THE ROLE OF SECURITY POLICY IN PROTECTING INFORMATION ASSETS

J. P. Senzige

Abstract: In the wake of integrated and interconnected information systems and increasing threats, protecting information assets are of paramount importance. The ISO 17799 standard stipulates ten domains of information systems security controls. Among these controls is the information systems security policy. This paper looks at the need for protecting information assets, the role of information security policy and outlines qualities of an effective information systems security policy.

INTRODUCTION

More and more businesses are increasingly becoming dependent on information systems for storage and retrieval of pertinent information about customers and business transactions. On the other hand, security breaches are also on the increase and therefore affecting availability, confidentiality and integrity of information systems (Senzige, 2003). Security breaches compromise protocols, services, permission settings, readable network data, downloadable components and e-mail messages (Mark Walla *et. al*, 2000). In the wake of these breaches, protection of information assets becomes of paramount importance if businesses are to retain the market segment that they already have and attract yet more customers. The objective of security of information systems policy is the protection of the interests of those relying on information systems from harm, resulting from failures of availability, confidentiality, integrity, efficiency and compliance (Clayton, 2001). Of particular importance in this regard is the existence of a written security policy. Policies and procedures in network security are integral to how the network will operate as well as how the people using it should function (Woodard, 2000). This paper starts by looking at the need for protecting information assets, the role played by security policy and ends by delineating salient features of a good security policy.

* Senior Lecturer and Head CTT Dept, Institute of Finance Management, Dar es Salaam, Tanzania.

THE NEED FOR PROTECTING INFORMATION ASSETS

The need for protecting information assets arises from imminent and emerging threats. So, a vital component of a proactive security posture is an analysis and understanding of the threats facing an organization. While each organization is unique, any organization, in its day to day operations, is likely to encounter a limited subset of threat agents responsible for nearly all successful and attempted intrusions of the organization's infrastructure (Devost, 2002). These threat agents include insiders, industrial espionage, organized crime and structured and unstructured hackers.

Although recent survey results seem to indicate that insider threat is diminishing (Devost, 2002), the insider threat remains one of the most prescient in today's information technology environment. It still accounts for about 75% to 80% (Woodard, 2000) of the security threat agents and in fact 85% to 97% of them go undetected (Patrick, 2001). It is more likely that "the insider threat is being missed out as organizations devote additional attention to monitoring their external environment and insiders become adept at hiding their activity" (Devost, 2002). In addition to discontented employee element of the insider threat, there is an increasing concern regarding the use of insider placement as a penetration tactic. Organized threat agents, unable to penetrate external security mechanisms will seek to place individuals

within the organization as temporary workers, employees or even as system administrators (Devost, 2002). In an era of distributed computing, additional vetting of subcontractors and support personnel and monitoring of internal network resources is required to counter this continuing threat.

The second category of threat agents is industrial espionage and organized crime. This is a threat agent coming from business competitors and state sponsored intelligence organizations. While industrial espionage is a continuing threat, it is one that many companies are familiar with and most attacks impact confidentiality and not the availability of the information (Devost, 2002). The sensitivity of business information will drive the safeguards required to protect its confidentiality and integrity. Similarly, organized crime attacks are likely to exploit information for financial gain or to obtain access to sensitive information that is useful in the conduct of a criminal act.

Hackers constitute another threat to information assets. A recent study concluded that a vulnerable system connected to a public network would be compromised within 24 to 72 hours (Devost, 2002). The most common threat – the hacker attack - should be the easiest to counter and so, by ensuring that an organization follows industry best practices for information security, it will be protecting itself from a majority of the attacks from this community.

Another threat to information assets is viruses and worms. A virus is a piece of malicious code that cannot live on its own; it has to attach itself to a program, a file or a disk (Mazuhelli, 2001). It will propagate itself to other programs, files or disks, but only after a manual operation from the unsuspecting victim. This operation can take multiple forms, but it's often the opening of a file attached to an e-mail message. A worm will also propagate itself, but it can do it with no human intervention as it exploits a vulnerability of the attacked system, for example, a buffer overflow vulnerability, (Mazuhelli, 2001). A worm doesn't need to attach to something else; it is self-contained

The environmental threats include fire, flood, earthquakes, excessive heat, humidity, electrical storms and dust. Flood, fire and earthquakes may result into not only the disruption of services but also into loss of hardware, software and personnel (Senzige, 2003). Excessive heat and humidity may affect the hardware parts of the information system.

INFORMATION ASSETS

But what exactly is an information asset? Is it the software, hardware or the databases? According to Kadam (2002) information assets fall in four categories. Every piece of information about the organization falls in this category. This information has been collected, classified, organized and stored in various forms such as databases (information about customers, personnel, production, sales, marketing, finances etc). This information is critical for the business. It's confidentiality, integrity and availability is of utmost importance. Under this category there are also data files (transactional data giving up to date information about each event), operational and support procedures (these have been developed over the years and provide detailed instructions on how to perform various activities), archived information (old information that may be required to be maintained by law or future use) and continuity plans and fallback arrangements (these would be developed to overcome any disaster and maintain the continuity of business). Absence of these will lead to *ad-hoc* decisions in crisis.

Software Assets

Under software assets there are two subcategories. The first is application software. Application

software implements business rules of the organization. Creation of application software is a time consuming task. Integrity of application software is very important. Any flaw in the application software could impact the business adversely.

The second subcategory is system software. An organization would invest in various packaged software programs like operating systems, data base management systems, development tools and utilities, office productivity suites etc. Most of the software under this category would be available off the shelf, unless the software is obsolete or non-standard.

Physical Assets

These are the visible and tangible equipment and could comprise of computer equipment (mainframe computers, servers, desktops and notebook computers), communication equipment (modems, routers, hubs, EPABXs, and fax machines), storage media (magnetic tapes, disks, CDs and DATs), technical equipment (power supplies, air conditioners), furniture and fixtures.

Services

These include computing services that the organization has outsourced, communication services like voice and data communication, value-added services, wide area networks etc., and environmental conditioning services like heating, lighting, air conditioning and power.

The task of identifying assets that need protection is a less appealing aspect of the information security. But as Kadam (2002) puts it, "unless we know these assets, their locations and value, how are we going to decide the amount of time, effort or money that we should spend on securing these assets?" While all these assets need to be protected from disgruntled employees, industrial espionage, hackers, theft and environmental disasters, the value and sensitivity of the assets determine the level of required protection. Every effort to secure an information system starts with policy decisions (Senzige, 2003); so determining level and type of protection required for each type of asset cannot be achieved without a comprehensive security policy.

ROLE PLAYED BY INFORMATION SECURITY POLICY

A security policy has been defined as a formal statement of rules, by which people that are given access to an organization's technology and information assets must abide (Frazer, 1997). The primary objective of any security policy is to maintain the confidentiality, integrity and availability of all corporate assets (Roese, 2001). It embraces all three of these objectives in order to address potential threats to the enterprise. Information systems security policies are necessary to provide a framework for selecting and implementing countermeasures against perceived security threats. Schneier (2000) argues that "an information system security without security policies is likely to be a disjoint collection of countermeasures that address a variety of threats." Having a detailed and enforceable security policy mitigates risky exposure. Security policies address information assets or critical systems that need protection against security threats (Senzige, 2003; Daniel Lee, 2001), but as majority of security threats and attacks (Woodard, 2000 and Roese, 2001) come from internal sources there is a need "for company personnel to have a code by which to abide while performing their daily tasks via the network" (Woodard, 2000). The main charter of a policies and procedures document is to provide a typical user a set of guidelines for performing their daily tasks while connected to the network (Woodard, 2000). An enforceable written security policy helps ensure that everyone in the organization

coherently behaves in an acceptable manner with respect to information security (Daniel Lee, 2001).

Information systems security policies are designed to inform members of an organization of their obligatory responsibilities for protecting the information systems of their organization (Daniel Lee, 2001). When security is breached, the whole organization goes into crisis, and managers have to make difficult decisions fast. Security policy " helps to have procedures in place that will guide diagnosis of the problem, guard against knee-jerk decisions, and specify who should be involved in problem solving activities" (Austin et al, 2003).

Salient Features of an Effective Information Systems Security Policy

Developing a good information systems security is a five-step activity involving: (a) identifying what we are trying to protect (b); determining what we are trying to protect it from (c); determining how likely the threats are (d); implementing measures which protect our assets in a cost-effective manner and; (e) reviewing the process continuously and making improvements each time a weakness is found. In other words the development of information systems security should be preceded by asset classification, identifying threats pertaining to each asset, determining the probability of occurrence of the threats and, identifying the available technology that can be used in protecting the assets and the associated cost. However, the whole process must have management's commitment as "without their support... for the information systems security effort, their employees are less likely to support the effort" (Daniel Lee, 2001). Management commitment to security is essential to motivate information resource owners and users and to provide visibility needed by the information systems security team to ensure support of the business units. Senior management has to recognize that the integrity of the enterprise depends on their commitment to information security and sets the example for the organization (Artner, 2000).

Either the information systems security team or the Information Technology policies and standards group under the direction of the information systems security team should be responsible for drafting appropriate policies and updates. The idea here is to have a person or a group of people who are responsible for ensuring that information systems security policy is in place. It is generally not a good idea to assign policy-writing task to third-party consultants or use shelfware since the style and form should be consistent with existing policies and should reflect the corporate culture (Crume, 2000; Desilets, 2001). It is important that the team drafting information systems security policy is sufficiently familiar with both current technologies and corporate culture to link them in coming up intelligent decisions (Daniel Lee, 2001).

Information systems security policies should be flexible and permit exceptions when appropriate. When policies are written at a sufficiently high level of abstraction, they do not need to be changed when the Information Technology department and organization change. Organizational changes such as mergers, acquisitions, reengineering or the adoption of an industry standard should occur with a little or no need to modify the policies. In short an effective security policy needs to have some significant forward-looking policy directives, which will ensure a foolproof security planning. It needs to be a formal document, which clearly delineates areas of responsibility amongst the staff. It needs to provide for appropriate training of employees to make sure that the system remains foolproof and optimally tuned. Further, it needs to be constantly tested, upgraded and reviewed so that it stays in line with the changing environmental dynamics" (Brian Pereira, 2001)

CONCLUSION

Information assets need to be protected against imminent and emerging threats because any damage to such assets means not only financial loss to the company, but also have legal implications to the company and loss of good will. Information systems security policies primarily address threats. In the absence of threats, policies would be unnecessary -one could do as one chooses with information. Unfortunately, threats do exist and information systems security policies are necessary to provide a framework for selecting and implementing countermeasures against them. To be effective an information systems security policy must be based on thorough understanding of business strategies, identified information assets sensitivity with clearly assigned responsibilities, have management support, be forward-looking and constantly tested, upgraded and reviewed so that it stays in line with the changing environmental dynamics.

REFERENCES

Artner, B., (2000). "Does Your Company Culture Value Corporate Security?" TechRepublic 2000 www.techrepublic.com article.jtml?src=search&id=r00520001009ggp05.htm

Austin, R.D and Darby, C.A.R., (2003). "Computer Security is for Managers, Too." Harvard Business School

Brian, P., (2001)."Enterprise Security: Chinks in the Armor." *Network Magazine*, India Express Group, 2001 http://www.networkmagazineindia.com/200112/cover1.htm

Craig, C and David, C (2001). "Three-Tier Security in an E-Commerce Environment." A White Paper, Microsoft TechNet

Crume, J., (2000). *Inside Internet Security: What Hackers Don't Want You to Know.* Pearson Education Limited,

Daniel, L. R., (2001). *Developing Effective Information Systems Security Policies.* SANS Institute, September 10, 2001

Desilets, G., (2001). "Shelfware: How to Avoid Writing Security Policy and Documentation That Doesn't Work." SANS Institute, 2001 *www.sans.org/onfosecFAQ/policy/shelware.htm*

Devost, M.G., (2002). "Current and Emerging Threats to Information Technology Systems and Critical Infrastructure." Business Briefing: Global Security Systems

Kadam, A., (2002). "Identifying and Classifying Assets," www.networkmagazineindia.com

Mark, W and Robert, W., (2000). *The Ultimate Windows 2000 System Administrator's Guide.* Addison Wesley

Mazuhelli, M., (2001). "A Virus and a Worm: Lessons From SirCam and Code Red in a University Environment". SANS Institute August 15 2001

Patrick W.F., (2001). "Creating an Information Systems Security Policy." SANS Institute October 29 2001

Roese, J.J., (2001). "Security for Today's Enterprise." *Newmediary (2001)*

Schneier, B., (2000). *Secrets and Lies: Digital Security in a Networked World.* Wiley Computer Publishing 2000

Senzige, J.P., (2003). Information Systems Security: Whose Responsibility? *African Journal of Finance and Management Vol. 12(1)*

Woodard, E., (2000). *Network Security: Policies and Procedures,* Technical Enterprises Inc. November.