Third-Party Risk Assessment Summary

Overview

This lab simulated a third-party risk assessment aligned with real-world vendor management practices. The objective was to identify, evaluate, and mitigate cybersecurity risks introduced by external vendors, particularly in a healthcare environment where HIPAA compliance is crucial.

Process

1. Created a structured Excel risk matrix to catalog third-party vendors, their services, and associated risks.
2. Classified vendors based on data sensitivity: High, Medium, Low.
3. Assigned likelihood and impact scores (1–5 scale) to each identified risk.
4. Calculated the risk score (Likelihood × Impact) and proposed mitigation strategies.
5. Estimated the residual risk after mitigation steps.
6. Documented business-critical notes related to urgency, data types, or compliance needs.

Sample Vendors and Risk Scenarios

- Goku Cloud Scheduling Inc. - High-risk due to lack of MFA for admin logins and missing SOC 2 report, exposing PHI.
- Zeta Data Analytics - Moderate risk from lack of encryption at rest, though data is anonymized.
- Nimbus Billing Solutions - Critical vendor with outdated SSL certificate and no documented business continuity plan.
- Elite HVAC - Low sensitivity but presents unauthorized remote access risk due to weak login policy.

Compliance Relevance

This lab helps simulate aspects of third-party risk management necessary for HIPAA and HITRUST compliance:

- HIPAA requires organizations to manage vendor relationships that involve PHI (Business Associate Agreements).
- HITRUST emphasizes vendor evaluation and ongoing monitoring as part of its control framework.
- NIST SP 800-161 and NIST 800-30 methodologies were used to define risk scoring and threat modeling.

Why This Lab Matters

Risk analysts are frequently tasked with evaluating third-party vendors before onboarding or contract renewals. This lab reflects how tools like Excel or GRC platforms are used to support governance. It demonstrates familiarity with key risk indicators (KRIs), basic scoring methodologies, and mitigation strategy planning—all essential to a junior GRC or cybersecurity analyst role.

References

Center for Internet Security. (n.d.). CIS Controls v8: Safeguards for third-party and service provider management. https://www.cisecurity.org/controls/cis-controls-list

U.S. Department of Health and Human Services. (n.d.). HIPAA Security Rule: Administrative safeguards – Business Associate Agreements. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

National Institute of Standards and Technology. (2023). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev. 1 Update 1). https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

Verizon. (2024). 2024 Data Breach Investigations Report (DBIR): Third-party and supply chain incidents. https://www.verizon.com/business/resources/reports/dbir/