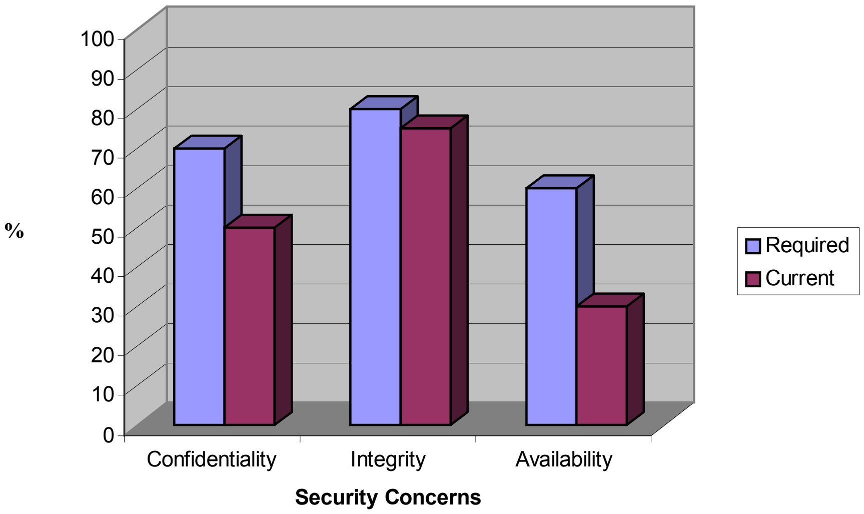

Figure 2. Security Preparedness

Table 1 consists of a lookup graph that displays the current security situation within the organization. By plotting the values of the security requirements and the current security situation, the ISHC determines whether the organization has:

1. Adequate protection
2. Acceptable protection
3. A security situation which needs further attention
4. A critical security situation

Armed with this information an organization can re-evaluate their current information security program.

Table 1. Lookup Graph

Current Security (%)	81-100	1	1	1	2	2
	61-80	1	1	2	2	3
	41-60	1	2	2	3	3
	21-40	2	2	3	3	4
	0-20	2	3	3	4	4
Required Security		0-20	21-40	41-60	61-80	81-100

It can therefore be seen that the drafting of the questions is very important for the ISHC to be effective and to be a true reflection of the organization's information security situation. The ISHC can therefore easily and effectively report the difference between the organization's security requirements and the organization's current security protection.

4. Conclusion

As can be seen from various statistics provided in this paper, most senior managements of organizations are not whole-heartedly committed to information security and furthermore that most organizations are ill prepared for information security. In order to whole-heartedly commit an organization to information security, an organization needs to be able to analyse their current security situation to see whether they are adequately protected or not.

The ISHC proofs to be an effective and easy to use tool to fulfil the above needs. It proves to be an effective tool in persuading senior management of their responsibility towards information security as well as effectively reporting the current preparedness of their organization. The ISHC can be used by any person in the organization with the necessary knowledge of the business operations and does not require a huge amount of technical skills or expertise, as might be the case with doing a thorough risk analysis. Thus, it can be concluded that the ISHC is an extremely beneficial tool for senior management by proving to be an invaluable exercise in the quest for secure information systems within the organization.

References

Briney, A. (October 2001). Information Security Magazine.
2001 Industry Survey, p. 34-47, [cited online: March 20, 2002]
(http://www.infosecuritymag.com/articles/october01/images/survey.pdf)

British Standards Institution. (1992).
Information Security Management – Part 1:Code of Practice for Information Security Management & Part 2: Specification for Information Security Management Systems. BS7799: 1999. London

Information Commissioner, [cited online: March 20, 2002]
(http://www.dataprotection.gov.uk/)

Jacobson, RV (1996). CORA. Cost-of-Risk Analysis.
Painless Risk Management for Small systems,
International Security Technology, Inc.

Pfleeger, CP (1997). *Security in Computing,* Prentice Hall, US.

Power, R (2002). *CSI/FBI Computer Crime and Security Survey,*
Computer Security Issues & Trends, Vol VIII, No.1, Spring 2002.

Security Stats.com – Your portal to statistical security data,
Most Requested Statistics, [cited online: May 20, 2002]
(http://www.securitystats.com)

South Africa Government Online, [cited online: March 20, 2002]
(http://www.gov.za/gazette/acts/2000/a2-00.pdf;
http://www.gov.za/gazette/acts/2000/a3-00.pdf)

Rapalus, P (April 2002). Computer Security Institute.
Cyber crime bleeds U.S. corporations, survey shows: financial losses from attacks climb for third year in a row,
[cited online: April 15, 2002]
(http://www.gocsi.com/press/20020407.html)

U.S. Senate Committee on Banking, Housing, and urban affairs
Gramm-Leach-Bliley Act of 1999, [cited online: March 20, 2002]
(http://www.senate.gov/`banking/conf/)

Von Solms, SH, *Corporate Governance and Information Security,* Computers & Security, Vol 20, No.3, 2001.

Von Solms, Basie, *Information Security – A Multidimensional Discipline*, Computers & Security, Vol 20, No. 6, 2001.