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.

Answer:

- Implement Data Loss Prevention (DLP) solutions to monitor and block the transfer of sensitive information.
- Apply encryption to emails containing sensitive data to prevent unauthorized access.
- Introduce strict access controls limiting which employees can view or transfer customer information.

Lab - Risk Management

What steps could the organization implement to eliminate the risk associated with accidental emailing or transferring of this information?
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 data emailed or transferred from the organization's network.
b. The organization has had several issues of employees sharing passwords or using weak passwords.
Answer:

- Enforce Multi-Factor Authentication (MFA) across all critical systems.
- Implement password management tools and regularly require employees to update passwords following strong password policies.

Implement organization password policies and guidelines, enforce the use of strong passwords on all organizational system.
Give two examples of an organization transferring risk.
Answer:
Examples of transferring risk:

- Purchasing cybersecurity insurance to cover financial loss from data breaches.
- Outsourcing IT security management to a third-party service provider under a service level agreement (SLA).

Answers can vary but the use of insurance or service level agreements should be referenced.

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 the failure to take appropriate actions to reduce risks, leading to significant vulnerability. An example would be ignoring software updates, resulting in a ransomware attack that compromises sensitive data.

Define due care and due diligence and explain the difference between these two terms.
Answer:
Difference between Due Care and Due Diligence:

- Due Care is about taking reasonable measures to lower risks (e.g., securing passwords).
- Due Diligence involves consistently maintaining security measures and improving processes to protect assets over time (e.g., conducting regular audits and risk assessments).

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.

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

Answer:

Vulnerabilities the cybersecurity staff should analyze:

- Hardware misconfigurations or failures.
- Inadequate protection against malware and hacking.

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

Answer:

- Potential system crashes due to hardware failure.
- Cyber-attacks such as malware infection or hacking attempts.

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

Answer:

- Data Breach: Loss of customer data could severely damage the organization's reputation and result in legal actions or penalties.
- Ransomware: A ransomware attack can cause operational downtime, leading to significant financial losses and tarnished reputation.
- Hardware Failure: Hardware failure can interrupt daily operations, leading to loss of revenue and productivity.

Lab - Risk Management

Answers will vary. The impact could range from complete loss of the database server to impacting the sales and revenue to the organization. The impact could also include damage to the business reputation.

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

Answer:

- Data Breach: Implement regular encryption of data, enforce access control, and conduct security awareness training.
- Ransomware: Regularly back up data and maintain updated antivirus/anti-malware software.
- Hardware Failure: Ensure redundancy by having backup hardware systems and regular maintenance.
- Malware: Use firewalls, antivirus software, and keep systems patched to prevent malicious software.

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.

Answer:

- Data breach impacting all customers: The impact could be over $100,000, with long-term damage to brand trust.
- Server hardware failure: Cost approximately $5,000 to replace, with two days of downtime.
- Ransomware attack: Could cost around $20,000 with several days needed to restore systems.
- Server room flood: Estimated at $50,000 for hardware replacement and recovery of lost 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.

Rank the vulnerabilities and propose possible countermeasure for each threat.

Answer:

- Data breach: High impact, requires encryption, employee training, and updates to software security.
- Server hardware failure: Medium impact, mitigated by backups and hardware redundancy.
- Ransomware: Low to medium impact, can be mitigated by frequent backups, endpoint security, and incident response plans.
- Server room flood: Medium to high impact, countermeasures include physical protection of server rooms (e.g., fire suppression systems that don’t damage equipment), and off-site backups.