Samuel N. Oruh | CYB3841-O 01 – Information Assurance & Compliance | Prof. Robin Alarcon
June 4, 2023

Assignment 1.8 - Risk Assessment

1. **Document the steps you will take to complete the risk assessment for iBank Financials?**

   To complete the risk assessment for iBank Financials, the following steps should be taken:

   a. Establish the scope of the risk assessment by determining the assessments boundaries and extent.
   b. Identify all the critical assets and resources of iBank Financial.
   c. Identify the potential threats and vulnerabilities in iBank's assets.
   d. Assess iBank's current security measures.
   e. Determine the likelihood of threat occurrence to iBank's assets.
   f. Determine the potential impact of threat occurrence to iBank.
   g. Determine the level of iBank's risk.
   h. Identify the effectiveness of iBank's current controls and identify the appropriate security measures needed to mitigate iBank's risks.
   i. Document the implementation of iBank's new security measures.

2. **What framework(s) did you use to guide your decisions? Why did you use the framework(s)? Be thorough in your explanation.**

   For this risk assessment framework, I chose to use the NIST Cybersecurity Framework. The NIST Cybersecurity framework provides a structured approach to managing and reducing cybersecurity risks. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover. The framework helps in identifying assets, assessing risks, and implementing appropriate security controls.

   I chose the NIST Cybersecurity Framework for the following reasons:

   1. The framework is widely recognized and adopted as a best practice in the cybersecurity industry. It provides a comprehensive and flexible approach to risk assessment and management.
   2. The framework aligns with other industry standards and guidelines, making it easier to integrate into existing risk management processes.
   3. The framework promotes a continuous improvement mindset by emphasizing the need for ongoing monitoring, assessment, and response to emerging threats and vulnerabilities.
   4. The framework covers various aspects of cybersecurity, including risk assessment, threat mitigation, incident response, and recovery. It provides a holistic approach to managing cybersecurity risks.

3. **Based on the steps from question 1, complete a risk assessment. List each asset and its corresponding information on a separate line.**

   Based on the steps from question 1, my risk assessment for iBank Financials are as follows:

   - Assets:
     - Computers in the main office (30)
     - Computers for client account management (20)
     - Laptops for remote work (5)
     - Computers for vendor applications, servers, cloud applications, and support (5)

Assignment 1.8 - Risk Assessment

- Wireless network shared with the insurance agency.
- Laptops issued to agents in iBank's remote offices.
- Personal tablets used to access client management system.
- Servers (on-premises and on AWS)
- Customer credit card information stored on the server.
- New employees' access to server data and applications.
- Employee ID badges for physical access.
- New computers in a non-sensitive location.

4. **List the risk score for each asset listed in question 3.**

The risk scores for each asset are as follows:

- Computers in the main office (30): High
- Computers for client account management (20): High
- Laptops for remote work (5): Medium
- Computers for vendor applications, servers, cloud applications, and support (5): High
- Wireless network shared with the insurance agency: Medium
- Laptops issued to agents in remote offices: Medium
- Personal tablets used to access client management system: Medium
- Servers (on-premises and on AWS): High
- Customer credit card information stored on the server: High
- New employees' access to server data and applications: High
- Employee ID badges for physical access: Medium
- New computers in a non-sensitive location: Low

5. **Provide the matrix graph that was used to determine the risk scores.**

Risk score matrix:

Asset	Likelihood	Impact	Risk Score
Computers in the main office (30)	High	High	High
Computers for client account management (20)	High	High	High
Laptops for remote work (5)	Medium	Medium	Medium
Computers for vendor applications, servers, etc. (5)	High	High	High
Wireless network shared with the insurance agency	Medium	Medium	Medium
Laptops issued to agents in remote offices	Medium	Medium	Medium
Personal tablets used to access client management system	Medium	Medium	Medium
Servers (on-premises and on AWS)	High	High	High
Customer credit card information stored on the server	High	High	High
New employees' access to server data and applications	High	High	High
Employee ID badges for physical access	Medium	Medium	Medium
New computers in a non-sensitive location	Low	Low	Low