Southern
New Hampshire
University

CYB 410 Module Three Activity Worksheet
Responding to Risk

Instructions

Complete this template by replacing the bracketed text with the relevant information.

Scenario One

1. What type of risk do you identify in this scenario?

The risk type is unauthorized access and potential data security breaches due to the use of unregulated USB ports.

2. How does your identified risk impact the organization?

Unauthorized access through USB ports could lead to data theft, malware infections, and potential breaches of sensitive operational information, severely compromising organizational integrity and operational safety.

3. How would you rate the probability and impact on a scale of low, medium, and high?

Probability: Medium, as it depends on whether an employee uses the port for unauthorized purposes.

Impact: High due to the potentially severe consequences of a data breach or malware infection.

4. What do you need to be successful in minimizing the risk?

Implement strict usage policies and monitoring for USB ports, educate employees on the risks of unauthorized device connections, and employ technology solutions that disable USB ports or restrict their functionality to only authorized devices.

Scenario Two

1. What type of risk do you identify in this scenario?

The risk is data loss and compliance risk due to the absence of a data retention policy and inadequate storage resources.

2. How does your identified risk impact the organization?

Running out of storage could lead to operational disruptions and data loss. Additionally, the lack of a retention policy might cause legal and compliance issues, affecting the organization's credibility and leading to potential fines.

3. How would you rate the probability and impact on a scale of low, medium, and high?

Probability: High, as storage capacity is already a pressing issue.

Impact: Medium, depending on the value of the data at risk and legal requirements.

4. What do you need to be successful in minimizing the risk?

Secure additional funding for storage solutions, develop and enforce a data retention policy, prioritize data importance to manage storage efficiently, and explore cost-effective cloud storage options.

Scenario Three

1. What type of risk do you identify in this scenario?

Physical security risk due to unauthorized access to a sensitive area (server room).

2. How does your identified risk impact the organization?

Unauthorized access could lead to tampering, theft, or damage of critical infrastructure, directly impacting operational capability and security.

3. How would you rate the probability and impact on a scale of low, medium, and high?

Probability: Medium, as the door is occasionally left unsecured.

Impact: High, due to the potential catastrophic consequences of server room breaches.

4. What do you need to be successful in minimizing the risk?

Ensure physical security protocols are strictly followed, including keeping doors closed and locked, monitoring access more rigorously, and educating all personnel on the importance of security in sensitive areas.

Overall View
(Scenarios One, Two, and Three)

1. What is your implementation strategy on a 30/60/90-day time line?

Scenario One: BYOD

30-Day:

- Assess and Audit: Perform an audit of current BYOD practices and USB port usage. Start developing a revised BYOD policy that includes USB port management.
- Training: Begin awareness training sessions on the dangers of unauthorized device connections and proper use of BYOD.

60-Day:

- Policy Implementation: Enforce the new BYOD policy. Implement USB access controls, including disabling ports or using device management software to monitor and restrict usage.
- Continuous Monitoring: Set up monitoring systems to detect and alert on unauthorized USB activities.

90-Day:

- Review and Adjust: Evaluate the effectiveness of the new BYOD policy and USB control measures. Adjust the policy based on feedback and monitoring data.
- Ongoing Education: Establish ongoing security training updates, focusing on BYOD security and compliance.

Scenario Two: **Data Retention**

30-Day:

- Needs Assessment: Conduct a thorough assessment of current storage capacity and future needs. Start discussions for budget adjustments to accommodate necessary hardware.
- Policy Drafting: Begin drafting a comprehensive data retention policy.

60-Day:

- Policy Implementation: Formalize and implement the data retention policy. Start purchasing and installing necessary storage hardware.

- Data Prioritization: Implement procedures for data prioritization and deletion according to the new policy.

90-Day:

- Policy Review: Review the impact of the data retention policy on storage management and compliance.
- Adjustment and Optimization: Adjust the policy and storage solutions based on operational feedback and storage utilization metrics.

Scenario Three: Physical Security

30-Day:

- Security Audit: Conduct a security audit of the server room and all physical access points.
- Protocol Reinforcement: Reinforce security protocols for accessing sensitive areas, emphasizing the importance of keeping doors closed and secured.

60-Day:

- Access Control Enhancement: Upgrade physical access controls, potentially integrating biometric systems or advanced keycard technologies.
- Training and Drills: Conduct security training and emergency response drills focused on physical security breaches.

90-Day:

- Effectiveness Review: Review the effectiveness of new physical security measures.
- Continuous Improvement: Implement a continuous improvement plan for physical security, including regular audits and updates to access protocols.