Section 2: Week 6: Design a Vulnerability Assessment Procedure

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 12, 2020

North Central University

# Design a Vulnerability Assessment Procedure

NCU Financial (NCU-F) operates on a finite budget and must prioritize investments into features and services. On the one hand, the business would like to spend all available resources delivering its core mission, enabling personalized investing. Allocating time and money into other projects might even appear to detract from this mission and feel like a waste. However, along the journey are risks from a litany of sources that can derail progress, cause financial hardship, and harm the organization’s reputation (Erickson & Neilson, 2018). Using a security framework, such as COBIT or NIST Cybersecurity, formalize processes for identifying and approaching threats from these risks (Devos & Van de Ginste, 2015). It would be economically prohibitive to remove every threat against the organization. Instead, a prioritization discussion must delineate between threats and vulnerabilities. A vulnerability occurs at the intersection of (1) system susceptibility; (2) threat accessibility; and (3) threat capability (Baskerville, Rowe, & Wolff, 2018). Nullifying any of these predicates mitigates an attacker’s ability to compromise the confidentiality, integrity, and availability from a specific threat. The costs to address these predicates range substantially and are highly scenario specific. For instance, the legacy main-frame lacks support for modern network encryption and authorization protocols. Upgrading or replacing the system are not feasible solutions, though moving the system to a private network segment disconnects the threat’s accessibility.