Assess Discovery Risks

Nate Bachmeier

TIM7030- Managing Risk, Security, & Privacy in Information Systems

June 7, 2020

# Introduction

The core objective of NCU Financial (NCUF) is to deliver on its mission of world-class banking services. Meeting that expectation requires a corporate strategy that minimizes risks where possible, through mitigation or transference strategies. When the business chooses to remove a vulnerability, that decision requires resources and detracts from the core mission. The corporate risk management program (RMP) needs to answer both ‘when and how’ to address these threats by operating on a feedback loop of assessing, prioritizing, and mitigating risks.

# Risk Assessment Requirements

Security assessments perform an audit of the people, processes, and products that are involved in a business workflow. This analysis needs to assess the controls at integration points and whether they are appropriate protections for the resources. Threat modeling is a formal process the enumerates these interactions and considers different spoofing, tampering, repudiation, disclosure, and elevation (STRIDE) attacks (Hennig, 2018).

# Regulatory Requirements

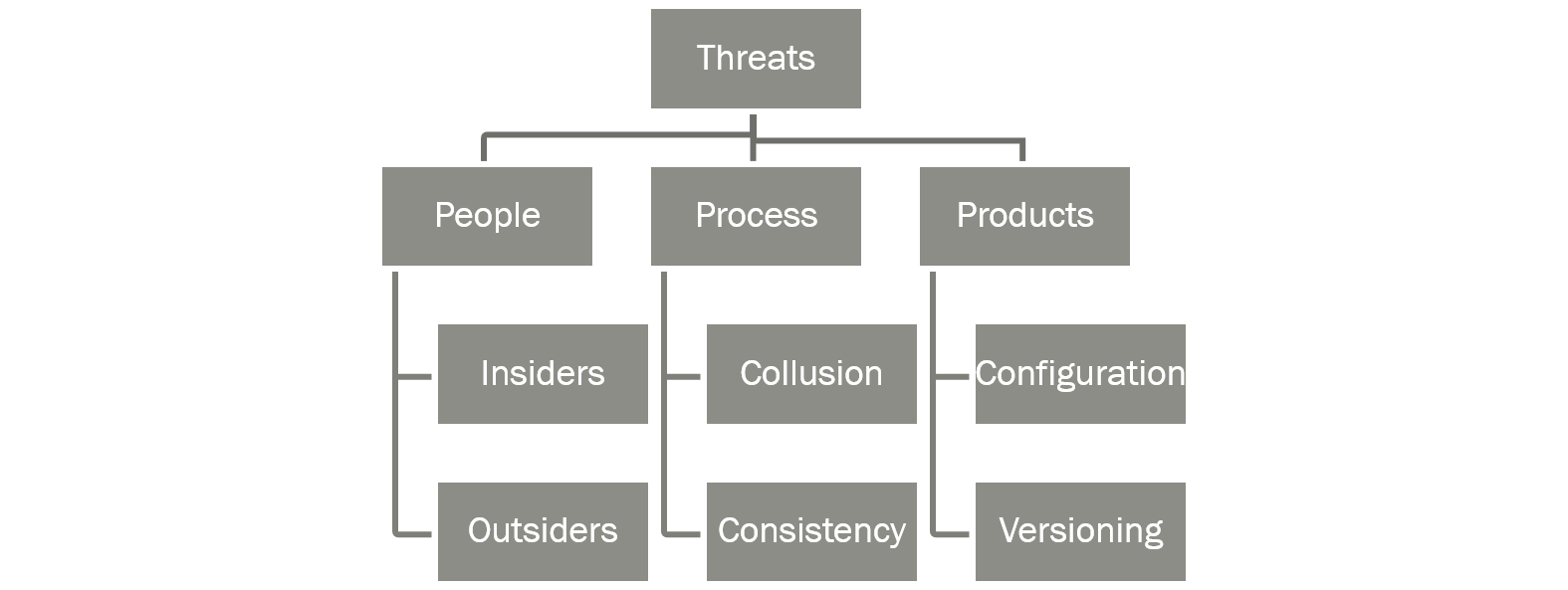
Financial institutions need to maintain the confidentiality, integrity, and availability of customer data. When these expectations are not maintained, then it results in economic loss and public embarrassment for NCUF.

Various regulatory boards have established regulatory requirements to create a baseline of policy expectations.

* *Sarbanes and Oxley Act (2002).* Requires audit and control systems
* *Payment Card Ind. Data Security Standard (PCI)*. Requires encryption of financial data
* *General Data Protection Regulation (GDPR)****.*** *Requires European data to reside in the EU*

# Taxonomy of Risk

Figure 1: Taxonomy



A taxonomy represents a hierarchical system for entity classification. NCUF uses this approach to group related items together and then prioritize which the buckets to tackle first. It would be prohibitively expensive to mitigate all business risks entirely. Vulnerabilities exist at the intersection of system susceptibility, threat accessibility, and actor capability (Baskerville, Rowe, & Wolff, 2018). Often removing one of these facets is more economical than the other.

# Primary Risks

CyberSecurity refers to a collection of mechanisms and processes that constrain risk to business systems by ensuring they meet performance and consistency expectations, even under erroneous conditions (Mickens, 2018). These erroneous conditions arise due to both malicious and negligent scenarios, degrading the confidentiality, integrity, and availability of our service offerings.

Nearly half of security incidents come from negligence, a quarter from external actors, and the remainder from technical glitches (Valiente, 2017). These statistics highlight the criticality of starting with controls that limit the blast radius of human errors. NCUF is always one lousy system command away from executing a disaster recovery process.

# Misconfiguration Networks

The misconfiguration of service policy can result in security incidents like outages or device compromise. Administrating network topologies are highly complex dynamic environments. Without automation, failures will eventually creep in.

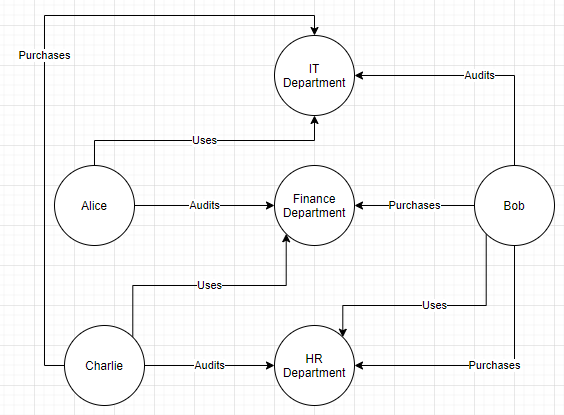
NCUF’s network topology spans five sites, and this introduces challenges keeping configuration settings coherent. For instance, the reuse of MAC addresses causes erroneous routes. There are several different solutions to this problem, such as partitioning the address space, where the first MAC address byte encodes the site number. Another approach could rely on Enterprise Resource Management (ERM) software to implement a virtual MAC address check-out solution.

# Collusion and Segregating of Duties (SoD)

The objective of SoD is to remove single points of failure from the organizational hierarchy. For instance, if an employee can purchase equipment and audit the inventory, then they could be tempted to make false invoices and embezzle the funds. NCUF minimizes this scenario by assigning these roles to different employees. However, there is also a risk that these different team members join forces, through collusion, to sidestep the protections.

One potential solution is to assign responsibility such that cross-validation occurs (see Figure 2). Alice is a manager in IT that audits the finance department. She has little incentive to collude with the primary user Charlie because Bob audits those interactions. Meanwhile, Bob is a manager in the HR department with auditing by Charlie.

Figure 2: Minimizing Collusion & SoD



# Avoiding Compromise

External actors attack the organization with vulnerability scanners, phishing scams, denial of service (DoS), and malware (Lee, Moon, & Park, 2017). The business can reduce the success of these attacks with firewall policies, anti-virus, and Intrusion Detection/Prevention (IDS/IPS) software.

When a compromise is detected, then the machine needs to be taken out of the rotation and investigated. After discovering the origin of the breach, updates to the security profile need to account for that scenario. These changes might include changes to patch management strategies, changes to access policy, quota management, or a broader mitigation effort.