|  |
| --- |
|  |
| [Document title] |
|  |

|  |
| --- |
| Guillermo, Michael Jhon G.  3-10-2025 |

1. Choose a Cybersecurity Incident:
   * Pick a reported cybersecurity incident in 2024 or 2025 (e.g., CrowdStrike Outage, Change Healthcare Ransomware, or another of your choice).
   * Sources: Rely on credible news organizations (e.g., BBC, CNN, TechCrunch), industry reports (e.g., Verizon DBIR), or cybersecurity blogs (e.g., Krebs on Security).
   * Identify the incident briefly (1-2 paragraphs): What occurred, who was impacted, and what were the implications?
2. Analyze the Incident Using NIST SP 800-30's Risk Management Process:
   * **Framing Risk (1 page):**
     + 1. **Define the context**: What was the organizational environment (e.g., industry, size, systems involved)?
       2. **Identify assumptions and constraints**: What might the organization have assumed about its security posture? What limitations (e.g., budget, staffing) could have affected the incident?
       3. **Determine risk tolerance**: Speculate what the organization's acceptable level of risk could have been (e.g., downtime, data loss).
   * **Assessing Risk (1 page):**
     + 1. Threats: What was the source of the threat (e.g., adversarial such as ransomware or non-adversarial such as a software glitch)?
       2. Vulnerabilities: What vulnerabilities were targeted (e.g., unpatched systems, inadequate testing)?
       3. Impact: What was the damage to operations, assets, individuals, or other organizations?
       4. Likelihood: How probable was this incident based on available data or trends (e.g., see Appendix G scales)?
   * **Responding to Risk (1 page):**
     + 1. Suggest alternative responses the organization might have taken to reduce the risk (e.g., increased testing, backups).
       2. Assess these alternatives: What are the advantages/disadvantages of each (e.g., cost vs. effectiveness)?
       3. Prescribe a specific response: Defend your recommendation based on the impact of the incident and organizational requirements.
   * **Monitoring Risk (0.5-1 page):**
     + 1. Recommend ongoing monitoring measures to avoid recurrence (e.g., real-time threat detection, periodic audits).
       2. How would these measures respond to new threats (e.g., AI-powered attacks)?
       3. Integrate NIST SP 800-30 Elements:
       4. Cite specific sections or appendices within NIST SP 800-30 to assist with your analysis (e.g., Appendix I for determining risk, Appendix G for likelihood scales).
       5. Utilize a minimum of two tables or templates (e.g., Table I-5 for adversarial risk or Table H-4 for impact) to structure your findings.
   * **Real-World Relevance:**
     + 1. Make your analysis relate to existing trends in cybersecurity (e.g., the increasing prominence of AI-powered threats as of March 2025).
       2. Cite at least one other recent event or statistic to put your incident into context (e.g., "In 2025, ransomware attacks rose by X% per [source]").
   * **Conclusion (0.5 page):**
     + 1. Briefly summarize your findings: What went wrong, and how might risk management have assisted?
       2. Reflect: What wider lessons can organizations take from this incident?