Computer Security week 3

Khaula Molapo

1.

Consider an e-commerce website that collects user data for purchases, including personal details, payment information, and browsing history. Without a strong risk management and policy framework, the site could be vulnerable to data breaches, identity theft, and fraudulent activities. To mitigate risks, the website implements a security policy outlining data encryption, access controls, and periodic vulnerability scans. Employees are trained to handle sensitive data securely, while customers are informed about privacy practices through a transparent policy page. The policy also defines procedures for responding to incidents, such as notifying users and regulators if a breach occurs. Regular audits ensure compliance with industry standards and legal regulations. By implementing these measures, the website reduces the likelihood of data loss or misuse. Policies act as a roadmap for both staff and users, ensuring trust, legal compliance, and a safer environment for online transactions, ultimately protecting the business's reputation.

2.

NIST 800-30 is a guide published by the National Institute of Standards and Technology that outlines how to conduct effective risk assessments. Its primary role is to help organizations identify, evaluate, and prioritize risks to information systems and operations. The framework provides structured steps for categorizing threats, vulnerabilities, likelihood, and potential impact. By using NIST 800-30, organizations can make informed decisions on security controls and resource allocation. It ensures that risks are addressed in a systematic way, supporting compliance with regulations and strengthening overall cybersecurity posture. In essence, it is a foundation for risk management planning.

3.

I tested Nessus to perform a vulnerability scan on a sample system. The tool automatically detected open ports, outdated software, and possible misconfigurations. It provided detailed reports with severity levels and recommendations for remediation. This experience highlighted how automated vulnerability scanning is crucial for identifying risks before attackers exploit them. The reports made it easier to prioritize issues based on criticality, ensuring that the most dangerous threats are addressed first. Nessus also reinforced the importance of regular scans

since risks change as systems evolve. Overall, it was a practical lesson in proactive risk management through automated security tools.

4.

The risk/policy workflow diagram created in Canva illustrates the cycle of managing risks within an organization. It begins with identifying potential threats and vulnerabilities, followed by assessing their likelihood and impact. Next, policies are drafted or updated to address identified risks. The workflow then moves to implementation, where employees follow guidelines and security measures. Monitoring and auditing ensure the policies are being enforced properly. Finally, the cycle includes continuous improvement, where lessons from audits and incidents feed into updated risk assessments. This diagram clearly shows how risks and policies are interconnected in a repeating, systematic security process.