NAMA	**: ANISATUL LATIFAH**
NIM	**: 2141762008**
ABSEN	**: 01 (SATU)**
KELAS	**: SIB – 4C**

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.

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 from emailing or transferring any customer data. Additionally, the organization could restrict access to sensitive information to only authorized personnel. To further reduce risk, the organization could screen and block all outgoing data that is emailed or transferred from the organization's network using Data Loss Prevention (DLP) tools. Regular employee training on data security could also be implemented to minimize human errors.

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

Name two ways to mitigate this risk.

Answer :

1. Implement strong organization password policies and guidelines, such as requiring complex passwords that include letters, numbers, and special characters.
2. Enforce the use of strong passwords on all organizational systems, and introduce Multi-Factor Authentication (MFA) to add an extra layer of security beyond just the password.

Give two examples of an organization transferring risk.

Answer :

1. The organization can purchase a cybersecurity insurance policy to manage the financial impact of a data breach or other cyber threats. This transfers the financial risk to the insurance provider.
2. Hiring a third-party contractor to handle specific areas, such as network security or system monitoring, can transfer operational risks to the contractor as outlined in a Service Level Agreement (SLA).

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:

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

Answer :

Negligence refers to a failure to take appropriate actions or precautions to reduce risk. It occurs when an organization ignores potential threats and does not implement necessary controls or policies to mitigate those risks. As a result, the threat level remains high, and the organization is exposed to significant danger.

Example:

If a company neglects to update its antivirus software, it could fall victim to a malware attack. The consequences of this negligence could include data breaches, financial loss, reputational damage, or even legal liabilities if sensitive customer data is compromised. In some cases, negligence can lead to criminal charges, especially if the organization is responsible for protecting sensitive or regulated data.

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

Answer :

- Due Care: This refers to the reasonable actions an organization takes to reduce the level of risk. While the risks are not completely eliminated, the organization implements sufficient controls to minimize potential damage. Due care focuses on taking responsible steps to ensure risks are kept to an acceptable level.
- Due Diligence: This refers to the steps an organization takes to actively investigate and assess potential risks before they arise. It involves continuous monitoring and implementing controls to prevent incidents. Due diligence is about being proactive in ensuring that the organization is fully informed and prepared for potential risks.

Difference:

- Due Care is about responding to risks by taking reasonable actions to manage them (reactive approach).
- Due Diligence is about actively researching, identifying, and preventing risks before they materialize (proactive approach).

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 :

1. Hardware Failure: The server could fail due to aging or faulty hardware components, which would disrupt the processing and storage of transactions.
2. Cyber Attacks: The database server may be vulnerable to attacks from hackers, such as data breaches, ransomware, or malware, especially if it lacks updated security patches or configurations.

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

Answer :

1. Hardware Failure: A potential threat could be the server's hard drive crashing, leading to a complete loss of data if backups are insufficient or outdated. This could halt operations and lead to financial losses.
2. Cyber Attacks: The server could be targeted by hackers attempting to breach sensitive customer data or inject ransomware, which would encrypt the data and demand payment for its release.

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

- **Data Breach:**

Answer :

A data breach could lead to the exposure of sensitive customer information, damaging the organization's reputation, and resulting in legal liabilities or fines. This could also cause a significant drop in customer trust, impacting sales and revenue for an extended period. Financial losses could be substantial, possibly exceeding $100,000, and require weeks to fully recover.

- **Ransomware:**

Answer :

A ransomware attack could encrypt the entire database, preventing access to critical customer and sales information. This could cause an extended shutdown of operations, potentially halting all sales and costing the business upwards of $20,000 per day. The ransom payment, recovery efforts, and system restoration could take days or even weeks.

- **Hardware failure:**

Answer :

A hardware failure, such as a server crash, could stop transaction processing and result in downtime, loss of data, and missed revenue opportunities. The company could lose $25,000 per day, and the repair costs for hardware could exceed $5,000, requiring a minimum of 2 days for full restoration.

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

- **Data Breach:**

Answer :

Implement strong encryption methods to protect customer data, both at rest and in transit. Additionally, regularly update software and hardware security patches to mitigate vulnerabilities that could be exploited by attackers.

- **Ransomware Attack:**

Answer :

Ensure regular data backups are taken and stored securely offsite, so the organization can quickly restore data in the event of a ransomware attack. Training employees on phishing and social engineering threats would also help prevent ransomware infections.

- Hardware Failure:

Answer :

Establish a hardware redundancy system, such as using a mirrored server setup, to ensure continuity of operations in the event of a hardware failure. Regular maintenance and hardware updates would also help prevent such failures.

- Malware:

Answer :

Deploy comprehensive antivirus and antimalware solutions on the server and continuously monitor for unusual activity. Keeping all systems updated and conducting regular malware scans will help in detecting and preventing 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.

Use the case study to formulate your answers.

- **Data breach impacting all customers:**

Answer :

The impact of a data breach could cost $100,000 or more. This includes legal fees, notification costs, potential lawsuits, and the time required to regain customer trust. Recovery may take at least 5 working days to restore operations and data, along with reputational damage that could have a long-term effect on sales.

- **Server hardware failure requiring hardware replacement:**

Answer :

A server hardware failure could cost $5,000 or more in equipment replacement. Recovery might take up to 2 working days, considering the time to replace the hardware and restore backups. During this time, the business could lose revenue due to transaction delays.

- **Ransomware affecting the entire server database:**

Answer :

A ransomware attack could result in costs exceeding $20,000. This includes ransom payments (if made), recovery efforts, and data restoration. It could take 5 working days or more to fully recover the data and resume normal operations, with additional costs for updating security protocols.

- **Server room flood caused by fire sprinklers being activated:**

Answer :

A server room flood could cost $50,000 or more due to water damage to hardware and the need to replace and restore systems. Recovery could take 3 working days to replace damaged equipment and restore backups, leading to lost revenue and productivity.

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 :

This risk is high. It could cause significant financial losses and damage the company's reputation. Countermeasures include employee training on cybersecurity best practices, implementing encryption for sensitive data, and regularly updating software to fix vulnerabilities.

- **Server hardware failure requiring hardware replacement:**

Answer :

This risk is medium. Although not as damaging as a data breach, it still disrupts business operations. Countermeasures include maintaining regular backups, having spare hardware available, and using redundant systems like RAID to minimize downtime.

- **Ransomware affecting the entire server database:**

Answer :

This risk is medium to high. The organization should implement data backups, strong antivirus software, and user education about phishing threats. Regular backups and testing of recovery procedures can mitigate the effects of an attack.

- **Server room flood caused by fire sprinklers being activated:**

Answer :

This risk is medium. While a flood can cause extensive damage, countermeasures such as elevating hardware off the floor, waterproofing the server room, and purchasing insurance can mitigate the financial impact.

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 :

1. Regular Backups: Ensure that critical data is backed up daily and stored securely offsite. This allows quick data restoration in case of a ransomware attack, minimizing downtime and data loss.
2. Employee Training: Conduct cybersecurity awareness training to educate employees about phishing scams and ransomware attacks. This reduces the likelihood of someone accidentally downloading malware.
3. Antivirus Software: Use updated antivirus and antimalware tools that actively scan for and remove potential ransomware threats. This adds a layer of protection and helps prevent the spread of malware.