Name : Selly Amelia Putri
Class : 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.

Lab - Risk Management

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

- Create and Enforce a No-Emailing Policy for Sensitive Data: Prohibit employees from using email to share customer data, especially via external platforms, to minimize accidental exposure.
- Restrict Access to Sensitive Information: Limit access to customer data only to employees who need it for their job responsibilities, applying role-based access controls to minimize exposure.
- Implement Data Screening and Blocking: Use technology to automatically screen and block emails or file transfers that contain sensitive customer information, preventing unauthorized data leakage from the organization's network.
- Use Encryption for Approved Data Transfers: Require encryption for any authorized data transfers, ensuring the data remains protected even if accidentally misdirected.
- Deploy Data Loss Prevention (DLP) Tools: Utilize DLP software to monitor, detect, and block unauthorized attempts to transfer or share sensitive information.
- Provide Employee Training: Educate employees on data handling policies and the importance of data security, reducing the likelihood of accidental disclosures.
- Conduct Regular Security Audits: Periodically review email logs, transfer logs, and access logs to ensure compliance with data protection policies and identify any risks early.

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.

Name two ways to mitigate this risk.

- Establish and Enforce a Strong Password Policy: Require employees to use complex passwords that meet specific criteria (e.g., minimum length, inclusion of upper and lowercase letters, numbers, and special characters) and mandate regular password changes.
- Implement Multi-Factor Authentication (MFA): Require MFA on all organizational systems, adding an extra layer of security beyond passwords and reducing the risk from shared or weak passwords.

Implement organization password policies and guidelines, enforce the use of strong passwords on all organizational system.

Give two examples of an organization transferring risk.

- Purchasing Insurance: An organization can buy insurance to cover potential losses from risks such as property damage, cyber-attacks, or liability claims, thereby transferring the financial impact of these risks to the insurer.
- Utilizing Service Level Agreements (SLAs) with Vendors: By establishing SLAs with vendors or third-party providers, an organization can transfer certain operational risks (e.g., IT system uptime, data protection responsibilities) to the vendor, who is then contractually obligated to meet specified service standards.

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.
Negligence is the failure to take reasonable care or steps to prevent harm or mitigate risks when it is expected or required. In a business or organizational context, negligence occurs when proper actions or controls are not implemented to address known risks, thereby exposing the organization or others to potential harm.

Example of Consequences of Negligence: If a company fails to implement basic cybersecurity measures, such as firewalls or data encryption, and a data breach occurs, sensitive customer information may be exposed. The consequences can be severe, including financial losses, legal liabilities, reputational damage, and even regulatory fines. In extreme cases, negligence in protecting customer data could lead to criminal charges for failing to comply with data protection laws.
Answers will vary. 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.

Define due care and due diligence and explain the difference between these two terms.
Due Care refers to taking reasonable and appropriate actions to minimize risks. It involves implementing basic safeguards and controls to lower the potential impact of a risk, but it acknowledges that some level of risk remains. Due care is about acting responsibly to avoid harm by following established practices.

Due Diligence involves a thorough and proactive approach to identifying, evaluating, and addressing risks. It goes beyond due care by taking comprehensive steps to eliminate or significantly reduce risks through multiple layers of controls and continuous monitoring. Due diligence is often part of the decision-making process to ensure all possible risks are considered and mitigated.

Difference: The primary difference between due care and due diligence is in their depth and intent. Due care is about taking reasonable steps to reduce risk, while due diligence is about actively investigating and controlling risks to a higher standard, often with a focus on preventing potential losses altogether.
Answers will vary. Due care involves taking reasonable steps to lower the level of risk. The risk still exists but reasonable steps lower a potential loss. Due diligence involves responsible steps taken to eliminate risk. Some risks still exist, but multiple controls are implemented to prevent potential loss.

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.

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

- Misconfigurations: Incorrect settings or configurations on the server, database, or network devices that could expose the system to unauthorized access or attacks.
- Malware: The risk of malicious software infecting the server, which could lead to data theft, corruption, or unauthorized access by attackers.

Answers will vary. Vulnerabilities could include hardware failures, attack by hackers, natural disasters, malware, and misconfigurations.

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

- Data Breach or Unauthorized Access: Due to misconfigurations, an attacker could exploit open ports, weak access controls, or improperly configured security settings to gain unauthorized access to sensitive customer data, leading to a potential data breach.
- Malware or Ransomware Attack: The presence of malware could infect the server, allowing attackers to steal, corrupt, or encrypt data for ransom. This could disrupt operations, compromise customer data, and lead to financial and reputational losses.

Answers will vary. Threats to the server should 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.

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

Data Breach:

- Financial Loss: A data breach could lead to significant financial losses, including costs associated with investigating the breach, notifying affected customers, and implementing additional security measures. The organization could also face fines or legal fees if it fails to comply with data protection regulations.
- Revenue Impact: Compromised customer trust could result in a decrease in sales, as customers may be reluctant to continue doing business with the organization. This loss of confidence can have a direct impact on daily revenue.
- Reputational Damage: A data breach can severely damage the organization's reputation, leading to negative publicity and loss of customer loyalty. Rebuilding trust and credibility can be costly and time-consuming.
- Operational Disruptions: Remediation efforts, such as system shutdowns for security assessments and implementing new controls, can disrupt business operations and impact productivity.

- Legal and Compliance Consequences: If customer data, especially financial information, is compromised, the organization could face legal action from affected individuals and regulatory bodies, resulting in fines, penalties, and increased regulatory scrutiny.

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.

Ransomware:

- Financial Loss: Ransomware can result in direct financial loss, either through paying the ransom (which is generally discouraged) or from the costs of recovering data from backups, restoring systems, and implementing additional security measures.
- Operational Disruption: A ransomware attack can disrupt regular business operations by rendering the database server and other critical systems inaccessible. This downtime can impact productivity and lead to delays in fulfilling customer orders or services.
- Revenue Impact: With systems down and sales affected, the organization may experience a direct hit to daily revenue, especially if the ransomware disrupts online transactions or prevents the recording of daily sales.
- Reputational Damage: Customers may lose trust in the organization's ability to protect their information, leading to a damaged reputation. This can result in customer attrition and reduced brand loyalty.
- Data Loss: In cases where data backups are also compromised, the organization may face permanent data loss, impacting customer information, historical transaction data, and operational records.
- Legal and Compliance Issues: If sensitive customer information is exposed or lost, the organization may face legal consequences, regulatory fines, and increased scrutiny from data protection authorities.

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

Hardware failure:

- Data Loss: If the database server experiences hardware failure without adequate backups or redundancy, there could be a complete or partial loss of customer data and transaction records, which may not be recoverable.
- Operational Downtime: Hardware failure can lead to system downtime, interrupting the ability to process transactions, access customer information, or carry out daily operations, resulting in delays and decreased productivity.
- Revenue Impact: With sales dependent on a functional server, hardware failure could immediately impact daily revenue, as transactions may be halted until the system is restored.
- Reputational Damage: Customers may view the organization as unreliable if frequent outages occur due to hardware issues, which could reduce customer confidence and loyalty over time.
- Recovery Costs: The organization may incur significant costs to replace or repair the server, restore data from backups, and implement redundancy solutions to prevent future failures.
- Increased Manual Processing: In the event of server failure, the organization may need to manually process transactions, consuming substantial time and resources and increasing the risk of human error.

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:

Data Breach:

Implement data encryption for all sensitive information within the database. Encrypting data ensures that even if unauthorized access occurs, the information remains unreadable and secure, reducing the risk of exposure in the event of a breach.

Answers will vary. Counter measures for data breaches can include updated policies or procedures, data encryption, employee training regarding security measures, security updates and limit access based on need.

Ransomware Attack:

Implement regular, secure data backups stored offline or in a separate, protected environment. This ensures that, in the event of a ransomware attack, the organization can restore its data without paying the ransom, minimizing downtime and loss of critical information.

Answers will vary. Counter measures for ransomware attack could include antivirus and antimalware software, updated OS and applications, data backups, enforce security policy, and physical access control mechanisms.

Hardware Failure:

Implement hardware redundancy by setting up a failover server or using a RAID (Redundant Array of Independent Disks) configuration. This ensures that if one piece of hardware fails, the backup system can take over, minimizing downtime and preventing data loss.

Answers will vary. Counter measures for hardware failure can include hardware redundancy, access control mechanisms, and replace obsolete equipment.

Malware:

Install and regularly update antivirus and antimalware software on the server. This software will detect, quarantine, and remove malicious files, reducing the risk of malware infections that could compromise data integrity or server functionality.

Answers will vary. Counter measures could include antivirus and antimalware software, updated OS and applications, data backups, enforce security policy, and physical access control mechanisms.

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:
Quantitative Value: $100,000

Justification: Given the sensitivity of customer data, including purchase history and payment information, a data breach would likely result in severe financial and operational repercussions. Direct costs might include:

- Data Recovery and System Restoration Costs: Estimated at around $20,000 to cover IT labor, forensic analysis, and system repairs.
- Customer Notification and Support: Regulatory requirements may necessitate notifying affected customers and providing support, possibly costing $15,000 in resources and outreach efforts.
- Legal and Compliance Fines: Depending on jurisdiction and the number of affected individuals, penalties and regulatory fines could amount to $40,000 or more.
- Lost Revenue Due to Customer Attrition: With a daily revenue of $25,000, the five-day downtime could result in $125,000 in lost sales, although some may be recoverable.
- Reputational Damage: While difficult to quantify, the breach could lead to customer loss and a damaged reputation, impacting long-term revenue.

The overall financial impact, factoring in direct costs and potential revenue loss, justifies assigning a quantitative value of $100,000 or more.
Answers will vary. The impact of a data breach could cost $100,000 or more and 5 working days to restore the data.

Server hardware failure requiring hardware replacement:
Quantitative Value: $5,000

Justification: Hardware replacement costs and downtime have a direct impact, with expenses including:

- Hardware Replacement Cost: Estimated at $2,500 to $3,000, depending on the server model and availability.
- Labor and IT Service Costs: Approximately $1,000 to cover IT labor for installation, configuration, and testing.
- Operational Downtime: With two days of downtime, potential revenue loss is $50,000 (based on $25,000 daily revenue). Some sales may be recoverable post-restoration, so the immediate financial impact is reduced.

Given these factors, the total impact is approximately $5,000, with additional revenue implications due to the temporary downtime.
Answers will vary. 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:
Quantitative Value: $20,000 or more

Justification: A ransomware attack on the server database could result in substantial costs associated with recovery, including:

- Data Recovery and Ransom: If no backup is available, paying a ransom could be considered (though discouraged), typically costing $10,000 or more. Alternatively, recovery from secure backups would involve expenses related to restoring and verifying data integrity.
- System Clean-Up and Security Enhancements: Approximately $5,000 for IT labor to remove the ransomware, install additional security measures, and ensure no residual vulnerabilities remain.

- Downtime Impact: With an estimated five days of downtime, potential lost revenue could be $125,000 (based on $25,000 daily revenue). While some transactions may recover post-restoration, there would still be an immediate financial impact.

Given the complexity and potential revenue loss, a ransomware attack's quantitative value is reasonably set at $20,000 for direct recovery costs, with additional indirect revenue impacts.
Answers will vary. 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:
Quantitative Value: $50,000 or more

Justification: A flood in the server room would likely result in extensive damage to hardware, as well as significant recovery and replacement costs:

1. Hardware Replacement: Estimated at $25,000 to replace servers, networking equipment, and storage systems damaged by water exposure.
2. Labor and IT Services: Approximately $10,000 for specialized labor to replace hardware, reconfigure the system, and verify operational integrity.
3. Data Recovery and System Restoration: If backups were also affected, additional recovery efforts may be needed, adding around $5,000.
4. Operational Downtime: Three days of downtime would impact revenue, potentially costing $75,000 in lost sales based on the $25,000 daily revenue, though some transactions might be recoverable.

Given the equipment replacement, labor, and operational impacts, a flood could easily reach or exceed $50,000 in direct and indirect costs.
Answers will vary. 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.

Rank the vulnerabilities and propose possible countermeasure for each threat.

Data breach impacting all customers:
Risk Ranking: High

Countermeasures:

- Data Encryption: Encrypt sensitive customer data both at rest and in transit, ensuring that even if data is accessed without authorization, it remains protected.
- Regular Employee Training: Conduct regular cybersecurity awareness training to help employees recognize phishing attempts and secure sensitive information.
- Frequent Software and Hardware Updates: Regularly update all software and firmware on the server to address vulnerabilities and prevent exploitation by attackers.
- Access Controls: Implement role-based access control (RBAC) to ensure only authorized personnel have access to sensitive data, reducing exposure.
- Intrusion Detection and Prevention Systems (IDPS): Deploy IDPS to monitor, detect, and respond to any unusual activity that might signal a breach attempt.

Answers will vary. 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:
Risk Ranking: Medium

Countermeasures:

- Data and System Backups: Maintain regular, secure backups of the database and critical systems to allow for quick restoration in case of hardware failure.
- Hardware Redundancy: Implement redundancy measures, such as a failover server or RAID configurations, to ensure that if one component fails, another can take over, minimizing downtime.
- Preventive Maintenance: Schedule regular maintenance checks on server hardware to identify and address any potential issues before they lead to failure.
- Service Contracts with Rapid Replacement: Secure a service agreement with hardware providers that guarantees quick replacement of failed components to reduce downtime.

Answers will vary. 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:
Risk Ranking: Medium

Countermeasures:

- Regular Data Backups: Conduct frequent, secure backups stored offline or in a separate network location to ensure data can be restored without paying a ransom.
- Employee Security Training: Provide regular training on identifying and avoiding phishing attacks and other common ransomware entry points to reduce the likelihood of infection.
- Anti-Malware and Endpoint Protection: Install and regularly update anti-malware software on all systems to detect and prevent ransomware from executing.
- Network Segmentation: Segment critical systems and databases from the rest of the network to limit the spread of ransomware if an infection occurs.
- Patch Management: Ensure all software and systems are up-to-date to protect against known vulnerabilities that ransomware may exploit.

Answers will vary. 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:
Risk Ranking: Medium to High

Countermeasures:

- Insurance Coverage: Purchase comprehensive insurance to cover costs associated with equipment damage, data recovery, and operational downtime due to flooding or water damage.
- Data Backups: Ensure daily data backups are stored offsite or in a cloud-based solution, allowing data restoration even if on-site equipment is damaged.
- Environmental Controls: Install flood sensors in the server room to detect leaks early and consider using gas-based fire suppression systems, which avoid water damage.
- Elevated Server Placement: Position servers and critical equipment on raised platforms to protect against flooding from sprinkler activation or other water sources.

Answers will vary. 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.

What actions could decrease the impact of a ransomware threat?

- Regular Data Backups: Conducting frequent and secure backups stored offline or in a separate, protected environment ensures that data can be restored without paying a ransom. This minimizes operational downtime and protects against data loss, allowing the organization to quickly resume business operations after an attack.
- Employee Security Training: Educating employees to recognize phishing emails, malicious links, and suspicious downloads can prevent ransomware from entering the organization in the first place. By reducing the likelihood of infection, the organization lowers the overall risk and impact of a ransomware attack.
- Anti-Malware and Endpoint Protection: Installing and updating anti-malware software across all devices helps detect and block ransomware before it can execute. This containment reduces potential data corruption and system downtime, effectively preventing the threat from spreading within the network.

Answers will vary. Choose two to three countermeasures and explain how they would eliminate potential impact.