Lab J

Brandon Trinkle

Arizona State University

Course Number: IFT 202

Professor Gary Grindle

Feb 25, 2024

**Part I**

The fictitious company I chose for this risk assessment is Trinkle Technologies. The six assets I chose to do a risk assessment on are the main building, server room, intellectual property repository, networking equipment, employee workstations, and our customer database. Below is a table of the STRIDE assessment.

Risk scoring scale:

* Low (1) – Low impact and low likelihood.
* Medium (2) – Moderate impact and low likelihood.
* High (3) – High impact and low likelihood.
  + Risk = Impact x Likelihood
    - Low risk: 1-3
    - Medium Risk: 4-5
    - High Risk: 6-9

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STRIDE Risk Assessment | | | | |
| Asset | **First Threat** | **Risk Score** | **Second Threat** | **Risk Score** |
| Main Building | Sabotage – Structure Damage | Likelihood-2  Impact-3  Risk = 6  (High) | Unauthorized access | Likelihood -2  Impact-2  Risk = 4 (Medium) |
| Server Room | Data tampering | Likelihood-3  Impact-3  Risk = 9 (High) | Denial of Service | Likelihood -2  Impact-2  Risk = 4 (Medium) |
| Employee Workstations | Malware | Likelihood-3  Impact-2  Risk = 6  (High) | Phishing attacks | Likelihood -2  Impact-2  Risk = 4 (Medium) |
| Networking Equipment | Eavesdropping | Likelihood-2  Impact-3  Risk = 6  (High) | Network disruptions | Likelihood -2  Impact-2  Risk = 4 (Medium) |
| Customer Database | Data breach | Likelihood-3  Impact-3  Risk = 9  (High) | Insider threat | Likelihood -2  Impact-2  Risk = 4 (Medium) |
| Intellectual Property | Theft | Likelihood-3  Impact-3  Risk = 9  (High) | Cyber Espionage | Likelihood -2  Impact-2  Risk = 4 (Medium) |

**Part II**

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Register | | | |
| **Asset** | **Associated Threat(s)** | **Risk Score** | **CVE ID (if applicable)** |
| Intellectual Property Repository | * Theft * Cyber Espionage | 9 (High) | [CVE-2023-33956](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33956) |
| Customer Database | * Data Breach * Insider Threat | 9 (High) | [CVE-2023-1934](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1934) [CVE-2023-4803](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4803) |
| Server Room | * Data Tampering * Denial of Service (DoS) | 9 (High) | [CVE-2023-47800](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47800) [CVE-2024-25407](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-25407) |
| Main building | * Sabotage * Unauthorized Access | 6 (High) | N/A |
| Employee Workstations | * Malware * Phishing | 6 (High) | [CVE-2024-0581](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-0581) [CVE-2024-24763](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-24763) |
| Networking Equipment | * Eavesdropping * Network Disruption | 6 (High) | [CVE-2023-51741](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-51741) [CVE-2023-27595](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27595) |

**Part III**

**Protect:**

*Protecting Physical Assets:*

Access Control (PR.AC-1, ): Implement robust access controls, including key card systems, biometric authentication, and surveillance cameras, to restrict and monitor access to physical assets. (National Institute of Standards and Technology, 2018)

Security Guards (PR.AC-2): Employ trained security personnel to patrol and monitor physical assets, providing a visible deterrent and a quick response to suspicious activities. (National Institute of Standards and Technology, 2018)

*Protecting Cyber Assets:*

Firewalls and Intrusion Detection Systems (PR.DS-2): Install firewalls to monitor and control incoming and outgoing network traffic and deploy intrusion detection systems to identify and respond to cyber threats in real time. (National Institute of Standards and Technology, 2018)

Regular Software Patching (PR.DS-2): Ensure that all software and systems are regularly updated with the latest security patches to address vulnerabilities and protect against cyber-attacks. (National Institute of Standards and Technology, 2018)

*Security Training for Privileged Users:*

Secure Coding Practices: Provide training on secure coding practices to ensure that privileged users involved in software development follow guidelines to prevent vulnerabilities. (National Institute of Standards and Technology, 2018)

Incident Response Procedures: Train privileged users on incident response procedures, including recognizing and reporting security incidents promptly. (National Institute of Standards and Technology, 2018)

**DETECT:**

*Detecting Physical Security Breaches:*

Surveillance Cameras (DE.CM-2): Implement surveillance systems to monitor key areas and detect any unauthorized access or suspicious activities. (National Institute of Standards and Technology, 2018)

Intrusion Detection Systems (DE.CM-8): Deploy sensors and alarms to identify physical security breaches, triggering immediate responses. (National Institute of Standards and Technology, 2018)

*Detecting Cybersecurity Breaches:*

Security Information and Event Management (SIEM) Systems (DE.CM-2): Implement SIEM systems to aggregate and analyze log data from various sources, enabling the detection of abnormal cyber activities. (National Institute of Standards and Technology, 2018)

Endpoint Detection and Response (EDR) Systems (DE.CM-3): Deploy EDR systems on endpoints to continuously monitor and respond to cybersecurity incidents at the device level. (National Institute of Standards and Technology, 2018)

**RESPOND:**

*Responding to Anomalies:*

Incident Response Team (RS.AN-1): Establish an incident response team trained to promptly identify and mitigate security incidents. (National Institute of Standards and Technology, 2018)

Communication Plan (RS.CO-4): Develop a communication plan to ensure effective coordination and communication during incident response. (National Institute of Standards and Technology, 2018)

*Physical Security Breach Response Plan:*

Emergency Evacuation Procedures (RS.CO-5): Develop and regularly practice emergency evacuation procedures to ensure the safety of individuals in case of a physical security breach. (National Institute of Standards and Technology, 2018)

*Cybersecurity Breach Response Plan:*

Data Breach Notification Plan (RS.AN-2): Establish a plan for notifying affected parties in the event of a cybersecurity breach, ensuring compliance with relevant regulations. (National Institute of Standards and Technology, 2018)

**RECOVER:**

*Recovering from Actions:*

Data Backups and Restoration (RC.CO-1): Regularly back up critical data and implement processes for quick data restoration in case of unauthorized access or destruction. (National Institute of Standards and Technology, 2018)

Recovery Plan for Physical Security Breaches:

Facility Repair and Restoration Plan (RC.CO-2): Develop a plan for repairing and restoring the physical facility after a security breach, including rebuilding damaged structures or systems. (National Institute of Standards and Technology, 2018)

Recovery Plan for Cybersecurity Breaches:

System Reconfiguration and Patching (RC.RP-1): After a cybersecurity breach, reconfigure systems, apply necessary patches, and update security protocols to prevent similar incidents in the future. (National Institute of Standards and Technology, 2018)

# References

National Institute of Standards and Technology. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from nvlpubs: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf