Current Security State

Tulasi Pilli

Wilmington University

October 2014

Table of Contents

Abstract

In this world, information plays a key role in all the transactions across the globe. Every human has to access some kind of information to perform any operation in the office works. For example, many people purchase goods and services through bank accounts. Daily, every individual has to access the banking account, in which online banking is very easy access anywhere, anytime. During these transaction procedures, unauthorized people try to enter and access the data illegally to gain some money. So, proper protection has to be given to the data, which is often known as information security. Many organizations, fail to protect their data which causes heavy financial damage. Therefore, some solutions have been discussed in this paper in order to face the challenges of current security state. It is better for every organization to identify the threats and implement these solutions. So that, many people can be survived from attackers.

Key Words: information security, threats, solutions

Introduction

Technology has improved to make man’s life easier and more comfortable in all the sectors of country. So, many companies and individuals are addicted to technology. For example, with the evolution of internet, importance of libraries has been decreased when compared to earlier days. With the development of online purchasing and services, human involvement of travelling to stores has been reduced gradually. However, severe threats have been increased gradually by the attacking skills of unauthorized people. Many innovative techniques have been developed by the ethical hackers. Day by day, many threats have increased due to the effect of increase in internet users. The attackers try to attack the systems in the form of developing new virus, malicious codes, spam through electronic mails, and spyware software programs. All these unauthorized programs cause severe financial damage to the organizations and psychological depression to humans in losing their confidential information regarding crucial money transactions.

The threats of information security resulting to the damage of organizational assets can be reduced with the involvement information technology people. Many innovative methods have been developed by the information technology department in order to reduce the effects of malware programs. With the development of new technology, attackers also improved their knowledge in developing new malicious codes, which has become a never-ending story. Some people think that, developing innovative computers like MAC can eliminate the intrusion of malware programs. However, people should be aware of main uses of a system, as a system is used to run various number of software programs. Whereas MAC cannot support software programs like Microsoft Visio, which is a useful program for drawing various data programs. So, the prevention of intrusions can be only avoided by the knowledge of users. Research scholar

Ding-Long (2012) says that, “No matter how well designed, security methods rely on individuals to implement and use them”, which means the prevention of malicious codes is completely depended on the user to identify the issues of the system and implement a new innovative anti-virus program in order to defend the upcoming malware programs (Ding-Long, 2010, p221).

Security Policy

Many organizations experienced huge financial loss due to the attacks of unauthorized people in the form of malicious programs. If the attacker is able to know the details of company, then mostly some employee is helping the attacker for the sake of money or any other personal benefit. The main reason behind this huge effect is lack of effective security standards and policies for employee discipline. So, some people are trying to adopt best methods to face the attacking challenges. However, there are some other organizations thinking that the defect is present inside the company, moving around the employees. These companies treat their employees as an internal threat. At this kind situation, management enquires each and every employee about the leakage of confidential data to unauthorized people. In this case, if the management has doubt on any person, management is taking extraordinary and severe actions against the employee. Research scholar Eriksson (2001) says that, “securitization implies that problems are identified as existential threats legitimating the use of extraordinary measures, such as secrecy or the use of violence”, which means the management justifies the issue with severe actions of violence, if the issue is proved to be a threat from the employees (Eriksson, 2001, p212). After implementing this solution, attackers are unable to get the data from the employees and resulted in the decrease of attacking the systems.

Single Sign On

The main drawback of authentication is using various number times on different places. By using many times, attacker may observe the typing of the user and catch the alphabetical sequence of password. So that, attacker is able to crack the password and enter into the network illegally as a regular user. Hence, many organizations are encouraging the use of single sign on format. Research scholar D'Costa-Alphonso (2010) says that single sign on refers to a "user entering just one set of credentials for authentication and authorization and thereafter being able to access multiple applications securely and seamlessly", which means the user will enter the ID and passcode only for once (p163). So that, attacker may not be able to grab the complete details of passcode. This technique is widely used all over the globe. For example, Google account is single sign on account. If the user entered the log in credentials for one time, user can access the accounts of various applications linked to google account like YouTube, Gmail, maps, scholar accounts, etc., Initially, this technology did not attracted the users because of its poor performance. Later on, many changes have made to improve the accessing speed by collaborating with business partners to increase the business transactions through computer networks and systems applications (D'Costa-Alphonso, 2010, p163). Thus, log in credentials can be utilized to increase the security levels of an organization along with the implementation of single sign on technology.

Multiple Factor Authentication

Many organizations have implemented this technique in sensitive areas of the company. Every organization and its users are familiar about the authentication which is the process of identifying and verifying the identity of users. There are many types of authentication developed and implemented in the industries such as, biometrics, passwords, smart cards, and digital certificates. Usually, every organization uses any one of these authentication methods at a given time. If the same authentication procedure consists of two or more authentication techniques, then it is known as multiple factor authentication method. Through this process security levels can be increased to a high range, such that attackers cannot reach them.

Any attacker can crack a password or steal the personal identification data; but it is not easy for the attacker to crack both password and personal identification details. This is why, if we call any customer care service, agents use to ask multiple questions, so that illegal user can say one correct answer but at the same time multiple answers cannot be given by unauthorized person. Even though attacker cracks both the authentication methods, unauthorized person takes more time than the authorized person to answer the questions. In this way, customer service member can identify the authentication of the users.

There are three types of multiple factor authentication known as something you know (user id, password, answering challenge questions, pin), something you have (smart cards, digital certificates, device specifications like EMEI number for mobile device), and finally something you are (biometrics like fingerprints, face recognition, voice recognition, typing speed) (D'Costa-Alphonso, 2010, p164). Recently many organizations have implemented the techniques of multiple factor authentications in the systems and devices like laptops, computers, log in doors, etc. If the user is interested, any person can implement this technique in the personal computers also. For example, my laptop requires password and face recognition authentications to log in the windows and access the data. Similarly, every person can arrange the multiple factor authorization to improve the security.

Organization of Information Security

There are many threats in the society through which every organization suffers financial damage. Initially, organization has to identify the types of threats causing the data loss. Thereafter, management has to plan to prevent these threats. Research scholar Whitman (2003) explains the types of threats as “act of human error or failure (accidents, employee mistakes), compromises to intellectual property (piracy, copyright infringement), deliberate acts of espionage or trespass (unauthorized access and/or data collection), deliberate acts of information extortion (blackmail of information disclosure), deliberate acts of sabotage or vandalism (destruction of systems or information), deliberate acts of theft (illegal confiscation of equipment or information), deliberate software attacks (viruses, worms, macros, denial of service), forces of nature (fire, flood, earthquake, lightning), quality of service deviations from service providers (power and WAN service issues), technical hardware failures or errors (equipment failure), technical software failures or errors (bugs, code problems, unknown loopholes), technological obsolescence (antiquated or outdated technologies)”, which are the most common threats developed by attackers to enter the network connections of an organization (Whitman, 2003, p92). So, the company has to organize all these security threats of information security.

Asset Management

Securing the data is not only in the hands of employees but also the company’s management responsibility. Some organizations blame their employees, in losing the assets. However, many individuals oppose these actions and say that, even though it is the work of employees to secure the data, management has to identify the issues and threats to the organization and give proper training and also adopt necessary policies for protecting the data. Research scholar Workman (2009) says that, “policies on information systems security behaviors include updating or protecting passwords, keeping security software up to date, using firewalls, backing up systems, using surge protectors and paper shredders, maintaining systems access controls, implementing redundant systems, and using system activity and intrusion detection monitors", which helps to protect any kind of information from attackers (Workman, 2009, p563).

Human Resources Security

It is the responsibility of the human resource department in an organization to take an initiative in preventing the malicious codes. For this process, the first and foremost step is the development of framing procedure. Research scholar Eriksson (2001) explains the process of framing as "symbolic contests over the social meaning of an issue domain, where meaning implies not only what is at issue, but also what is to be done", which means the development of exact replica of the issues in the systems of an organization is possible by identifying the domain name and also the preventive steps to reduce the effect of problematic domain (Eriksson, 2001, p211). So, framing is one of the most important conceptual frameworks in identifying the malicious programs entered in the system and also the solution to delete the malicious program is defined clearly by the framing process.

It is the responsibility of policy makers to avoid the process of illegal threat framing, hiring and training, which involves the publishing of internal affairs to public through various sources of media or social networking. Even the employees have followed all the policies and regulations of the company, some people who enter as a customer or any media person may leak the details to attackers. So, it is very important for the management to maintain the secrecy and privacy of confidential issues and should never reveal anything in presence of outside people. There are two basic procedures in framing known as diagnostic and prognostic, in which diagnostic refers to analysis of a perceived problem by blaming or identifying the reasons of the issues in organization. Whereas prognostic means finding the appropriate solution for the issues found in analysis program (Eriksson, 2001, p212).

Physical and Environmental Security

In any organization, physical and environmental issues play a crucial role in securing the data. The maintenance process of the various operations in the company is completely depended upon the employees and the environmental resources. So, it is the responsibility of the management to identify the threats caused by human activities like employees helping attackers and estimate the upcoming environmental issues like power failure, lack of raw material supply, etc. Usually, unauthorized people try to attack the network by taking the advantage of these human and environmental threats. Attackers are able to know the information of loop holes in the organization frame by convincing the employees and providing huge amounts of money in the form of bribes or gifts.

Unauthorized people also take advantage of environmental issues in the form of diverting the company's security personnel to other aspect and then attacking the network. These natural threats also include bursting of pipes that can easily flood the computer room (Stoneburner, 2002, p13). At this situation, attacker may enter the organization as a helping person, and steal crucial data silently. So, it is very important for the organization to make proper planning by estimating the issues at early stage. So that, physical and environmental security levels of an organization can be improved.

Communications and Operations Management

Every organization prefers communications a major aspect in order to run a plant efficiently and effectively. Without a proper communication, it is not possible to process any operation in the company, because without knowing the work completed by an employee in the first stage, next level employees do not understand anything about the project. So, there should be proper co-ordination and communication between the employees. Moreover, it is also important for the management to make sure the employees are aware of the company's vision and goals (Copa, 2012, p49). So, management has to arrange frequent meetings with the employees and deliver the basic functionality and performance expected in order to reach the goals.

Research scholar Copa (2012) says that, "plant operational reliability elements are design, equipment, processes, and people", which means an organization is completely depended mainly on the working of employees, methods followed, availability of machinery, and technology adopted to complete a project efficiently (Copa, 2012, p49). Thus, the communications and operations management is very crucial for any organization to improve the maximum performance and deliver best products to the customers.

Access Control

Every organization consists of hundreds or thousands of employees working in various shifts and timings. Company cannot provide a personal system for every employee individually. So, the ratio is usually one computer for two or three employees. Hence, a computer is operated by more than one person. So, the administrator has to give proper access to the employees accordingly. Thus, access control came into existence for the usage of system at the entrance of organization as well as reentry of the same user in the computer systems. Simply, access control can be described as the authority of accessing the data in a computer system. Research scholar Sehgal (2011) says that, “the access control can be resolved at a hardware level with a special access device such as a dongle connected to the USB port or built-in security keys”, which means an additional device is used to increase the protection of computer system or the protection feature is installed in the computer itself (p282). This access control technique is utilized with the process log in credentials.

It is the responsibility of the management to handle the procedure of access control. Research scholars Conklin & White (2012) explains that, there are four types of handling access control. They are mandatory access control which is, “a process of controlling access to information based on the sensitivity of that information and whether or not the user is operating at the appropriate sensitivity level and has the authority to access that information”, which means the administrator verifies the confidentiality of the use and the accessing capability to reach the confidential levels of authentication (p585). Discretionary access control is “the process of using file permissions and optional access control lists to restrict access to information based on a user’s identity or membership”, which refers to verification of authorized user’s registration details to access the information or the computer system, which requires permission from owner or group of authorized members (p586).

The other two types of handling access control are role-based access control and rule-based access control, through which a user can access the system by the assigned roles and predefined rules respectively (p587). Thus, access control can help to improve the security levels of information systems in any organization by implementing various types of access controls as discussed. It is also important to select the perfect type of access control depending on the issues in the organization.

Information Security Incident Management

Technology has developed many innovative techniques rapidly in the past decade. Many changes have occurred in the field of information technology. Even the attackers have increased their capacity; information technology people have achieved huge confidence of facing these threats by security incident management with the development of semantic threat graphs. Research scholar Foley (2011) defines the semantic threat graph as “a graph that represents the meaning of threat domain, and makes explicit the information that is typically implicit in a threat tree”, which means the basic domain caused for the threat is identified and the data can be easily known by threat trees (p572).

Many organizations follow a particular type of top down threat modelling approach known as threat tree, attack tree and many other similar technologies, in order to identify, represent and analyze the threats intruded into the organization’s system in a semi-formal and logical way of identifying the reasons of issue (Foley, 2011, p567). Moreover, the configuration of security systems is the main agenda of eliminating threats in semantic threat graph approach.

The network and security configuration and the relation between the networks and threats can be easily demonstrated by the implementation of ontology concept in semantic threat graphs. Firewalls also play an important role in defining the threats and its mitigation technique. The arrival of illegal packets can be destroyed by the implementation of firewall. Moreover, the replica of original interface packets can be avoided by dropping the reserved internal IP addresses, which results in the improvement of security levels of an organization. Thus, it is very important for the organization to identify the incident and implement a particular approach to reduce the issues of an information system.

Business Continuity Management

Every employer starts an organization, just to earn money. The employer invests huge amounts money to start an organization. So, the employer expects an increase in Return on Investment (ROI). Return on investment is nothing but, the total amount of money returned to the employer apart from the investment contributed to the organization. In this scenario, if a sudden disaster occurs, then the organization will be destroyed which results in huge loss for the employer. So, here comes business continuity management on to the screen.

Business continuity management means to survive form the disaster by preparing with various precautions and preventive steps. In order to survive from the disaster, proper plan with knowledgeable team is required. Research scholar Nicoll (2013) says that, "plans must be regularly updated and refined to reflect changing business conditions and activities", which means management has to initiate not only to make a proper plan but also the same plan has to be updated frequently with necessary corrections learned from lessons taught with every disaster.

Conclusion

The main threat to information security and the major required solutions to improve the security levels for an organization is explained in this paper. In order to conclude that, it is recommended for any organization to train its employees to be aware of the latest malware programs. So, the employees can take necessary actions to avoid the malicious code. Without knowledge, no one can control the data loss and survive from the attackers. Managements have to take initiation to educate the employees and it is the responsibility of the company to provide necessary programs to eradicate these kinds of threats. Moreover, the organization has to identify the issues without any delay and implement the solutions discussed in this paper. Finally, each and every organization must be united to d co-operate each other and prevent the attacks from unauthorized people; as we all know ‘Unity is Strength’.

References

Conklin, W. A., & White, G. (2012). Principles of computer security: Comptia security and beyond. (3rd ed., pp. 1-714). New York: McGraw-Hill companies.

COPA, M. M. (2012). maintaining STANDARDS. Mechanical Engineering, 134(7), 48-51. Retrieved on October 6, 2014 from http://mylibrary.wilmu.edu:2052/login.aspx?direct=true&db=aph&AN=77348157&site=ehost-live

D'Costa-Alphonso, M., & Lane, M. (2010). The Adoption of Single Sign-On and Multifactor Authentication in Organisations -- A Critical Evaluation Using TOE Framework. Issues In Informing Science & Information Technology, 7161-189. Retrieved on October 6, 2014 from http://mylibrary.wilmu.edu:2052/login.aspx?direct=true&db=aph&AN=53700210&site=ehost-live

Ding-Long, H., Rau, P., & Salvendy, G. (2010). Perception of information security. Behaviour & Information Technology, 29(3), 221-232. doi:10.1080/01449290701679361. Retrieved on October 5, 2014 from http://mylibrary.wilmu.edu:2052/login.aspx?direct=true&db=aph&AN=50218717&site=ehost-live

Eriksson, J. (2001). Cyberplagues, IT, and Security: Threat Politics in the Information Age. Journal Of Contingencies & Crisis Management, 9(4), 200. Retrieved on October 5, 2014 from http://mylibrary.wilmu.edu:2052/login.aspx?direct=true&db=aph&AN=6633317&site=ehost-live

Foley, S. N., & Fitzgerald, W. M. (2011). Management of security policy configuration using a Semantic Threat Graph approach. Journal Of Computer Security, 19(3), 567-605. doi:10.3233/JCS-2011-0421. Retrieved on October 6, 2014 from http://mylibrary.wilmu.edu:2052/login.aspx?direct=true&db=aph&AN=60886905&site=ehost-live

Nicoll, S. R., & Owens, R. W. (2013). Emergency Response & Business Continuity. Professional Safety, 58(9), 50-55. Retrieved on October 6, 2014 from http://mylibrary.wilmu.edu:6609/ehost/pdfviewer/pdfviewer?sid=bd43d0f6-6759-4019-9391-b8c8df489612%40sessionmgr115&vid=0&hid=116

Sehgal, N. K., Sohoni, S., Ying, X., Fritz, D., Mulia, W., & Acken, J. M. (2011). A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing. IETE Technical Review (Medknow Publications & Media Pvt. Ltd.), 28(4), 279-291. doi:10.4103/0256-4602.83549. Retrieved on October 6, 2014 from http://mylibrary.wilmu.edu:2052/login.aspx?direct=true&db=aph&AN=65095698&site=ehost-live

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. Nist special publication, 800(30), 800-30. Retrieved on October 6, 2014 from http://www.security-science.com/pdf/risk-management-guide-for-information-technology-systems.pdf

Whitman, M. E. (2003). ENEMY AT THE GATE: THREATS TO INFORMATION SECURITY. Communications Of The ACM, 46(8), 91-95. doi:10.1145/859670.859675. Retrieved on October 5, 2014 from http://mylibrary.wilmu.edu:2052/login.aspx?direct=true&db=aph&AN=10538013&site=ehost-live

Workman, M., Bommer, W. H., & Straub, D. (2009). The amplification effects of procedural justice on a threat control model of information systems security behaviours. Behaviour & Information Technology, 28(6), 563-575. doi:10.1080/01449290802556021. Retrieved on October 5, 2014 from http://mylibrary.wilmu.edu:2052/login.aspx?direct=true&db=aph&AN=44813110&site=ehost-live