

Protection of Information Assets

Abstract

Information asset protection is an aspect of business management process that helps to protect the organizational information. This is why it information asset protection highly valued by organizations when it comes to security measures that will consistently eliminate or reduce the potential threat to data files, hardware, and, of course, the application files (Boran, 1999). These threats can be minimized or eliminated to an acceptable level either logically or physically or with a combination of both, depending on the company's security arrangements (Cliff, 2001). It is important to note that both logical and physical protection mechanisms are both important. It is, therefore, upon the organization in question to ensure that all the physical and logical aspects of information security are in place as per its security guideline policy. This paper discusses some of the information assets and security issues, as well as the way they can be managed to enable an organization to keep its information assets safe.

Introduction

Information asset protection is a very critical aspect of business management process for the successful operations and continuity of any business. Any form of threat to the security of the electronic or computerized information and its process is a definite threat to the quality of the end result (Boran, 1999). However, the threats can be eliminated or at least minimized to an acceptable level either logically or physically or with the combination of both, depending on the company's security arrangements (Cliff, 2001). Physical protection of information entails physical limitation of access to the information resource places (computers) by putting a limitation to such areas like the building, and specific rooms that have these

equipments. However, as has been observed, protecting the places or areas physically is never sufficient enough to provide maximum confidentiality of the information, which is why it is important to put logical and adequate information protection system in the place that would ensure maximum security control of information and, thus, enforce confidentiality of the sensitive company data. It is, therefore, upon the systems administration team to ensure that all the physical and logical aspects of information security are in place according to the minimum standard required by the company.

The first and the foremost requirement for adequate logical and physical information protection is for the company to identify, in order of priority, the most important information that needs protection (Cliff, 2001). The identification can be carried out by critical analysis of possible threats and impacts the latter are likely to have on the running of the information system. Subsequent calculation of different risks will ensure that all security issues are noted and prioritized (Granger, 2002). However, according to Gallegos (2005), it is important to take note of some critical security issues that the system management teams have to keep in mind when dealing with information protection, namely:

- One should just keep the data system simple, especially if the issue seems complicated, since complicated scenarios are not likely to have a serious effect and are very expensive.
- It is important to set minimum coherent security management system with a complicated system that does not rely on external factors much, since the dependence on the outer factors may make the system lose privacy.
- Use some of the tested methods of protection for easy evaluation (Gallegos, 2005, p. 41).

Physical Access and Threat

Any business that relies on computers to store information is prone to all types of physical threats, and that protection of information in computers takes more than just password and installation of antivirus software as some people believe. An intruder can get access to any computer or computer system and cause physical damage to its functionality by altering or replacing a computer part, plant some damaging programs like Trojan horse, or change the settings of the machine and get specific security numbers that may be detrimental to the general security of the information system (Granger, 2002). Granger advises that some very critical links for communications such as switches (routers) are supposed to be protected at all costs. It is thus logical to reason that physical protection is the first and most critical aspect of protection that every company should observe. Physical location, layout, design, and setting up of the facility would determine the level of access and ease of monitoring (Granger, 2002).

Other than attacks from intruders and hackers, and errors from the employees themselves, physical threat to information system has revolved around other concerns such as natural disasters e.g. water, fire, electricity failures, and many other environmental mishaps. Many information security experts believe that most of the information security risks like fraud, sabotage, and theft are as a result of internal arrangements by the companies' own employees (Micki & Harold, 1997). However, according to the survey conducted by the SearchSecurity.com (2002), many problems are accidentally caused by human error or just mistakes from unauthorized users in most cases. The survey carried out in 2001 indicated that many respondents gave human error as the most probable security risk challenge,

and it is even more disturbing that those questioned ranked human factors as the most difficult aspect of information security to enforce. As the report says,

Some sees the typical computer criminal a non-technical authorized user of the system who has been around long enough to locate the control deficiencies and use them to cut corners, or it may be a plain accidental errors or people not affiliated to the company or intruders trying to exploit deficiencies in the security system to commit harm against the business. (SearchSecurity.com, 2002)

The situation may be complicated when the company physically restricts their employees to such locations. So, how can a company reinforce such a policy without jeopardizing the general operations of the company?

Natural disasters, as it was mentioned earlier, are another physical threat to the information security. As illustrated by ISACA (2001), fire, electricity, lightning, water, earthquake, and other environmental disasters are some of the common natural disasters that pose a challenge to the information security management. Fire, depending on its intensity, can cause different level of damages to the system or even to the whole building. Water, mists, gases, and smoke can be disastrous to the operations of the computer systems (ISACA, 2001). Electric faults can result from frequent power interruptions that may interfere with general operations of the business and at worse cause fire leading to unexpectedly big catastrophe, according to ISACA (2001).

Control of Physical Access

Physical protection of information involves the physical restrictions to the access of the resources to prevent accidental or intentional damages to the computer systems, storage devices, microcomputers, computer terminals, and other communication equipments (Singleton, 2006, p. 6). The first step to take here is to asses the conditions of the present security structure of the company. Such operation will include the following elements: the entire building, office doors, desks

and cabinets; computer and telecommunication rooms; the way the company controls the access to information and whether it is secure; the way the information access is monitored by the company; and, finally, the way the general information protection is carried out (Singleton, 2008, p. 16). The process depicted above is supposed to give guidance and the basic understanding of the general information security in the company that will offer an overall benchmark for any improvement proposed (Singleton, 2008, p. 19). The evaluation will demand the analysis of possible risks and threats against the cost of mitigation and control, as Singleton (2008, p. 21) assures.

Classification of Access Controls

Experts have classified physical access controls as preventive and detective controls (Singleton, 2008, p. 24). The preventive control generally helps to avoid events that are unwanted, while detective controls are meant to identify unwanted events after they have occurred (United States General Accounting Office, 2002). Some of the commonly used physical security control systems include: manual doors/ cipher key-locks, magnetic door locks with electronic keycards, biometric authentication, security guards, photo ID's, Entry logs perimeter fences, computer terminal locks among many other methods (Micki & Harold, 1997, p. 43). On the other hand, detective security controls trigger the following: smoke and fire detectors, motion detectors, visual and electronic surveillance systems, intrusion alarms erected at the perimeter fence (Micki & Harold, 1997, p. 45). So, which way to go, preventive or detective access control? Well, just to begin with, Micki & Harold (1997, p. 51) explains the difference between the two methods in terms of their functionality. The scientists claim that the detective method, being "invisible" never affects the everyday working life of the employees. The effect only comes to action

when there is a security breach and the need for investigation emerges, for example, the response of the alarm, which by any means indicates that there is already a problem (Micki & Harold, 1997, p. 66). On the other hand, preventive control (for example, door locks and security guards) limits the employees' space, that is, restricts their movements to some particular areas and the type of information they are supposed to use (Micki & Harold, 1997, p. 68). It is, therefore, imperative to suggest that preventive controls are more effective than detective controls, since, in the first place, they prevent the problem from occurring. However, it may be a very challenging process if the employees fail to cooperate with the security team. Experts, therefore, advise that all employees should be given enough information about such arrangements to enhance understanding among the team, according to what Gallegos (2005) says. However, it would be more efficient if both methods are comprised to enhance both detective and preventive measures, since they tend to complement each other (Gallegos, 2005). When controlling accesses to restricted zones, areas defined as sensitive (like computer labs) should be monitored to ensure that only a limited number of people can get access to the area with authorization from the designated people. National Institute of Standards and Technology (1995) proposes the following methods of controlling access to restricted zones:

- Using electronic access controls, combination of mechanical locksets, or deadbolts;
- Restricting the number of points for entry as required by the safety regulations;
- Monitoring through personnel e.g. receptionist or guard situated at the entry points to ensure only approved persons allowed in especially during

working hours and all the entries should be video-recorded for references in case of security breach.

In addition, it is necessary to make a list of specific people who are authorized to access such sensitive information areas that house IT-assets. The need to trust the data to a certain group of people is backed by the recording all the detailed information of the visits of such areas like time and date of entry, reason for entry, and exit time (Micki & Harold, 1997, p. 31).

Backup Information

In any information storage system, it is important to create a backup for the information stored, which is supposed to act as an “insurance compensation” in case of any loss of the primary information (Micki & Harold, 1997, p. 44). Losing information about the business venture can sometimes be a frustrating experience that can disorganize all the company operations. The backup media is, therefore, stored in rooms or safes, at a reasonable distance away from the origin of the primary information to avoid losing all the data because of the same calamity. As Granger (2002) marked it, “backups of sensitive information should have the same level of protection as the active files of same information.”

Maintenance of Workplace

To prevent any unauthorized person from accessing any sensitive information about the organization, every employee should leave his or her desk clean and organized (Royal Canadian Mounted Police, 1997). All IT equipment that handles confidential information should be positioned so that no one could have access to the information other than the authorized people. The preventive measures include positioning of the monitor, fax, and printers in a secure place so that no unauthorized person could get access to them (Micki & Harold, 1997, p. 98). A practical method of

preventing any potential overview of the information on the monitor screen is to put the screen away from the window or away from the vicinity of the visitors, and the printers meant for confidential information should be placed in restricted zones, as Micki & Harold (1997, p. 99) explain.

Contingency Plan

IT experts advise that businesses should have contingency plans just in case of some extraordinary events (ISACA, 2001). The plan should be able to cover all the eventualities like power failures or surge, information theft, flood, fire, etc. The contingency document plan should provide essential services in case of losses (Singleton, 2006, p. 9). It should also take care of both on-site and off-site recovery process like the recovery of information due to system failure, and critical support system loss (Singleton, 2006, p. 11).

Controlling Access Location

Whatis.com (2002) proposes a number of preventive measures that should be taken to ensure proper safety of the information, offering their own idea about the location of such facilities. Some threats like flood can be minimized by proper selection of a facility location that would not be prone to flood, e.g. near the rivers that flood annually. The area should also be free from fire threats, mist or high humidity, or electromagnetic interference that may be detrimental to the efficient operations of the information system (Granger, 2002).

Control of Logical Access and Exposure

The control of logical access and exposure is the most commonly recognized information access control that involves a combination of computer hardware and software to restrict or detect access by unauthorized people, as Micki & Harold (1997, p. 83) mark. For example, most of the specific areas or sites will require the

user to have some personal identification numbers, or passwords that will allow access to the areas. IT professionals emphasize that logical controls should be designed in a way that would limit the authorized user to a particular system, programs and files that the user may need and absolutely deny others who may be hackers trying to access the system (Singleton, 2006, p. 67).

Well-used, logical security controls would be able to support the company in an effort to protect information assets even if individuals get access to the computer hardware. The software security strategy, thus, helps businesses to:

- Identify or recognize specific individual users, particular computers authorized to get access to computer networks, and other resources;
- Limit or restrict the specific data or information access;
- Easily produce as well as analyze the trails of user activities and audit the system (United States General Accounting Office, 2002);
- Take defensive actions against the intruders, and require more information to prove the legality of the access. For example, the employees who may not have authority to access specific information may try to access the information without the express authority of the person in charge. With accurate and well planned logical control system, they cannot gain access to such information (Granger, 2002).

Some of the commonly used logical controls are: antivirus software, access control software, passwords, encryption, smart cards, dial-up access control and callback systems, audit trails, and intrusion detection programs, as Royal Canadian Mounted Police (1997) explains.

Access Control Programs

There are a number of proven and tested methods to detect unauthorized access to information assets in a computer system namely:

Access control software. This software is installed purposefully to offer protection to the information resources considered important and confidential by the company (Cliff, 2001, p. 94). The ability to control and monitor the access to the computer system information that the software offers is vital for the company's information safety (Cliff, 2001, p. 109). The software limits the access by making sure that only particular registered members, or users, have the express access to the computer information or some very specific data, requiring them to insert their unique user ID accompanied by a password. A good example is the Computer Associates eTrust CA-ACF2 Security for mainframes (Cliff, 2001, p. 114).

Another important aspect of the problem in question is a password. A password is a set of computer encrypted characters that is protected and meant to authenticate the person accessing the computer system. It is normally a second identification method after the user has entered the username or ID, according to the information provided by Singleton (2008, p. 48). As ISACA (2001) says, "password is the first line of defense against outside attacks." However, weak passwords are easy to break especially by a password breaker tools such as L0phtCrack. Strong password will, therefore, make it difficult for such tools work, or it may make the process long and boring for the intruder. Depending on the access control system, password guideline sets up criteria differs. However, there are some general minimum criteria for setting up a secure password as illustrated by the NIST (2001); a fairly secure password should have the length of between 5-8 characters, be able to accept a combination of numerical numbers, alpha, both lower and upper case,

and, most important, some special characters that are not identifiable with the user details like date of birth or name. It is worth mentioning that the system must not allow passwords previously used and changed after 5-10 generations to be reused; in addition, it is necessary to periodically change the passwords (between 60-90 days), since that will assure the security of the data, they should never be displayed when entered, immediate replacement after implementation is necessary if it is a vendor-supplied one, and finally it is advised that all passwords should be personal and should never be shared at all levels if the information it safeguards is very vital. It is thus important to establish a proper password policy that would guide the usage.

Antivirus software must be mentioned as well among the issues concerning information assets protection. Viruses have proved to be one of the most frustrating disruptions to the computer network information safety. According to ISACA (2001), viruses are code segments that have the ability to replicate, acting remotely and sometimes proving difficult for some of the known antivirus. Viruses are malicious programs that are able to bring down the whole system or completely damage the existing user files. Once replicated, they attach themselves to the existing executables. Moreover, a new copy of the virus is executed when a user executes the new host program (United States General Accounting Office, 2002). The primary sources are downloaded from the Internet, via downloaded files and local computer networks. There are numerous types of viruses that have caused havoc to the business operations in the past years (NIST, 2001); the ones like W32.SirCam caused a considerable damage to companies' files and information. The most effective and proven way to control the virus in the computer system is to install antivirus software (NIST, 2001). Antivirus is able to detect, prevent attacks from the virus, and sometimes remove or repair the infected files. Some of the known

antiviruses are AVG, Kaspersky, NOD32, and NVC among many available ones (NIST, 2001). Other than antivirus installation, a company should be in position to establish clear and relevant antivirus policy that guides its usage. To be effective, the policy should make a part of a contingency plan, guide the usage procedure outlining when, how and by whom it should be used (NIST, 2001).

A smart card, which is also an essential element of data protection, is an intelligent chipped device, size of credit card that is used to authenticate the user (Granger, 2002). It requires the user to illustrate that he or she is the real owner of the card by requiring entry of some unique personal identity codes (Granger, 2002). One enters his or her PIN once the card is inserted into the system to allow access. It is a sure way of authenticating the identity of the user as it requires the person to own the card and at the same time have and remember the PIN (Granger, 2002). Smart cards have been used at the doors of sensitive computer/data rooms, and IT experts' project that smart card use will definitely increase in the future considering the expected increase in technological advancement (Granger, 2002). Probably this is why the PC/SC Workgroup companies like Microsoft, Intel, and Toshiba have defined certain standards for the interface between programming and PC hardware in a smart card (PC/SC Workgroup, 2002).

Encryption is a technique used to protect texts through the use of codes to hide the data for any other reader other than the informed. It is commonly used to protect data on transit or stored data from any intrusion or interception by unintended person (Boran, 1999). However, encrypted data is still prone to loss so the encryption programs can easily be compromised (Boran, 1999). It is, therefore, advisable to use it as a part of the security details for a company, which must be accompanied by other more reliable information asset security efforts.

Dial-Up Access Control and Callback Systems

In some cases the users of computer system may attempt to remotely connect to the computer systems from home or any other location other than the business enterprise via a dial-up line. It is advisable to restrict such uses through a dial-up access control. This method prevents any attempt by such people to get access to the secured information (Singleton, 2006, p. 18). It's also able to authenticate the remote user other than affecting a call-back system. When in action, the link for telecommunication lines that are established by a dial back into a computer remotely is interrupted so that "the computer would dial back to the caller" (Boran, 1999). The security catch here is that the caller can only be permitted if the number is valid and recognized. Boran (1999) advises that phone numbers should be regularly changed to ensure maximum safety, and warns that if the company's business is not adequately secured by dial-up access controls, the information stored are vulnerably exposed to war dialers, e.g. Toneloc, that can sweep the company's extensions, with an intention to get access to an open modem to answer the call (Singleton, 2006, p. 22).

The other useful information security tool is the audit trail. It is used to trace back any illegal input of information from some other source to the original user (Boran, 1999). Any improper attempt by an employee, for example, accessing restricted information database, is automatically reported back to the original source. The strategy of audit trails is useful in areas where specific employees are allowed some specific areas access but not all the database (Boran, 1999). If they attempt to access the unauthorized data, it can be reported back to the central location.

Conclusion

It has turned out that there are numerous risks that information assets can be exposed to, both natural and man-made. It is, therefore, upon the organization to have a proper analysis of the potential risks and take precautions to avoid any disastrous loss of data or information. It is important to manage and maintain both logical and physical security in an equal measure to adequately protect the organization's information. The actual challenge for any organization would be to get the right security, both physical and logical, in place that would correctly fit the particular organization's needs.

References

- Boran, S. (1999). *The IT security cookbook*. Retrieved from <http://secinf.net/info/misc/boran/>
- Cliff, A. (2001). *IDS terminology, part two: H-Z*. Retrieved July 18, 2009 from <http://online.securityfocus.com/infocus/1214>
- Granger, S. (2002). *The simplest security: A guide to better password practices*. Retrieved from <http://online.securityfocus.com/infocus/1537>
- Gallegos, F. (2005). *Computer forensics: An overview* (Vol. 1). Retrieved from http://www.infotex.com/portal_blog/white_papers/computer_forensics_overview_isaca.pdf
- ISACA (2001). *CISA review, technical information manuals*. Rolling Meadows, IL: ISACA, Inc.
- Krause, M., & Tipton H. F. (1997). *Handbook of information security management*. Retrieved from <http://secinf.net/info/misc/handbook/>
- National Institute of Standards and Technology. (1995). *An introduction to computer security: The NIST handbook - special publication 800-12*. Retrieved July 18, 2009 , from <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>
- Royal Canadian Mounted Police. (1997). *Technical security standard for information technology (TSSIT)*. Retrieved July 18, 2009, from <http://cryptome.org/jya/rcmp1.htm>
- SearchSecurity.com. (2002). *A TechTarget site for security professionals – A search for the definition of “Intrusion detection.”* Retrieved July 18, 2009, from <http://searchsecurity.techtarget.com/>
- Singleton, T. W. (2008). *What every IT auditor should know about access controls*

(Vol. 4). Retrieved from

<http://www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/IT-Audit-Basics/Pages/What-Every-IT-Auditor-Should-Know-About-Access-Controls.aspx>

Singleton, T. W. (2006). *What every IT auditor should know about cyberforensics*

(Vol. 3). Retrieved from <http://www.isaca.org/Journal/Past-Issues/2006/Volume-3/Pages/What-Every-IT-Auditor-Should-Know-About-Cyberforensics1.aspx>

Whatis.com. (2002). *A search for the definition of "Intrusion detection."*

Retrieved July 18, 2009, from: <http://whatis.techtarget.com/>

PC/SC WorkGroup (2002). *PC/SC WorkGroup*. Retrieved July 18, 2009, from:

<http://www.pcscworkgroup.com/>

United States General Accounting Office. (2002). *Federal information*

systems control audit manual – volume 1: Financial statements audit,

GAO/AIMD-12.19. Retrieved from July 18, 2009, from

<http://www.gao.gov/special.pubs/ai12.19.6.pdf>