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 analyzing the various components of the risk before proceeding.

TASK 1

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 1

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

ANSWER

The organization can implement a policy prohibiting employees to email or transfer any customer data. The organization could also prevent employees from accessing this information. The organization could also screen and block all the data emailed or transferred from organization’s network.

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

QUESTION 2

Name two ways to mitigate this risk.

ANSWER

- Use of strong password on all organizational systems
- Implement password policies and guidelines

QUESTION 3

Give two examples of an organization transferring risk.

ANSWER

- Use of insurance
- Outsourcing security risks to third party company

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 4

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

ANSWER

Negligence means that no actions or controls are taken to lower risk. The threat is very high, and the cost of an incident could be catastrophic and can lead to criminal charges.

An employee forgets to update antivirus software on their company laptop. As a result, the device gets infected with malware, leading to a data breach. The organization suffers **financial loss**, **reputation damage**, and **legal consequences**.

****QUESTION 5****

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

****ANSWER****

Due Care: Taking reasonable steps to protect people or data. It's about acting responsibly and doing what is expected to avoid harm. Example: Setting a strong password policy for all employees.

Due Diligence: The process of investigating, reviewing, and analyzing risks before taking actions. It's about evaluating the situation to make informed decisions. Example: Checking the security practices of a third-party vendor before signing a contract.

Due Care	Due Diligence
Action taken to protect from risks	Research and assessment before taking action
Reactive (you do it after understanding the risk)	Proactive (you investigate before risk happens)
Doing the right thing	Checking before doing anything

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.

TASK 2

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.

QUESTION 1

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

Physical Security Vulnerabilities: lack of physical access control, risks of natural disaster

Network Security Vulnerabilities: open port, lack of encryption, weak firewalls rule

QUESTION 2

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

ANSWER

Threats to the server include hardware crash based on equipment failing, a data breach or ransomware attack, fire, tornado, hurricane, earthquake, system corrupted or damage due to malware or system failure or poor performance due to misconfigurations.

QUESTION 3

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

ANSWER

Data Breach: loss of data, reputation damage, loss of customer trust, legal penalties

Ransomware: loss of access to the required data and information, disruption in normal business operation

Hardware failure: loss of database server, high cost of recovering hardware

QUESTION 4

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

ANSWER

Data Breach: implement policies regarding access control and data encryption, conduct employee training regarding security policies and standards

Ransomware Attack: have backup files, install strong firewall rules and antivirus software

Hardware Failure: use redundant hardware, regular backups, consistent monitoring

Malware: install antivirus software, update OS and software application, monitoring

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.

TASK 3

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).

QUESTION 1

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. Use the case study to formulate your answers.

ANSWER

Data breach impacting all customers: The impact of a data breach could cost $100,000 or more and 5 working days to restore the data.

Breakdown:

40,000 customers' data could be stolen.
→ May cost about $20–$50 per customer to fix the damage (credit monitoring, legal help).
→ Total = around $800,000 to $2,000,000.

Loss of daily sales
→ Business makes $25,000 per day.
→ If system is down for 5 days = $125,000 lost.

Extra manual work
→ 50 person-hours/day to handle orders manually.
→ Cost = around $1,000 to $5,000.

Server hardware failure requiring hardware replacement: The impact of hardware failure could cost $5,000 or more and 2 working days to replace failed hardware.

Ransomware affecting the entire server database: The impact of ransomware attack could cost $20,000 or more and 5 working days to restore the data and remove the ransomware.

Server room flood caused by fire sprinklers being activated: The impact of the flood could cost $50,000 or more and 3 working days to replace damaged hardware and restore the data.

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 2****
Rank the vulnerabilities and propose possible countermeasure for each threat.

****ANSWER****

Data breach impacting all customers: The impact of a data breach is high. It could cost $100,000 or more and the customer trust and company reputation. Some of countermeasures can be employee training, data encryption, and software and hardware updates.

Server hardware failure requiring hardware replacement: The impact of server hardware failure is medium that could cost $5,000 or more and service disruption. Some of countermeasures can be data and system backups.

Ransomware affecting the entire server database: The impact of ransomware attack is low that could cost $20,000 or more. It could cause service disruption and data loss. Some of the countermeasures can be security training and data backup.

Server room flood caused by fire sprinklers being activated: The impact of ransomware attack is low that could cost $50,000 or more. It could cause service disruption and data loss. Some of the countermeasures can be purchase insurance and back up data.

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 3

What actions could decrease the impact of a ransomware threat?

ANSWER

1. Regular Data Backups: If ransomware locks files, we can restore them from a clean backup without paying the ransom.

2. Employee Awareness Training: Staff learn to avoid clicking on suspicious links or downloading unknown attachments, which are common ways ransomware spreads.

3. Keep Software Updated (Patching): Fixes known security holes that ransomware can exploit to infect systems.