5-2 Short Response: Breach Analysis Simulation Two

Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

1 August 2024

When reporting technical issues to senior management, clarity and context are paramount. It is crucial to distill complex technical issues into straightforward concepts that resonate with non-technical stakeholders. For instance, explaining security vulnerabilities as "unprotected gateways that could potentially expose our system to intruders" simplifies the issue while conveying the risk. Visual aids like diagrams and charts can effectively demonstrate how such vulnerabilities might be exploited and the potential impact on our operations. It is essential to prioritize the issues based on their potential impact on business continuity and regulatory compliance. Each technical problem should be accompanied by a recommended solution and actionable steps, ensuring management understands the implications and the measures necessary to mitigate risks. According to Lucidchart (2020), employing visual communication tools to link technical solutions to business outcomes is crucial for enhancing comprehension and engagement among non-technical senior executives. This approach helps make abstract concepts more tangible and emphasizes the importance of security measures in protecting the organization's objectives.

In assessing our cybersecurity infrastructure, it becomes apparent that enhancements to our Account Monitoring and Control (CIS Control 16) are essential. Implementing granular monitoring policies that track access patterns in real-time can significantly bolster our security posture. For instance, setting alerts for unauthorized attempts or deviations from standard access patterns can preempt potential breaches. This adaptation safeguards sensitive data and ensures rapid response to anomalies, which is critical in maintaining robust data integrity (*Securing Industrial Control Systems | CISA*, 2020). Additionally, refining our Boundary Defense (CIS Control 12) to include automated, real-time scanning for unauthorized connections could further secure our network perimeters. By integrating these automated responses, we can swiftly

neutralize threats at the boundary level before they infiltrate deeper into our network. Such proactive measures are crucial for organizations that manage vast amounts of sensitive client data, ensuring compliance with stringent industry regulations and preserving trust (Barrett, 2020).

Integrating RSA key fobs for two-factor authentication significantly upgrades our security measures. RSA key fobs provide a dynamic passcode that users must enter alongside their regular password, doubling the security verification process. This method benefits from RSA's strong encryption capabilities, which are complex enough to thwart most decryption attempts by unauthorized parties. According to research by Cobb (2021), the strength of RSA encryption lies in its long key lengths, which make the encrypted messages difficult for potential intruders to decode without the specific key. This added layer of security is crucial in environments dealing with sensitive legal and financial information. Enhancing our VPN software with modern encryption methods such as AES ensures that data transmitted over our networks remains protected from interception and misuse. AES is recognized for its efficiency and security, making it an ideal choice for high-speed data exchanges that require confidentiality. Moreover, SSL/TLS encryption protocols can secure web-based communications, effectively safeguarding sensitive transactions and remote access needs. According to SSL Corp. (2023), adhering to updated SSL/TLS best practices is essential for maintaining data privacy and integrity across digital communications. Choosing a reliable Certificate Authority that undergoes rigorous third-party audits and maintains high-security standards is also critical, as the trustworthiness of certificates heavily depends on the authority that issues them. SSL.com emphasizes the importance of selecting a CA that actively keeps up with evolving industry

standards and responds effectively to new vulnerabilities, ensuring that our digital interactions remain secure and trustworthy.

References

Barrett, M. P. (2020, January 27). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. NIST. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

Cobb, M. (2021, November 4). *RSA algorithm (Rivest-Shamir-Adleman)*. Security. https://www.techtarget.com/searchsecurity/definition/RSA

How to explain technical ideas to a non-technical audience. (2020, February 27). https://www.lucidchart.com/blog/how-to-explain-technical-ideas-to-a-non-technical-audience

Securing Industrial Control Systems | CISA. (2020, December 17). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/resources-tools/resources/securing-industrial-control-systems

SSL Corp. (2023, October 9). *SSL/TLS Best Practices for 2023 - SSL.com*. SSL.com. https://www.ssl.com/guide/ssl-best-practices/