Our Services

- Essay and Assignment Writing
- Dissertation Writing
- Assignment Marking and Critiquing
- Proofreading and Editing service
- Disertation topic and plan/outlet
- Disertation proposal writing
- Statistical Analysis
- Personal Statements

Risk Assessment And Mitigation In Computer Networks Information Technology Essay

Abstract

Over the past few years, the diversity of risk that the computer network face by sophisticated attackers has increased drastically across all societal boundaries and has enforce difficult economic burden on life, health and organization. This is as a result of plethora features of modern technology, rapid growth of internet services, collective usage and sharing of information. Therefore, making risk assessment an extremely crucial issue in computer network. This paper discusses the risk that may occur in computer network, risk assessment, risk mitigation and strategic control.

Keywords: Risk Assessment; Risk Mitigation; Risk Control

1. Introduction

Statistically, there has been an alarming trend in the number of security leverage such as financial fraud, theft of proprietary information, data or network treachery or espionage, system penetration by hackers or denial of service attacks in many organizations in recent years; many and big companies have been victim of these explosive computer network security breaches. Thus, the utmost key priority of any organization is the security of their information and in order to meet the requirements of the business (information security) i.e. Confidentiality, Integrity and Availability (CIA) the value of information must be sustained. Therefore, the likelihood of loss (Risk) in the computer network of an organization should be put into consideration because as computer network yield great value to businesses it also carries risks and uncertainty.

This essay is an example of a student's work

Disclaimer

This essay has been submitted to us by a student in order to help you with your studies. This is not an example of the work written by our professional essay writers.

1.1 Risk

Risk is the concept or probability of the likelihood of loss that will have an effect on the achievement of the objectives that is, how much the business is going to lose if the computer goes down because of down time. Lose can come from a number of different places, for instant:

Down time: when the server is down

Fraud: hacker, spoofing, phishing, spammer etc

Legal issues:

Furthermore, Risk is a vulnerability that could allow loss of confidentiality, integrity or availability of computer network. The sources or risk can be natural (like flood, fire, power surge etc) or man-made that can be intentional or unintentional.

Risk can be said to be:

Risk = Threat * Vulnerability

Threats are the outside forces that could compromise the system, threat is not just about hackers but other threats are:

Natural disaster: i.e. flood, fire etc

System failure: quality of the components used, the higher the quality of the components the lower the probability of network failure.

Accidental human: that someone is going to do something accidently is usually high

Malicious human: here there are;

Impersonation is when someone try to become another person to get the account details or money

Interception is when someone hack the server or mail to acquire data

Interference is when someone damage the business by stealing the server but not the information

The threat of malicious human is done for the purpose of making money illegally and the higher the possibility of all these the higher the threat

Vulnerability is refers to the flaws or weakness in a computer network that can expose it to a threat (attack); What protection or setup is put into place to protect the system i.e. The higher the protection the lower the vulnerability.

The table below show the different Threat and Vulnerability

THREATS

VULNERABILITIES

Natural disaster

Exposure to natural disaster like server placed ground floor of the building and no fire extinguisher.

System failure

Using inferior or low quality components.

Accidental human

No group policy.

Malicious human: Impersonation

Interception

Interference

Careless placement of vital document and no shredder.

Lack of firewall, Antivirus, Group policy and so on.

No lock on doors or server room.

Table 1

The higher the threat and vulnerability the higher the risk but if vulnerability is low, threat is reduce and the lower the risk.

2. Overview of Risk Assessment

Computer security is the use of technology to do a job or task properly that is, making sure that the system work properly. Security is the process that requires input from the entire organization to be effective.

Risk assessment simply means looking at each specific task and considering the safety way to complete it, this helps to be aware of the hazards involved in performing the task and taken actions to prevent injury. To assess risk, one first need to identify the hazards (that is, tools, equipments, materials and work method); Secondly, to decide who might be harmed and how. Furthermore, evaluate the risk and put measures to control the risk. Also, record the discovery and implement them and lastly, examine the evaluation and update as necessary.

2.1 Risk Assessment Process: in risk assessment the series of actions to achieve result includes:

What valuable assets used for the network (for example, computers, information trade secret)

What are threats to the network (hackers, fraud, impersonators, and internal employees); Hackers could be internal or external vandalism.

What are the vulnerabilities to the network (infrastructure vulnerability and so on).

2.2 Techniques used to assess risk

Over the years, different techniques have been used to perform risk assessment in computer network of which are: National Institute of Standard and Technology (NIST) technique, Operational Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) and benchmarking.

NIST assist organizations to develop, maintain and retain standard measures of technology needed to improve the quality of product, to ensure the use of updated actions to achieve results, to ensure the reliability of the product and to assist the rapid growth of marketing. It is the assessment of Access Control System.

OCTAVE is self directed activities that allow an organization to identify and manage the information security risk that is important to its task, that is, the threats to the valuable assets and the vulnerabilities that may expose the assets to threats. With these the organization will be able to design protective strategies to reduce the overall risk exposure of its information assets. In addition, OCTAVE addresses the CIA of the assets or information of the organization.

This essay is an example of a student's work

Disclaimer

This essay has been submitted to us by a student in order to help you with your studies. This is not an example of the work written by our professional essay writers.

Who wrote this essay ▸

Place an Order ▸

The latter, is the technique used to measure the performance of computer network. Benchmarking tools is a set of programs that is used to measure and evaluate performance, network protocols, devices and networks under certain conditions. More so, benchmark help to determine and improve the potential and stability at different speed of hardware and software (valuable assets). Furthermore, it help to know how well a computer network can hold up under a stressful situations and also to determine the location of a particular problem which in turn, help to reduce expenses when repairing and updating the network. Network connections, CPU function, server and many more are part of the computer network that can be benchmarked.

2.3 Scope of Risk Assessment

In an organization where information is being generated on a daily bases, security of information is the most important priority that should be put into consideration on order to prevent any cybercrime that seek to compromise the network. Risk assessment carries out the security and information threat that may occur in an organization, it helps to plan for the unforeseen circumstances. Threat could be internal or external forces to undermine the organization not to be able to achieve its information security goals (CIA).

To assess risk there is need to identify the threats that may occur and the vulnerabilities to the threats, threat is not just about hackers but include the following:

2.3.1 Natural disaster:

In the world where nature regulates itself, natural disasters pose serious threats on life and property safety. Common natural disasters are flood and fire, which occur without any warning. According to Blaikie, [YEAR] disaster occurs when hazards meet vulnerability. Therefore, the utilization of some methodology will protect against loss to natural disasters; for instant a failsafe mechanism being in place at all times will be of great help. The mechanism involves the placement of servers in the upper room of the building, the use of back-ups servers, building of structures to the best one can, the use of fire alarm and fire extinguisher.

2.3.2 System failure:

In many cases, when an organization is trying to reduce cost tend to buy inferior components for their computer network which may result to network failure. The higher the quality of the components or system the higher the vulnerability then probability of network failure is low.

2.3.3 Accidental Human: OR HUMAN INCIDENT (title error)

The probability that someone will intentionally or unintentionally do something that will course harm to the computer network is very high or that someone is going to do something retarded (like shutting down the server). In this case, there is need strong authentication and encryption (the use of public and private keys) or password to be able to have access to the computer. In addition, the use of locks on valuable assets so that no one will do away with them or even is able to carry them.

2.3.4 Malicious Human: (or persons with criminal minds)

These are people with malicious intent; it is classified into three, which are: Impersonation, Interception and Interference

Impersonation is likening to spoofing or Phishing. This is when one successfully deceives or disguises to gain access by falsifying data into someone else's resources illegitimately.

Interception is when one hack the server or mail basically to acquire vital information or data or trade secret in order to sabotage the organization, espionage trade secret or to blackmail the organization.

Inference is when one damages the business by stealing the server (not stealing information or doing fraud), computer systems or any tangible assets in order to make money out of it.

Therefore, in malicious human the use of good authentication and encryption of information for specific resources are important and also the use of locks to bolt down computers from being stolen. Leverage by criminals could be internal or external.

2.4 Points at which risk should be assess in a computer network

Risk assessment is process that must be periodically repeated, it requires an ongoing effort. There is never a wrong time to assess risk and examine network vulnerabilities. Risk assessment is not only to understand the technology solution to security but also to understand the business justification for implementing the security. Important areas where risk needs to be assessed are:

This essay is an example of a student's work

Disclaimer

This essay has been submitted to us by a student in order to help you with your studies. This is not an example of the work written by our professional essay writers.

When new code, program or application are developed, to ensure the security state of the system and to know whether the analysis performed earlier will help if security problem exist.

Whenever changes are made on the programs or systems which will help to reveal vulnerabilities that as a possible side effect.

Risk assessment and vulnerability assessment should be done carried out regularly to examine the control implemented and anytime there is leverage in security, intrusion or attack. Thus, help to detect how the breach occurred and the problem with the policy used.

3. Mitigation of Risk in Computer network

This is the process that when a disaster happened, it is looked into, fixed and prevents or reduces the consequence hazard from happening in the future. Mitigation of risk is preventing future occurrences; that is, making the bad not so bad next time. It is a technological safe guide ways of protecting the system, to lessen the vulnerability. Mitigating risks would go a long way towards improving security. Ways to protect the system and lessen probability of threat or vulnerability impact in an organization includes:

3.1 Firewalls

Administrator setup firewalls to restrict a computer network from unauthorised packets in and out of the local network. Firewall could be hardware as external devices located between the LAN and the router connected to the internet or as software installed on each PC. Firewalls act as packet filtering that receive and examine all coming data. It guards the internal computer network against malicious access from outside and can also be configured to limit the access of internal users to the outside world. It is setup at every connection to the internet subjecting all data flow to careful monitoring and also setup to obey security rules that only gives the administrator control over the traffic that flow in and out of the network. Firewalls offer security that makes the computer network less vulnerable and mitigate risk.

3.2 Antivirus software

Antivirus software is setup to protect and defend the computer against malicious threat or viruses like Trojans, hijackers, Keyloggers etc and other codes that can destroy the system which can be initiated by the users while browsing the web or via CDs, USB, memory sticks across the network. The threat can slow the computer down and also cause an unusual and unwanted behaviour to the computer. There is need for solid antivirus scanner to detect that there is a malicious threat on the system and clean the system from these threat enabling the user to have a malware clean system. Antivirus software should run in the background at all times and be updated when expired to maintain the integrity of the network.

3.3 Group policy

This is setting up of policy that allows or provides centralized control of users and computers. It provides control over application and removes the application when it is no longer required. It create a specific customize desktop configuration for group of users and computers. It provides a logged on to the computer using an account that has administrator privilege in order to use the policy.

3.4 Backup System

The use of network backup software enables backup of all computer and servers through the network, it allow backup of data, database, applications and operating system. It comes with an interface that allows the software to automatically backup the data from time to time. The network backup uses strong encryption technology so that unauthorized users can not access the data. More so, it allow backup into different destination such as CDs, USB, DVD, Zip disk in the event of disaster. It reduces down time because it restores data immediately and can also be used to recover file.

3.5 Physical security

Physical security for the system is the use of good lock on the steel door to the server room to makes it more difficult to break in. All confidential is locked at all time so that any intruder will not have access and bolt down the computers to prevent them from being stolen.

3.6 Operational Security

Setup security where things are stored in the organization, that people do not know where important things are stored in the organization except important people that make use of the place.

4. Conclusion

Risk assessment is an essential management function that plays a crucial role in protecting the organization information and ability to achieve the goals of computer security (CIA). Risk assessment helps the organization to identify where the present and future risks are and how to increase or enhance the level of security. Risk assessment analyzes the safety way of completing a task and also performs core system maintenance. It makes the business robust and makes return (money) higher than the cost of establishing the business.

This paper explore the risk assessment and mitigation in computer network, it identify the threats and vulnerabilities that could cause risk in the computer network. Discuss the techniques used to access risk and risk assessment. It analyze the preventive measures such as setting up of firewall, Antivirus software, group policy, backup system, physical security and operational security to mitigate risk which have more significance for managerial planning by organization for computer network dependability particularly with regards to computer information safety.

Finally, risk assessment does not guarantee the total elimination or stop to all malicious threats but reduces risk to its minimal. Thus, adequate training should be given to guide the staffs on the policy of the organization and response to certain internal and external influences because the biggest computer risk is actually the user behind the computer in most cases. Practice safe internet habits and use updated virus protection and review assessment periodically.