Name : Rizqi Zamzami Jamil

Class : SIB-4C

NIM : 2141762089

Lab - Risk Management

Introduction

An organization's process of identifying and assessing risk is a continuous effort because types of threats change and they never completely disappear. The goal of risk management is to reduce these threats to an acceptable level. There are different levels of risk management. Organizations must properly manage risk to protect information and information systems. Risk management also helps to prevent legal actions, interruptions to operations, and safeguards the organizations' reputations.

Objectives

Explore the Risk management process.

Part 1: Explain Risk Action Levels

Part 2: Explain Risk Management Concepts

Part 3: Explain Risk Management Processes

Required Resources

PC or mobile device with internet access

Instructions

Part 1: Risk Action Levels

Risk management is the identification, evaluation, and prioritization of risks. Organizations manage risk in one of four ways. Each may be an appropriate choice, depending on the circumstances and type of risk in question:

- **Avoidance (Elimination)** - Risk avoidance is the complete removal or elimination of risk from a specific threat. For example, avoiding or eliminating the threat of users sharing or misusing passwords could involve implementing a fingerprint authentication system on all user workstations.
- **Mitigation (Reduction)** - Risk mitigation involves implementing controls that allow the organization to continue to perform an activity while using mechanisms to reduce the risk from a particular threat. An organization could also increase its technical controls and network oversight to reduce risk from operational threats.
- **Transfer** - Organizations can transfer risk from specific threats. The financial risk of a threat can be managed by purchasing an insurance policy, or hiring a contractor to deal with specific threats.
- **Accept** - Accepting risk involves the identification of the threats but not implementing mitigation processes only after a conscious decision has been made to do so. The conscious decision is informed by analyzingthe various components of the risk before proceeding.

Step 1: Manage risk.

In this Step, you will describe examples of managing risk associated with specific threats to the organization's information or information systems.

a. An organization is regularly required to handle sensitive customer information. The release of this information poses a serious risk to the organization.

Question:

What steps could the organization implement to eliminate the risk associated with accidental emailing or transferring of this information?

Answer:

Implement data loss prevention (DLP) software to automatically detect and block sensitive information in outgoing emails. Enforce encryption for all sensitive data transfers and implement strict access controls.

b. The organization has had several issues of employees sharing passwords or using weak passwords.

Questions:
Name two ways to mitigate this risk.

Answer:
Implement multi-factor authentication (MFA) and biometric verification for all user accounts. Enforce strong password policies with regular password changes and complexity requirements.

Give two examples of an organization transferring risk.

Answer:
Purchase cybersecurity insurance to cover potential data breach costs and financial losses. Hire a third-party security company to handle security monitoring and incident response.

Step 2: Explore risk levels.

An organization's process of identifying and assessing risk is a continuous effort because types of threats change and they never completely disappear. The goal of risk management is to reduce these threats to an acceptable level.

Perform an internet search using the following terms: negligence, due care, and due diligence to answer the following questions:

Question:
What is negligence? Give an example of the consequences of negligence.

Answer:
Negligence is the failure to exercise reasonable care that results in harm or damage to another party. An example consequence would be facing legal liability and financial penalties for failing to protect customer data.

Define due care and due diligence and explain the difference between these two terms.

Answer:
Due care involves taking reasonable steps to protect assets and meet security requirements, while due diligence is the continuous process of maintaining and monitoring those security measures. The main difference is that due care refers to the initial implementation of security measures, whereas due diligence involves ongoing assessment and maintenance.

Part 2: Risk Management Concepts

Risk management is a technique used to identify and assess factors that may threaten information and information systems. The study of risk analysis includes several commonly used terms and concepts, including the following:

Assets – Assets are anything of value that is used in and is necessary for completion of a business task. Assets include both tangible and intangible items such as equipment, software code, data, facilities, personnel, market value and public opinion. Risk management is all about protecting valued organizational assets.

Threats – Threats are a malicious act or unexpected event that damages information systems or other related organizational assets. They can be intentional actions that result in the loss or damage to an asset. Threats can also be unintentional like an accident, natural disaster, or equipment failure.

Vulnerability – Vulnerabilities are any flaw or weakness that would allow a threat to cause harm and damage an asset. Examples could be fault code, misconfigurations, and failure to follow procedures.

Impact - Risk impact is the damage incurred by an event which causes loss of an asset or disruption of service. This damage can be measured quantitatively or qualitatively based on the impact to the organization's operations.

Risk – Risk is the probability of loss due to a threat to an organization's assets.

Countermeasures – Countermeasures are an action, device, or technique that reduces a threat or a vulnerability by eliminating or preventing it. An example would be antivirus software, firewalls, policies, and

training.

Risk Assessment – Risk assessment is the process of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls.

What is a security risk assessment? A risk assessment identifies, quantifies, and prioritizes the risks and vulnerabilities in a system. A risk assessment identifies recognized threats and threat actors and the probability that these factors will result in an exposure or loss.

Case Study:

A business manages a customer database that tracks online purchases of the products. These purchases are made with PayPal accounts or credit cards. The database server has several vulnerabilities. The database is on a server in the server room at the company headquarters. The server cost $25,000. The database consists of all 40,000 customers and over 1.5 million transactions. The server records over 120 transaction per day generating over 25K per day in sales. The data base is backed up daily at 2AM. All orders are also tracked and logged on separate systems in case of server failure. This process can take up to 50-person hours of entry to manually process every day.

Questions:

Name at least two types of vulnerabilities the cybersecurity staff should analyze:

Answer:
Outdated server software with unpatched security vulnerabilities. Physical access control vulnerabilities in the server room.

Describe possible threats to the server based on the vulnerabilities you identified:

Answer:
Cyber attackers could exploit unpatched software vulnerabilities to gain unauthorized access to the database. Unauthorized personnel could physically access the server room and compromise the system.

Describe the impact to the organization due to the following threats:

Data Breach:

Answer:
Exposure of customer payment information and personal data could lead to legal liability and regulatory fines. The organization would face significant reputational damage and potential loss of customer trust.

Ransomware:

Answer:
The organization would lose access to critical customer data and daily transaction processing capabilities. Direct financial losses would include ransom payment consideration and lost sales of $25K per day.

Hardware failure:

Answer:
Server downtime would require 50 person-hours per day for manual order processing. The organization would need to spend $25,000 to replace the failed server hardware.

List one **countermeasure** for the following threats to the organization's database server:

Data Breach:

Answer:
Implement end-to-end encryption for all customer data and transactions. Regular security audits and vulnerability assessments should be conducted.

Ransomware Attack:

Answer:
Maintain secure, offline backups of the database with regular testing of restoration procedures. Implement advanced endpoint protection and email filtering systems.

Hardware Failure:

Answer:
Install redundant server hardware in a high-availability configuration. Implement automated failover capabilities to the backup systems.

Malware:

Answer:
Deploy next-generation antivirus software with real-time monitoring and threat detection. Implement network segmentation and strict access controls.

Part 3: Risk Management Processes

Risk management is a formal process that reduces the impact of threats and vulnerabilities. You cannot eliminate risk completely, but you can manage risk to an acceptable level. Risk management measures the impact of a threat and the cost to implement controls or countermeasures to mitigate the threat. All organizations accept some risk. The cost of a countermeasure should not be more than the value of the asset you are protecting.

Step 1: Frame and Assess Risk

Identify the threats throughout the organization that increase risk. Threats identified include processes, products, attacks, potential failure, or disruption of services, negative perception of organization's reputation, potential legal liability, or loss of intellectual property.

After a risk has been identified, it is assessed and analyzed to determine the severity that the threat poses. Some threats can bring the entire organization to a standstill while other threats are minor inconveniences. Risk can be prioritized by actual financial impact (quantitative analysis) or a scaled impact on the organization's operation (qualitative analysis).

In our example, the following vulnerabilities have been identified. Assign a quantitative value to each risk based on your committee answers. Provide justification for the value you determined.

Question:

Use the case study to formulate your answers.

Data breach impacting all customers:

Answer:
The quantitative value would be approximately $4 million, considering regulatory fines and potential legal settlements. This calculation includes $100 per affected customer for 40,000 customers.

Server hardware failure requiring hardware replacement:

Answer:
The quantitative value would be $50,000, including $25,000 for new hardware and $25,000 in lost daily sales. Additional costs include 50 person-hours of manual processing per day.

Ransomware affecting the entire server database:

Answer:
The quantitative impact would be $100,000, including potential ransom payment and lost sales during recovery. The value includes costs for incident response and system restoration.

Server room flood caused by fire sprinklers being activated:

Answer:

The estimated impact would be $75,000, including water damage to server hardware and potential data loss. This includes cleanup costs and temporary service disruption.

Step 2: Respond to Risk

This step involves developing an action plan to reduce overall organization risk exposure. Management ranks and prioritizes threats; a team then determines how to respond to each threat. Risk can be eliminated, mitigated, transferred, or accepted.

Question:

Rank the vulnerabilities and propose possible countermeasure for each threat.

Data breach impacting all customers:

Answer:
Implement database encryption and access controls as highest priority measures. Regular security audits and employee training should be conducted.

Server hardware failure requiring hardware replacement:

Answer:
Install redundant hardware systems and implement automated failover procedures. Establish preventive maintenance schedules and monitoring systems.

Ransomware affecting the entire server database:

Answer:
Deploy advanced threat protection and maintain secure offline backups. Implement network segmentation and user access controls.

Server room flood caused by fire sprinklers being activated:

Answer:
Install water detection systems and relocate critical servers to a higher elevation. Implement a water-based fire suppression alternative system.

Step 3: Monitor Risk

Continuously review risk reductions due to elimination, mitigation, or transfer actions. Not all risks can be eliminated, so threats that are accepted need to be closely monitored. It is important to understand that some risk is always present and acceptable. As countermeasures are implemented, the risk impact should decrease. Constant monitoring and revisiting new countermeasures are required.

Question:

What actions could decrease the impact of a ransomware threat?

Answer:
Maintain daily offline backups and regularly test restoration procedures. Implement employee security awareness training and email filtering systems.