Topic 4 Discussion 2

Explain why testing technical controls, defensive software, and sensitive assets must, whenever possible, be performed on alternate (e.g., backup) systems or high-fidelity virtual environments.

Hello Class,

Testing technical controls, defensive software, and sensitive assets on alternate systems or high-fidelity virtual environments is crucial for maintaining operational continuity and data integrity. Performing tests on backup systems or virtual environments minimizes the risk of disrupting live production systems(Sagal, 2021). This approach allows for thorough evaluation of data backup and recovery plans without impacting ongoing operations. For instance, a strategy might involve documenting critical data, assessing the existing infrastructure, and then simulating various scenarios to test the effectiveness of the backup and recovery processes.

Key differences between backup types should be understood, and best practices for safeguarding infrastructure should be applied during these tests. Effective testing often includes conducting a full-system restore(CSF, 2020). It's also vital not to skip spot-checking, which involves testing smaller sets of data.

Furthermore, testing ensures that processes, procedures, and technical measures are in place to assess risks to operational continuity(Clarke, 2022). This is particularly important when considering the risk associated with keying material management.

By utilizing alternate systems or virtual environments, organizations can confidently validate their data protection strategies, ensuring that in the event of a primary system failure, data can be reliably recovered and operations can resume promptly(Tozzi, 2025). This proactive testing is a cornerstone of robust cybersecurity and business continuity planning.

References:

Clarke, M. (2022, February 11). *How to Test a Database Backup*. TechnologyAdvice. https://technologyadvice.com/blog/information-technology/how-to-test-database-backup

CSF. (2020, August 13). *Backups of information are conducted, maintained, and tested - CSF Tools*. CSF Tools - the Cybersecurity Framework for Humans. https://csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ip/pr-ip-4

Sagal, M. (2021, July 26). *Backup and Recovery Testing: The What, Why, And Five Pointers How*. OpenText CloudAlly Backup; CloudAlly. https://www.cloudally.com/blog/backup-and-recovery-testing

Tozzi, C. (2025, August 27). *An easy 10-step guide for testing backups*. SearchDataBackup. https://www.techtarget.com/searchdatabackup/tip/Ten-important-steps-for-testing-backups