Virtual Case Experience Cybersecurity

Model Work Task 1

Integrated Information Defense I

Part 1

Boldi AG's missteps represent a situation where both due care and due diligence were lacking:

- Due Care Oversight:

Due care necessitates the identification of information risks concerning essential objectives, processes, or assets. In this instance, Boldi AG did not adequately recognize the information risks associated with their offsite backup storage. They failed to take the necessary steps to assess and acknowledge potential risks related to this practice.

- Due Diligence Neglect:

Due diligence involves the continuous monitoring of controls and periodic verification of their efficacy. In the case of Boldi AG, not only were there no controls in place, but there was also a complete absence of any routine verification. This means they made no proactive efforts to ensure the security of their backup storage setup and its ongoing ability to protect critical data.

Integrated Information Defense II

Boldi AG's missteps represent a situation where both due care and due diligence were lacking:

➢ Due Care Oversight:

- Due care necessitates the identification of information risks concerning essential objectives, processes, or assets. In this instance, Boldi AG did not adequately recognize the information risks associated with their offsite backup storage. They failed to take the necessary steps to assess and acknowledge potential risks related to this practice.

➢ Due Diligence Neglect:

- Due diligence involves the continuous monitoring of controls and periodic verification of their efficacy. In the case of Boldi AG, not only were there no controls in place, but there was also a complete absence of any routine verification. This means they made no proactive efforts to ensure the security of their backup storage setup and its ongoing ability to protect critical data.

In summary, Boldi AG's errors were a result of a deficiency in both due care and due diligence. They did not recognize the risks associated with their data storage practices and had no controls in place to safeguard their vital data. Furthermore, they failed to periodically verify the effectiveness of any non-existent controls. This lack of attention to information risk management exposes a significant vulnerability in their data protection strategy.

Integrated Information Defense III

Part 2

Subject: Defense Principles & Risk Mitigation for Boldi AG

Dear Stefan,

I wanted to highlight key principles of defense options for Boldi AG:

- ✓ Deterrence: Means discouraging threats through visible security measures. Boldi AG can deter attackers by visibly enhancing security, making breaches less attractive.
- ✓ Detection: Detection is the process of identifying or recognizing threats and breaches swiftly through monitoring systems and processes, allowing for prompt response and mitigation.
- ✓ Prevention: refers to the implementation of security measures designed to stop threats from materializing
- ✓ Avoidance: consists of strategic actions to circumvent or entirely eliminate risks.

By integrating these key defense principles and risk mitigation options, Boldi AG can better protect its data and assets from potential risks and security breaches.

If you have any questions or need further information on this topic, please feel free to reach out.

Best regards,

Lahcen Tizi

Information Security Concerns at Boldi AG
Subject: Addressing Risks in File Management and Access Controls

At Boldi AG, information is stored both on paper and within cloud-based systems, yet these systems exhibit inconsistent file formats, posing challenges for effective analysis. Additionally, navigating these systems proves difficult due to their complexity. Compounding this issue is the absence of adequate access controls, leaving the company without defined parameters over who can access these files.

CIA Triad Impact

Below is how those concerns impacts:

- Confidentiality: Inconsistent formats risk unauthorized access

  Lack of encryption or standardized formats can lead to unauthorized access to sensitive data
- Integrity: Potential data manipulation or inaccuracies
- Availability: Lack of access controls might lead to system overload or unauthorized access impacting availability.

  Implications of compromised availability on business operations.

Risk and Consequences

Detail the potential risks associated with identified concerns:

- Data breaches, unauthorized access due to format inconsistencies
- Data manipulation or errors affection reliability
- Operational disruptions due to inaccessible or hard-to-use systems

Mitigation Strategies & Implementation

Below is the recommendation of mitigation steps for Boldi AG's:

- Standardize file formats for consistency and security
- Implement robust access controls and user permissions
- Transition from paper files to secure, easily managed digital systems

Implementation Plan

- Outline a high-level implementation plan:
- Timelines, responsible parties, and key milestones for each strategy

Graphic Description:

The graphic depicts the interconnectedness of key elements in Information Systems Security.

1. Vulnerability Assessment:

   - Initial step in understanding potential weaknesses or vulnerabilities within the system.

2. Vulnerability Scanning:

   - Utilizes tools to actively scan and identify vulnerabilities within hardware, software, or networks.

3. Mitigation Planning:

   - Involves strategies and plans to address identified vulnerabilities.

4. Hardware and Systems Security:

   - Ensures that hardware components and systems are fortified against potential threats.

5. Information Systems Security Baseline:

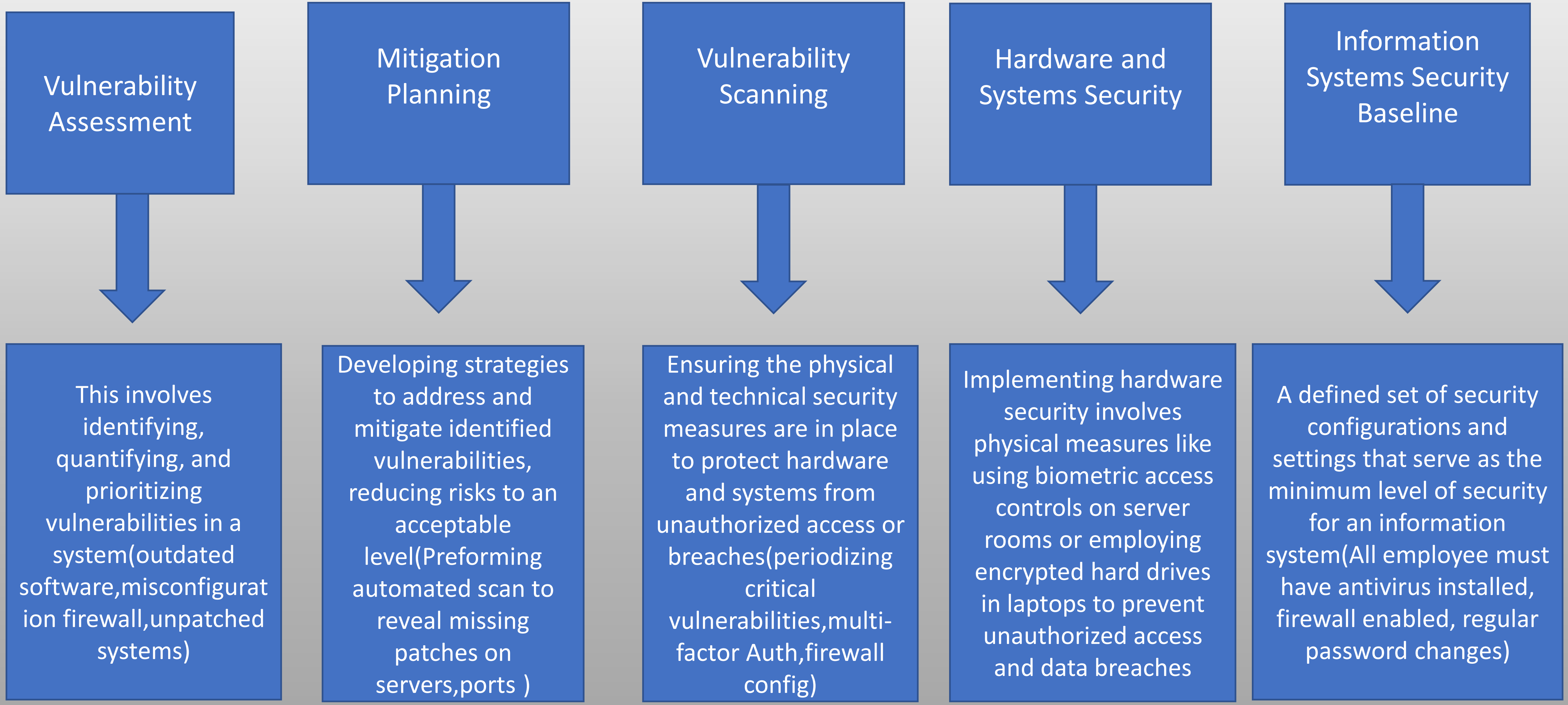
   - Represents the minimum level of security required across the organization's systems and networks.

Relationships:

- Vulnerability Assessment leads to identifying weaknesses.
- Vulnerability Scanning actively identifies vulnerabilities.
- Mitigation Planning is based on the results of assessment and scanning.
- Hardware and Systems Security implementation supports mitigation plans.
- Information Systems Security Baseline sets the standard for overall security measures.

IT System Security Baseline

Chart illustrating each of the information system security components and relationships:



Vulnerability Assessment

This involves identifying, quantifying, and prioritizing vulnerabilities in a system(outdated software,misconfiguration firewall,unpatched systems)

Mitigation Planning

Developing strategies to address and mitigate identified vulnerabilities, reducing risks to an acceptable level(Preforming automated scan to reveal missing patches on servers,ports)

Vulnerability Scanning

Ensuring the physical and technical security measures are in place to protect hardware and systems from unauthorized access or breaches(periodizing critical vulnerabilities,multi-factor Auth,firewall config)

Hardware and Systems Security

Implementing hardware security involves physical measures like using biometric access controls on server rooms or employing encrypted hard drives in laptops to prevent unauthorized access and data breaches

Information Systems Security Baseline

A defined set of security configurations and settings that serve as the minimum level of security for an information system(All employee must have antivirus installed, firewall enabled, regular password changes)