Enterprise Risk Register Lab – Write-Up

This lab simulates the process of creating an Enterprise Risk Register following the NIST SP 800-30 risk assessment methodology. It demonstrates my ability to identify, evaluate, and manage internal cybersecurity risks by assessing their likelihood, impact, and appropriate mitigation strategies. This is a key function in many cybersecurity analyst and GRC roles, including those requiring HIPAA and NIST-based controls.

Steps Taken

1. **Asset Identification:**
   - Researched common critical assets used in corporations and chose five to use for this lab that I felt were the most applicable. The five I settled on were VPN Access, Shared File Drive, Employee HR records, Email System, and Endpoint devices. These are all common entry points or contain sensitive information within an enterprise environment.
2. **Threat Identification:**
   - For each asset, I researched relevant threats and chose common industry risks such as phishing, ransomware, and credential theft.
3. **Vulnerability Mapping:**
   - Researched and thought of potential vulnerabilities for each asset, modeling real risk evaluation based on commonly found vulnerabilities.
4. **Likelihood and Impact Scoring:**
   - Used industry standard risk scoring to rate each risk from 1 to 5 based on likelihood and impact and then calculated the total risk score.
5. **Mitigation Strategy:**
   - For each risk I researched and came up with potential mitigation strategies to mitigate any risk.
6. **Residual Risk Assessment:**
   After mitigation is implemented, I then assigned a residual risk score to each.

Conclusion

This lab demonstrates foundational risk management skills and the ability to structure risk evaluations in a methodical, actionable way. It reflects knowledge of frameworks like NIST SP 800-30, aligns with HIPAA security principles, and prepares me for risk assessment responsibilities in entry-level cybersecurity roles.

References

Center for Internet Security. (n.d.). CIS Controls v8: Cyber defense best practices. https://www.cisecurity.org/controls/cis-controls-list

Cybersecurity & Infrastructure Security Agency. (2023). Stop ransomware: Resources and prevention guidance. https://www.cisa.gov/stopransomware

National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST SP 800-30 Rev. 1). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Verizon. (2024). 2024 data breach investigations report (DBIR). https://www.verizon.com/business/resources/reports/dbir/