Nama : Winda Umi Fatimatus Sa'diyah

NIM : 2141762055

Absen : 19

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.

Lab - Risk Management

Question:

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

- Create and enforce a strict policy that forbids employees from emailing or transferring sensitive customer data without proper authorization.
- Implement role-based access controls to limit access to sensitive information to only those employees who need it for their work.
- Utilize advanced data loss prevention (DLP) technologies that monitor and restrict the transmission of sensitive information outside the organization's network.

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

Questions:

Name two ways to mitigate this risk.

- Establish a strong password management policy that requires all employees to create complex passwords and mandates regular password changes.
- Implement two-factor authentication (2FA) across all organizational systems to add an extra layer of security, reducing the chances of unauthorized access.

Give two examples of an organization transferring risk.

- Purchasing cybersecurity insurance to cover potential financial losses arising from data breaches or other security incidents.
- Partnering with third-party security firms to outsource certain security functions, allowing those firms to manage risk on behalf of the organization.

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.

- Negligence refers to a failure to take appropriate actions or precautions to mitigate risks. For instance, if a company neglects to implement basic security protocols and a data breach occurs, it may face severe legal repercussions, including lawsuits and fines, as well as damage to its reputation.

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

- Due care involves taking prudent measures to manage and lower risks to an acceptable level, acknowledging that while risks still exist, the organization is doing its part to mitigate potential losses. Due diligence, on the other hand, refers to the ongoing responsibility to investigate and implement effective risk management practices, ensuring that reasonable safeguards are in place to prevent risks from materializing. The key difference is that due care is about reasonable actions taken, whereas due diligence emphasizes the active pursuit of risk elimination and assessment.

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. **Lab - Risk Management**

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:

- Network **vulnerabilities:** These could include unpatched software, open ports, and weak firewall configurations that could be exploited by external attackers.
- Human **factors:** This involves social engineering risks such as phishing attacks that could lead to compromised credentials or insider threats from employees.

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

- **Unauthorized access:** Due to network vulnerabilities, attackers might gain unauthorized access to sensitive data, leading to data breaches or data manipulation.
- **Social engineering attacks:** If employees are targeted through phishing, they may inadvertently provide access to the server, resulting in data theft or unauthorized actions.

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

- A data breach could result in significant financial losses due to potential fines and legal fees. It could also lead to the loss of customer trust, resulting in decreased sales and customer retention. Moreover, the organization may incur costs related to notifying affected customers and implementing remediation measures.

Ransomware:

- The impact of a ransomware attack could be severe, as it may render the database inaccessible until a ransom is paid, resulting in operational disruptions and lost revenue during downtime. Additionally, the organization could face reputational damage if customers' data is compromised or if they perceive the organization as incapable of safeguarding their information.

Hardware failure:

- Hardware failure could lead to system outages, causing interruptions in transaction processing and potential loss of revenue from halted sales. The recovery from such failures could be time-consuming and resource-intensive, as data recovery efforts might be necessary, impacting business operations and leading to a backlog of orders that require manual entry..

Lab - Risk Management

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

- One effective countermeasure against data breaches is the implementation of **data loss prevention (DLP) tools** that monitor and control data transfers within and outside the organization, helping to prevent unauthorized access and leaks of sensitive information.

Ransomware Attack:

- To combat ransomware attacks, organizations can deploy **intrusion detection systems (IDS)** that monitor network traffic for suspicious activity and potential threats, allowing for quick detection and response to prevent malware from infiltrating systems.

Hardware Failure:

- A proactive countermeasure for hardware failure is the establishment of a **comprehensive maintenance schedule** that includes regular hardware assessments and timely upgrades or replacements of aging components to ensure reliability and performance.

Malware:

- Implementing a robust **security awareness training program** for employees can serve as a countermeasure against malware, educating them on recognizing phishing attempts, unsafe downloads, and other risky behaviors that can lead to malware infections.

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:

Lab - Risk Management

Server hardware failure requiring hardware replacement:

- **Quantitative Value Assignment: $30,000**
  Justification:

- **Ransom Payment:** The organization may face a ransom demand that could exceed **$20,000** to regain access to encrypted data.
- **Restoration Costs:** Beyond the ransom, restoring the database and ensuring it is free from ransomware could require 5 working days, resulting in an estimated revenue loss of **$125,000** (5 days x $25,000/day).
- **Mitigation Expenses:** Additional costs for cybersecurity professionals to analyze the breach and secure the system may add another **$5,000** to the total.

Total Estimated Impact: Combining the replacement costs, lost revenue, and labor costs, the total impact from server hardware failure is approximately **$10,000**.

Ransomware affecting the entire server database:

- **Threat: Ransomware Affecting the Entire Server Database**
  Quantitative Value Assignment: $30,000
  Justification:

1. **Ransom Payment:** The organization may face a ransom demand that could exceed **$20,000** to regain access to encrypted data.
2. **Restoration Costs:** Beyond the ransom, restoring the database and ensuring it is free from ransomware could require 5 working days, resulting in an estimated revenue loss of **$125,000** (5 days x $25,000/day).
3. **Mitigation Expenses:** Additional costs for cybersecurity professionals to analyze the breach and secure the system may add another **$5,000** to the total.

Total Estimated Impact: The combined costs from ransom payment, lost revenue, and mitigation expenses could total approximately **$30,000**.

Server room flood caused by fire sprinklers being activated:

- **Threat: Server Room Flood Caused by Fire Sprinklers Being Activated**
  Quantitative Value Assignment: $75,000
  Justification:

1. **Damage Costs:** The cost to replace damaged hardware due to flooding can exceed **$50,000**, considering the extensive nature of server components that may need replacement.
2. **Data Recovery Costs:** Even with daily backups, there could be additional costs involved in restoring lost data, which may amount to another **$20,000**.
3. **Operational Downtime:** The impact of being unable to conduct business for 3 working days could result in an estimated lost revenue of **$75,000**.

Total Estimated Impact: The overall financial impact of a server room flood could be around **$75,000**, taking into account hardware replacement, data recovery, and lost sales.

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:

- **Impact Ranking: High**
- **Potential Cost: $100,000 or more**
- **Countermeasures:**
  - **Employee Training:** Implement regular security awareness training to educate employees on data handling and phishing risks.
  - **Data Encryption:** Utilize encryption for sensitive customer information both at rest and in transit to protect against unauthorized access.
  - **Access Controls:** Enforce strict access controls to limit employee access to sensitive data based on role necessity.
  - **Incident Response Plan:** Develop and maintain an incident response plan to quickly address any potential breaches.

Server hardware failure requiring hardware replacement:

- **Impact Ranking:** Medium
- **Potential Cost: $10,000 or more**
- **Countermeasures:**
  - **Regular Maintenance:** Schedule routine hardware checks and maintenance to identify and address potential issues before failure occurs.
  - **Redundancy:** Implement hardware redundancy (e.g., RAID configurations, backup servers) to minimize downtime during hardware replacement.
  - **System Backups:** Ensure regular backups are taken to prevent data loss in the event of hardware failure.
  - **Inventory Management:** Keep an inventory of critical spare parts to expedite hardware replacement.

Ransomware affecting the entire server database:

- **Impact Ranking:** Medium
- **Potential Cost: $20,000 or more**
- **Countermeasures:**
  - **Antivirus and Antimalware Software:** Deploy and regularly update antivirus and antimalware solutions to detect and prevent ransomware attacks.
  - **Data Backups:** Maintain regular, secure backups of the database and test restore processes to ensure data can be recovered quickly.
  - **User Education:** Conduct training sessions focused on recognizing phishing attempts and safe internet practices to minimize infection risk.
  - **Network Segmentation:** Implement network segmentation to limit ransomware spread if an infection does occur.

Server room flood caused by fire sprinklers being activated:

- **Impact Ranking:** Medium
- **Potential Cost: $50,000 or more**
- **Countermeasures:**
  - **Insurance Coverage:** Purchase comprehensive insurance that covers water damage to hardware and data loss due to flooding.

- **Flood Mitigation:** Install flood barriers or drainage systems to prevent water from entering the server room.
- **Offsite Backups:** Maintain offsite backups to ensure data can be recovered in the event of physical damage to the primary server.
- **Environment Monitoring:** Use sensors to monitor environmental conditions such as humidity and temperature, and implement alerts for any anomalies

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

Lab - Risk Management

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?

- **Regular Data Backups**
  Explanation: Implementing a robust data backup strategy ensures that critical data is regularly backed up to secure, offsite locations. By maintaining frequent backups, the organization can quickly restore data from a point prior to the ransomware attack, minimizing data loss and operational disruption. This countermeasure effectively reduces the impact of ransomware, as it provides a means to recover without having to pay the ransom.
- **Endpoint Detection and Response (EDR) Solutions**
  Explanation: Deploying advanced EDR solutions allows for real-time monitoring and response to suspicious activities on endpoints. These tools utilize machine learning and behavioral analysis to detect ransomware behavior, such as unusual file encryption patterns or rapid file modifications. By identifying and isolating potential threats before they can cause significant damage, EDR solutions help to mitigate the impact of ransomware on the organization's systems.
- **User Training and Awareness Programs**
  Explanation: Conducting regular training sessions for employees on recognizing phishing attempts and safe internet practices can significantly reduce the likelihood of a successful ransomware attack. Educating staff about the dangers of opening suspicious emails, clicking on unknown links, and downloading unverified attachments empowers them to act as the first line of defense against ransomware. By minimizing human error, this countermeasure helps to decrease the risk of infection and, consequently, the impact of any potential ransomware threats