GRC Case Study: Recommendations to Security Breach

Ryan Dozier, William Droge, Kyle Krause, and Daniel Wayland

GRC 100

SecureSet Academy

Dr. Erik Huffman PhD

August 25, 2019

Security Breach Incident

A case study involving a penetration test (pen test) was presented for review. Recommendations are to be presented here based on security protocol flaws identified during the penetration test and how they relate to; Governance, Risk Management and Compliance (GRC) guidance. The objective of the pen test was to infiltrate a credit union and gain access to their network closet. Social engineering and spear phishing where the main modus operandi with the underlying emphasis placed on creating both a sense and normality, then later urgency. A risk management resolution matrix is presented as a supporting document in the Appendix and referenced, as; Appendix. The main risks identified as important to us are as follows:

**Recommendations and Associated GRC**

1. Risk: Inability to follow established procedures.

Threat: Allowing external personnel into secure areas without proper clearance or vetting

Standard: Bank Protection Act of 1968, NCUA 748.2, Gramm-Leach-Bliley Act

Proposed Fix: Employees should be trained on the proper procedures and standards of allowing third party entities to access critical infrastructure. Also, IT employees should escort anyone outside the organization that requires access to any of the IT infrastructure.

1. Risk: Social Engineering through phishing emails and in-person phishing of employees

Threat: Malicious emails can cause network and system failures when opened and malware is allowed to run. Employees that are untrained in the company policies will possibly allow malicious personnel to access unauthorized areas. Standard: Bank Protection Act of 1968, NCUA 748.2, ISO 27000, ISO 27001, & Gramm-Leach-Bliley Act

Proposed Fix: Semi-annually employee training on how to recognize, respond to and report suspicious emails or attachments. All employees that are authorized to grant access into critical areas trained to adhere to the company policies.

1. Risk: Network Security.

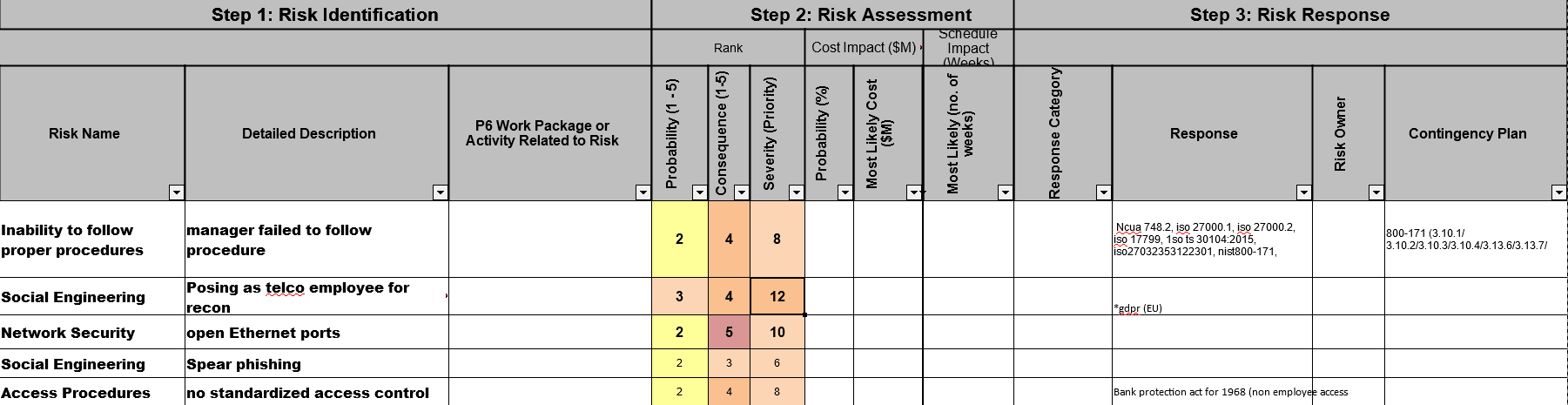
Threat: Unauthorized devices being authenticated on the network with no prior authorization or checking from IT personnel. Standard: 802.1x, ISO 27002, NIST 800-171.

Proposed Fix: Implement authentication mechanisms that validate all new devices to the network. Network should be closed to only allow IT personnel that have proper access and clearance to implement new devices.

**Conclusion**

The vulnerabilities that were identified were exploited in a controlled environment and stand as a testament to the importance of live compliance exercises. Vigilance is not just in the flawless execution of established policies, but also the comprehensive understanding of how all facets of business operations can play a role in secure operations. The recommendations presented can be used as a starting point for further conversations, future training or to conduct in-house business hygiene functions.

**Appendix**



References

Gramm-Leach-Bliley Act (1999). Financial Institutions and Customer Information: Complying with the

Safeguards Rule Retrieved August 22, 2019 from

https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-

complying

Information security management systems, ISO 27000 (2013)

Information technology, Security techniques, Information security management systems, Requirements, ISO 27000.1 (2013)

Information technology, Security techniques, Code of practice for information security controlsInformation technology, Security techniques, Information security management systems, Overview and vocabulary, ISO 27000.2 (2013)

Procedures for monitoring Bank Secrecy Act (BSA) compliance, NCAU 748.2 (2016).

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, NIST 800-171 (2015).