Physical threats essay example

Business, Strategy

Introduction

Technology has become part of the major sections of the security of any facility. For example, a busy pharmacy in a shopping mall is unique and requires proper physical and logical access controls. The systems are required to protect the medication and funds located on the business. The system would also assist in the access of the personally identifiable information as well as the protected health data of the customers that exist in the system. The security may be installed through reliable as well as logical technological methods that would be essential to eliminate the risks that would be available. The elements that will be necessary for the system include one firewall, four desktop computers, windows 2012 Active Directory Domain Controllers (DC), Dedicated T1 Connection, and one file server.

The accurate performance of the computer system will depend on the consideration of exclusive physical threats. These are the elements that are likely to affect the system and are physical. It means they are threats that can be controlled through physical means. Physical threats may be in the system or the environment surrounding the system.

The common physical threats in a computer system include improper environment for storage, natural disaster, inadequate hardware maintenance, human error, as well as sabotage. It is evident that all the physical threats are observable through the eyes or proper knowledge of the computer system.

The threats have direct damage to the computer or the system, and the effects of each of them are only rectifiable through proper use of a unique

physical threat intervention strategy. Physical threats are easy to solve following their accessibility within the computer system.

Logical threats

Also, there are a number of logical threats that would be controlled through the technological system. They include Virus, Trojans, Worms, Spyware, Keyloggers, Adware, denial of Service Attacks, Distributed Denial of Service Attacks, unauthorized access of computer systems, as well as phishing (Announcement, 2013).

The threats are highly sensitive to the data or the information of the business. They determine how certain data may be attacked by nonphysical objects and bring down the entire system. The nonphysical objects are highly sensitive to detect since they can only be identified through critical analysis of the system (Announcement, 2013).

The virus, Trojan, worms, and spyware among other logical threats are extremely sensitive on how the form. They behave as malware programs that when executed, multiply by copying itself into other computer programs, data files, as well as the boot sector of the hard drive. Therefore, dealing with such threats requires specialized intervention. On the other hand, other logical threats require special intervention to ensure the success of the systems being employed (Announcement, 2013).

Controlling the physical threats

Improper storage environment

The control strategy that will be most effective for this threat is administrative. The developers of the computer system must take precaution

and develop a system that will cope with the environmental conditions within which it operates. The administrator if in charge of reviewing the region that he or she will use for the installation of a computer system. As a result, the area must be free from hazardous elements that are likely to cause a negative effect to the computer system (Northcutt, 2013). The region of installation must be well protected to ensure the computer system is installed in the most outstanding manner and the environment does not affect it in any negative way.

Corrective and preventative control measures may also be highly relevant in controlling the effect of improper storage environment. The administration must correct all the elements that may seem hazardous to the operations of the system. Therefore, it must undertake the corrective measures that will ensure the proper environment for the system. Preventative control comes in when the administrator wishes to protect the system from unknown environmental threats (Northcutt, 2013).

Sabotage

The physical threat mainly refers to the cases of theft and vandalism. The preferable control measure for the threat is administrative. The administration may have direct control o the issues of theft and sabotage to the computer system. The administrator is aware of all the loopholes of the system, and he has control over them. Therefore, he may have a direct impact in controlling the level of theft or vandalism.

Intact security measures may be installed to the system, making it difficult for the thieves and any other person with negative motive from accessing the system. The system must be installed in such a way that no nonusers are

allowed to access it. It means there must be proper (Northcutt, 2013).

In this case, detective control measure may be applicable. It means installation of the device within a system that detects the entry of an unauthorized person to the system. For example, an alarm may be set to alert the administrator once an unauthorized person gains entry to the computer system (Northcutt, 2013).

Human error

It is common to find mistakes in the computer systems as a result of human error. The action or inaction of a human being in the system may influence its performance in one way or the other. It is wise to take precautionary measures to avoid errors in a computer system through human actions and inactions.

The most outstanding control measure for human error is preventive. The system should be developed in such a way that it is easy for the users to operate. It means every person with the authority to access the system should have the necessary knowledge of the system. The prevention may come with the proper outline of the instructions that the user is supposed to follow in accessing the system (BCP Business Center, 2014). A user guide may be provided to assist the user in making the most outstanding use of a computer system.

Inadequate hardware maintenance

Every computer system requires installation of the right hardware to ensure its proper operations. The physical outlook of a computer system is defined by the hardware it contains. There is exclusive significance of the use of high

profile hardware in developing a computer system. However, the success of a computer system may highly depend on the maintenance of the hardware in the system.

The preferable control measure for the threat is administrative. It is the role of the administrator or the developer of the system to ensure proper operations of the system. In that case, proper maintenance must be carried out to ensure the problems arising from faulty hardware do not exist.

Also, corrective measures may work extremely well for this threat. The administrator may develop a well-structured plan for correcting errors that may arise within the system. There should be outstanding maintenance techniques, which are developed in a bid to correct the faults that are likely to rise from the computer system. There may be a maintenance team, which is responsible for correcting all the problems that may arise in a computer system(BCP Business Center, 2014).

Natural disaster

In most cases, the administrator cannot choose the natural occurrences that will influence the computer system. There are hazards that are likely to affect the computer system, but they come directly from nature. For example, rain, wind, and earthquake are natural occurrences that the administrator cannot prevent from occurring but he can come up with a strategy to hold their extensive effects (BCP Business Center, 2014).

The effects of the natural occurrences can be controlled through detective controls. The system may be developed in such a way that it reports on the occurrence of natural disasters such as earthquake and fire through the alarm.

Control for logical threats

Denial of Service Attacks

It is logical threat where people who have been protected from accessing the computer system device attack to the system. It is mainly linked to common computer-hacking. The threat may be controlled through administrative measures. The measures involve using controlled access to the computer system. Necessary passwords should be used to control the number of people accessing the system.

Unauthorized access of computer systems

In some computer systems, it will be easy for any person in the office to access all the computers (BCP Business Center, 2014). However, the problem may be resolved with the necessary measures being undertaken.

The main control measure for the threat is administrative. There should be controlled access to the computer system. Only authorized users should have the passwords for the access of the system.

Phishing

It is a technological threat where some programs and programmers roam on the internet looking for unprotected computer systems so that they may take advantage through access of the passwords and entry codes. The threat may be resolved through preventative and detective control measures.

Preventative and detective measures may be installed where the administration protects the passwords and entry codes of its computer system from access by the public. The passwords may be maintained by one person who may be the administrator of the system. Detective control

measures may take charge of the system where any attempt to access the system is shattered.

Virus

It is a common logical threat to computer systems. It is a program that is usually developed with the aim of offering counter performance to the real program. The effect of the virus in a computer system may be controlled through installation of antivirus. The installation of the antivirus may be through the detective control option. The administration must ensure the computer system is well protected with the most effective computer antivirus.

Trojan

It is a non-self-multiplying malware program containing malicious code that once executed carries out activities determined by the nature of the Trojan. In most cases, the Trojan is used in the theft of data, as well as probable harm for the system (BCP Business Center, 2014).

The logical threat may be controlled through detective measure. The system may be set in a way that it detects that malware as it attacks the system. Exclusively strong detectors may be installed to resolve the problem.

Handling physical threats risks

The physical threats may pose exclusive challenges that require proper or reliable risk handling techniques. The techniques include risk mitigation, risk assignment, risk acceptance, and risk avoidance (Four Types of Risk Mitigation and BCM Governance, Risk and Compliance (GRC), 2013).

Improper storage environment

The best risk avoidance technique for the threat is risk avoidance. It means developing necessary technological strategies to ensure the threat does not attack the system. Once that is done the developer will have avoided the risks that come with the improper storage environment (BCP Business Center, 2014).

Sabotage

The risk involved in this kind of physical threat may be resolved through risk avoidance strategy. Such activities as theft can be avoided by ensuring the existence of necessary security measures that take charge of the computer system (Four Types of Risk Mitigation and BCM Governance, Risk and Compliance (GRC), 2013).

Human errors

Since it is impossible to employ human beings who cannot make mistakes, it is impossible to have a system that is free from human errors. However, an action may be undertaken to ensure the errors are less harmful to the system. The risk handling strategy that is most effective for this threat is risk mitigation. Human beings can always learn to rectify their mistakes hence, the need for the mitigation strategy (Four Types of Risk Mitigation and BCM Governance, Risk and Compliance (GRC), 2013).

Inadequate hardware maintenance

The maintenance of a computer system depends on the willingness of the administrator to have a safe computer system. The risk that comes with the problem can be resolved through the risk assignment strategy. Some people

must be allocated the duty of ensuring consistent maintenance of the system (Northcutt, 2013).

Natural disasters

It is clear that natural disasters are unavoidable. The risk that comes with the natural disasters to a system may be resolved through acceptance that they are natural, and they will always occur (BCP Business Center, 2014). Therefore, risk assignment would be the most outstanding strategy to resolve the problem.

Handling logical threats risks

Like the physical threats, logical threats can also be resolved through consideration of the risks surrounding the system.

Denial of Service Attacks

The preferable risk solution strategy to this logical threat is risk avoidance. The system should be protected fully to avoid the possible attack of the system by other people. It is possible to control the programs that access a system

Unauthorized access of computer systems

Also, this threat may be dealt with through risk avoidance. The system may be set in a way it can detect when the wrong people accesses the computer system (BCP Business Center, 2014).

Virus

The administrator may deal with the risks that come with this risk through risk assignment strategy. He or she may set up a team that ensures there is proper installation of up-to-date antivirus to eliminate the viruses.

Phishing

Following the sensitivity of this logical threat to the system, risk avoidance should be a crucial risk resolution strategy (Northcutt, 2013). The method is unique in ensuring all the platforms through which phishing may occur do not exist. Anybody who may be out for phishing over the computer system must be eliminated completely from the system.

Trojan

Since the threat can be avoided through proper control of the system, risk avoidance strategy would be the most effective. It can bring in substantial solution to the existence of a threat in a computer system (Northcutt, 2013).

Conclusion

The computer systems will always have threats whether physical or logical. The system should be developed uniquely to ensure it can identify the threats easily. However, solutions must be installed to ensure the threats do not occur or do not affect the system. The threats may be controlled through administrative, preventative, detective, and corrective techniques. The risks that comes with the risks may be resolved in a number of ways, which include risk mitigation, risk assignment, risk acceptance, or risk avoidance.

References

Announcement. (2013, April 13). Retrieved December 12, 2014, from http://forums. iobit. com/forum/iobit-security-software/iobit-security-softwares-general-discussions/other-security-discussions/15251-28-types-of-computer-security-threats-and-risks

Dorian, L. (2011, February 5). ICABC: Industry Insights -- Risk Management: Understanding Risk Mitigation. Retrieved December 12, 2014, from http://www. ica. bc. ca/ii/ii. php? catid= 17

Four Types of Risk Mitigation and BCM Governance, Risk and Compliance (GRC). (2013, May 17). Retrieved December 12, 2014, from http://www. mha-it. com/2013/05/four-types-of-risk-mitigation/

Northcutt, S. (2013, April 11). Security Laboratory. Retrieved December 12, 2014, from http://www. sans. edu/research/security-laboratory/article/security-controlTop of Form

Security Check: Reducing Risks to Your Computer Systems | BCP Business Center. (2014, September 17). Retrieved December 12, 2014, from http://www. business. ftc. gov/documents/bus58-security-check-reducing-risks-your-computer-systems