Andree Salvo

Southern New Hampshire University

CYB 410 - 3-1 Activity: Responding to Risk

Instructor: Johnathan Hammitt

Scenario One: BYOD

You work as an analyst for a fire station that has begun updating its bring your own device (BYOD) policy. Gaps have been identified in the existing policy that would permit any employee to access the USB ports on their workstations. The firefighters want to use the USB ports to access movies and music during their free time.

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

   The risk that's identified from the given scenario is an Insider threat risk. This allows an unrestricted USB from an employee that can unintentionally bring malware, misuse access to copy or steal sensitive data.

2. How does your identified risk impact the organization?

   The organization can face ransomware infections, unauthorized data transfer, and severe downtime of the network if someone were to conduct a Denial-of-Service (DOS) attack.

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

   Probability: Medium – I chose medium because I think that not every employee would plug an infected USB Drive, but the chances are significant enough to be concerning if someone were to try to exfiltrate the data

   Impact: High – if a misuse occurs, it can lead to a severe breach or disrupt critical systems inside the firehouse station.

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

   To mitigate this risk, a clear policy should be in place regarding the use of USB ports, software should be installed to monitor and block any unauthorized devices, and employees should receive proper training to understand the importance of these changes.

Scenario Two: Data Retention

Your company does not have a data retention policy in place because of a limited IT budget that will not cover the costs of necessary hardware. There have been discussions about developing one, but the process has been on hold in favor of other projects. Along with this lack of policy for storing old data, no money has been budgeted to buy hardware that could store the additional data for the long term. Storage space has been running out, and soon data will need to be deleted to make space for new data.

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

   Operational and compliance risks. Examining the scenario reveals a lack of a formal data retention policy, combined with limited storage capacity, which can lead to data loss and potential regulatory violations.

2. How does your identified risk impact the organization?

   If the organization runs out of storage, it may lose important records, violate retention laws, and make it more difficult to handle incident response or audits. On top of this, not having enough space for new data could completely stop operations.

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

   Probability – High: Storage space is running out
   Impact – Medium and high: It depends on the value of the lost data, but the impact could be significant — things like compliance fines or losing key operational data could seriously harm the organization.

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

   To successfully minimize this risk, we'd need to establish a data retention policy as soon as possible and find a cost-effective way to expand storage so that nothing will be lost, or we will not have to delete old data.

Scenario Three: Physical Security

Your company is repainting the walls in its server room. A small team of additional painters has been granted access to the space. The door to enter the room is usually locked with a key card that prevents entry to anyone without preset permissions. You notice they have propped open the door for ventilation and to move their supplies in and out.

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

   From the scenario, this is a Physical Security risk. Propping the server room doors leads to bypass access controls and can expose critical systems to unauthorized personnel if entry.

2. How does your identified risk impact the organization?

   Unauthorized personnel who don't have access to the server room can tamper with the servers, steal expensive equipment, or install malicious devices in the server room.

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

   Probability – High: Painters and regular staff have limited access, whether intentionally or unintentionally, which means someone could abuse it to cause harm.

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

   To keep this risk under control, the organization should ensure that server room doors always remain locked. They could also investigate other ventilation options so the door doesn't need to be opened for security reasons.

Overall View
(Scenarios One, Two, and Three)

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

First 30 Days

- Update: the Bring Your Own Device (BYOD) & USB port policy and enforcing physical server room security.
- Fixing group policy restrictions on USB ports and enforcing supervision for contractors when going to high clearance rooms.

Next 60 Days

- Drafting a formal data retention policy with input from compliance and IT teams.
- Securing a low-budget, friendly storage expansion.
- Providing employee training sessions on BYOD security and physical access protocols.

By 90 Days

- Implementing a technical solution for data retention, like cloud storage, automated backup, and data classification
- Automate the Enforcement of data lifecycle management
- Conduct an audit of BYOD compliance and physical security controls for improvements.
-