Nama : Sasmita Rachmawati

Absen : 15

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.

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:

To eliminate the risk associated with accidental emailing or transferring sensitive customer information, the organization could:

- **Implement Data Loss Prevention (DLP) systems to automatically detect and block sensitive data transfers, whether through email or other file transfer methods.**
- **Restrict access to sensitive customer information to only essential personnel, minimizing the chance of accidental exposure.**
- **Enforce policies and training on handling sensitive data, ensuring that employees understand the risks and proper procedures.**
- **Use encryption for sensitive data so that even if it is accidentally sent, it remains protected from unauthorized access.**

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

Questions:

Name two ways to mitigate this risk.

Answer:

To mitigate the risk of employees sharing passwords or using weak passwords, the organization could:

- **Enforce a strong password policy requiring complex, regularly updated passwords.**
- **Implement multi-factor authentication (MFA) for an additional layer of security, reducing reliance on passwords alone.**

Give two examples of an organization transferring risk.

Answer:

1. **Purchasing cybersecurity insurance to cover potential financial losses from data breaches or cyber-attacks.**
2. **Outsourcing specific IT functions to a third-party provider with a service-level agreement (SLA) that transfers responsibility for certain security risks, such as system uptime or data recovery, to the contractor.**

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.

Questions:

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

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

Answer:

Negligence is the failure to take necessary actions to prevent risks, often by ignoring potential threats or not implementing controls. For example, if an organization fails to install antivirus software on its systems, it could lead to a severe malware attack, resulting in significant financial losses, data breaches, and possibly legal consequences.

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

Answer:

- **Due Care involves taking reasonable steps to reduce risk to an acceptable level, such as implementing basic security measures. The organization acknowledges risks but takes action to lower them.**
- **Due Diligence goes further by implementing comprehensive measures to actively manage and mitigate risks. This may involve ongoing monitoring and updating of security measures.**

Difference: Due care is about responsible actions to lower risk, while due diligence is about thoroughly managing and preventing risks by continuous efforts and proactive controls.

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:

Cybersecurity staff should examine vulnerabilities including:

- **Hardware Failure Risks: Aging or overused hardware components that may fail.**
- **Software Misconfigurations: Incorrect server or database settings that could create security gaps.**
- **Malware Risks: Potential infection through unprotected network access or lack of endpoint security.**

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

Answer:

- **Hardware Failures: Risk of equipment crashing, leading to data access loss and potential sales interruptions.**
- **Malware Attacks: Possibility of a malware infection that corrupts data or disrupts server functionality.**
- **Natural Disasters: Events such as floods or fires that could damage the physical server.**

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

- Data Breach:

Answer:

Data Breach: A data breach could cause the complete loss of sensitive customer information, harming the organization's reputation and potentially resulting in financial and legal repercussions.

- Ransomware:

Answer:

Ransomware: Could lead to a complete shutdown of operations, revenue loss, and additional costs for data recovery.

- Hardware failure:

Answer:

Hardware Failure: Server downtime could disrupt daily sales and reduce revenue, with additional resource allocation needed for manual processing, potentially damaging the organization’s reputation.

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

- Data Breach:

Answer:

Data Breach: Implement data encryption, regular employee training on data protection policies, and access restrictions based on roles.

- Ransomware Attack:

Answer:

Ransomware Attack: Ensure regular data backups, use of updated antivirus/antimalware solutions, and enforce strict access policies.

- Hardware Failure:

Answer:

Hardware Failure: Set up hardware redundancy, maintain a maintenance schedule, and promptly replace outdated equipment.

- Malware:

Answer:

Malware: Use antivirus and antimalware software, enforce regular updates for systems and applications, and control physical access to critical systems.

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:

Impact Assessment: Estimated cost could reach $100,000 or more in financial impact and require approximately 5 working days for data restoration. The high cost and recovery time are justified by the sensitivity of customer data, potential reputational damage, and legal repercussions.

- Server hardware failure requiring hardware replacement:

Answer:

Impact Assessment: Estimated cost around $5,000 and 2 working days to replace and restore failed hardware. The hardware replacement and downtime costs are moderate, reflecting the expense of equipment and disruption to operations.

- Ransomware affecting the entire server database:

Answer:

Impact Assessment: Estimated cost could reach $20,000 or more, with about 5 working days needed to remove the ransomware and restore the data. This estimate includes the potential downtime, restoration expenses, and security intervention needed to prevent reoccurrence.

- Server room flood caused by fire sprinklers being activated:

Answer:

Impact Assessment: Estimated financial impact of $50,000 and 3 working days to replace damaged hardware and restore data. The estimate accounts for extensive equipment repair/replacement, water damage, and potential downtime.

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:

- **Risk Ranking: High**
- **Countermeasures: Regular employee training to recognize security threats, data encryption to protect sensitive information, and software and hardware updates to address vulnerabilities. These actions reduce the likelihood of a breach and the potential for data exposure.**

- Server hardware failure requiring hardware replacement:

Answer:

- **Risk Ranking: Medium**
- **Countermeasures: Regular data and system backups to minimize data loss, and periodic hardware maintenance and replacement schedule to ensure reliable functioning. These actions can reduce downtime and facilitate faster recovery in case of a failure.**

- Ransomware affecting the entire server database:

Answer:

- **Risk Ranking: Low to Medium**
- **Countermeasures: Implement security training to enhance awareness of phishing attacks, ensure frequent data backups to safeguard against data loss, and establish anti-malware software on all systems. These measures help prevent ransomware infection and ensure data can be restored if an attack occurs.**

- Server room flood caused by fire sprinklers being activated:

Answer:

- **Risk Ranking: Low to Medium**
- **Countermeasures: Consider insurance policies to cover damages, maintain regular data backups stored off-site, and install flood sensors to alert for water leakage. These actions minimize both the financial impact and data loss in the event of water damage.**

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:

- **Regular Backups: Implementing regular backups ensures that, in case of a ransomware attack, the organization can restore recent data with minimal loss. Backups should be stored securely, separate from the main system.**
- **Anti-Malware Software: Up-to-date anti-malware software can detect and block ransomware before it encrypts files, reducing the likelihood of a severe impact.**
- **Employee Training: Conduct training sessions to help employees identify phishing emails and other social engineering tactics commonly used in ransomware attacks, decreasing the chance of accidental infection.**

By regularly monitoring the effectiveness of these measures and updating them as needed, the organization can reduce its vulnerability to ransomware and minimize disruption if an attack occurs.