Example of essay on primary physical and it security threat to organizations

Business, Company

Abstract

This paper is written in the form of an advice by a chief security officer to the CEO of a company. It shows the general physical and IT threats that a company is faced with and how it can be dealt with. The study shows that there are physical threats that affect a firm's computer hardware. This includes threats to the hardware itself and threats to the premises and intermediary systems. IT threats includes threats to data security and breaches to the system. This can be handled through a strategic approach that involves risk assessment, formulation of an IT security plan and its implementation.

Introduction

Information is an important aspect of every organization. Information technology (IT) is a tool for competitive advantage and it is important for the efficient and effective utilization of resources in an organization. Therefore, keeping information within our IT infrastructure and Information Systems is an important part of ensuring that we achieve the main goals of our investments into the IT systems and processes.

In this paper, the Chief Security Officer of an organization outlines the primary challenges of physical security threats and IT security threats. The scope of the paper will cover the two individually and collectively. The paper will show ways of balancing the two threats and achieving the best and optimal results in using a firm's information systems.

Physical Threats

The physical challenges that relate to an information system have to do with the hardware system of the IT process and system of a company. This hardware system includes " storage and transmission media and information processing machines". These are the tangible elements and aspects of a computer based system that an organization uses to carry out its processing and activities.

Thus, the physical threats of the information system include the threats against these physical parts of the computer system. They are diverse and could be wide range in effect and impact. This includes:

Physical Breaches of Integrity; This is a major problem which involves the access of hardware tools that a firm possesses which could lead to major breaches in password and other materials. This could be stole and abused by malicious persons and can lead to major problems in a given organization.

Theft: The elements of a company's IT infrastructure including computers, hardware devices and others could be stolen by third parties. There could be a major break-in that will cause a firm to lose some of its expensive devices and equipment. This could lead to the loss of important assets and expensive devices that will go to affect the capital base of an organization. There could also be a loss of information that could lead to loss of vital data that might be needed to work. Additionally, there could be cases of blackmail and public embarrassments as the case has been with major banks and major US departments.

Natural Disasters: There is the risk of major natural disasters like earthquakes, lightening, floods and hurricanes that might stand in the way of a firm's information systems and processes. This includes the loss of vital information and data like data relating to major clients and other information. There have been cases where the impacts of some natural disasters have been exaggerated by people in companies. For example, in major audits, there have been cases where people have blamed the lack of vital information on the loss of some important hardware that was lost during a natural disaster.

Apart from the physical threats to the equipment of a given company, there is the physical threat to the premises within which the computer hardware is being stored. These are threats to the building and other levels of protection that is guaranteed to the information system hardware. These are prone to major risks including break-ins, terrorism, bombings, natural disasters and other things that could put the information system equipment in some form of risks. There is the need for some kind of checks and controls to be put in place to prevent breaches that might leads to the loss of information and other vital materials and tools.

Finally, in the arena of physical threats, there is the threat of Supporting Facilities and this includes the facilities like electric power, communication services and environmental controls. These are mainly intermediary threats and risks that could affect the functioning of information systems and processes. This includes the voltage consistency and other concerns that could damage equipment. The functionality of an internet or communication service provider is also vital. There are risks and threats relating to other matters like air-conditioning and heating and the moderation of its usage.

This is because the extreme use of these in any form or level might end up damaging the hardware systems of a given hardware system.

IT Threats

Technical IT risks include the risks related to the integrity of the software features and information content that is stored in the IT system of a company. Vulnerability can be classified in three main ways and forms:

Internal Risks: This includes the risk of the software system operating in a manner that is less than ideal, hence allowing third parties within the organization to gain access to information that is required to be confidential. This includes risks relating to the network system and its protocol and the inability to ensure that the security systems like passwords operate appropriately to cover all the necessary security limits. These are risks that are inherent in the system and might give way to some major information integrity loops because there are bugs and weaknesses in the system. This will make it easy for some people to get into the system and make information to be loosely given away;

Intermediary Risks: This is the risk relating to the loss of information through the loss of information and data to other third parties. These are risks relating to the data that is not properly moved through the system of an organization or a company’s system. Therefore, there is the risk that the information that is shared and protected is not done in a way and manner that meets the security needs of the firm. Hence, there is a risk that people within a given system might not be able to communicate in the way and manner possible.

External Risks: These are risks that relate to the way and manner within which a firm's information system can be accessed by malicious and unauthorized third parties. These include hackers and other entities who break protocols and enter the system inappropriately.

Balancing the two Threats

There is the need for a conscious approach to be employed to ensure that the threats of all the different aspects of a given company's information systems and other IT risks are handled appropriately and prevented from going overboard or becoming negative in outlook

System Risk Assessment: Every system has its physical and IT risks. There are bugs and other risks and threats that can be identified by conducting an audit. This should be done to review the physical issues and other software matters that could prove to be problematic. Through this, there should be a method of documenting possible risks and issues with the information system of the company in question.

Fault Follow up: Where there are issues and other problems found in the system and physical environment, there must be a documentation of this report and it should be added to the risks that are identified within the system. This should help to provide a broad framework for risk management.

Draw an IT and Physical Risk Plan: Where the broad framework of risks are identified, there must be a blueprint for formulating solutions to these risks. This could include amongst other things, a set of solutions and back up plans as well as detection plans and systems. These detection and resolution systems must be deduced and options evaluated in order to choose the best systems and processes.

Implementation of IT and Physical Risk Plan: The plan must be formulated and this must include amongst other things, putting in place detection measures and physical risk prevention. There must also be the implementation of various access controls and other integrity breach prevention mechanisms to ensure that the existing system is not compromised. In cases where there are compromises and risks are actualized, there must be a system of early response to ensure that all these risks are identified and handled promptly.

Education of Personnel: The workers will have to be educated about the new risk management systems. They must understand the framework of the risks and help in monitoring and detecting risks in order to control these systems and prevent them from being breached.

Monitoring of the System: There must be the proper monitoring and care of the system in order to identify important trends and issues and also resolve all these problems in a timely manner.

Conclusion

This research has shown that physical IT risks include the risks with hardware and the risks in the premises and other environmental factors that can affect hardware. There are also risks with software which includes access controls and external attacks. The study identifies that a firm can achieve the best results by using strategic approach to draw an IT risk framework, implement it and monitor it.

Bibliography

Bidgoli, H. (2014). Handbook of Information Security, Threats, Vulnerabilities, Prevention. Hoboken, NJ: John Wiley and Sons.

Landoll, D. (2014). The Security Risk Assessment Handbook: A Complete Guide for Performing. New York: CRC Press.

Merkow, M. S., & Breithaup, J. (2014). Information Security: Principles and Practices. London: Pearson.

Tipton, H. F., & Kraus, M. (2010). Information Security Management Handbook. New York: CRC Press.

Vacca, J. R. (2010). Computer and Information Security Handbook. Indianapolis, IN: Newnes Publishing.