Assess Discovery Risks

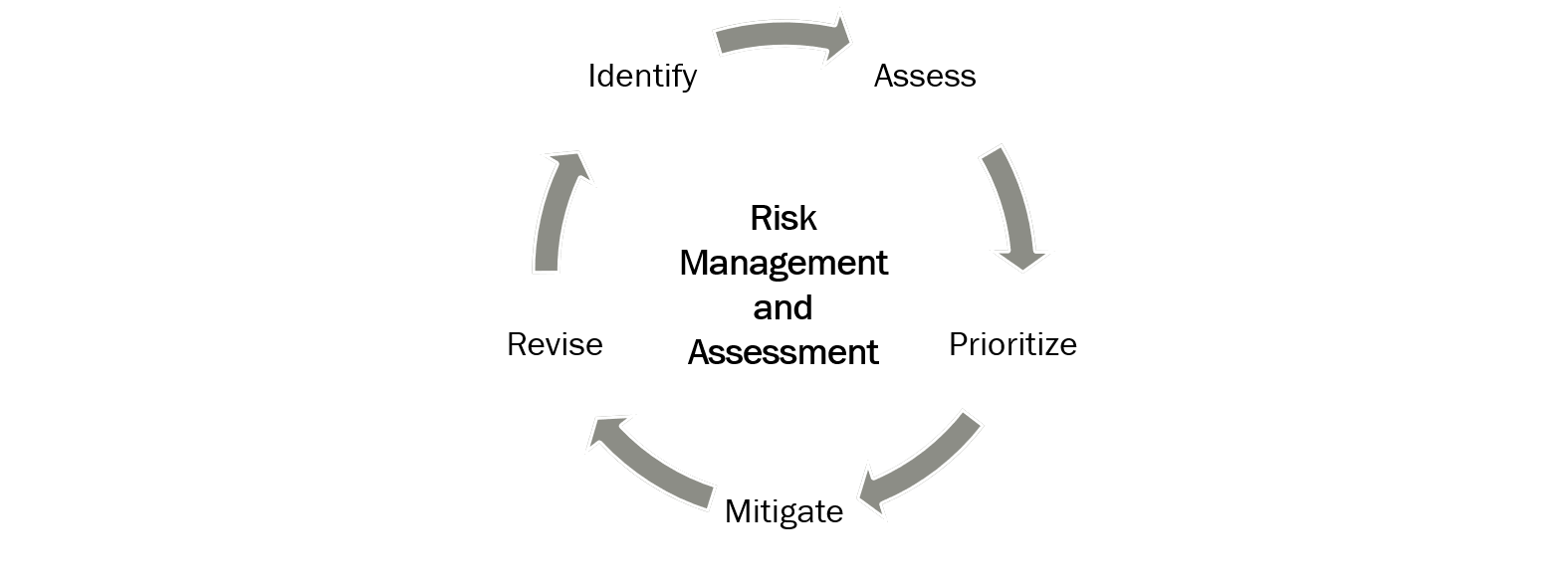
Nate Bachmeier

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

June 7, 2020

# Introduction

Figure 1: Risk Assessment



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 using mitigation, avoidance, and transference strategies (Baskerville, Rowe, & Wolff, 2018). 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 address both ‘when and how’ these threats are resolved (Dai Zovi, 2019). Those answers typically come from a feedback loop of identity, assessing, prioritizing, mitigating, and revising vulnerabilities (Gillies, 2011).

# Risk Assessment Requirements

Security assessments perform an audit of the people, processes, and products that are involved in a business workflow (Hennig, 2018). This analysis needs to assess the controls at integration points and whether they are appropriate protections for the criticality of those resources (Combass & Shilling, 2016). Threat modeling is a formal process the enumerates these interactions and considers different spoofing, tampering, repudiation, disclosure, and elevation attacks (Kohnfelder & Garg, 1999).

After identifying the potential threats, a strategy needs to remove the vulnerability. 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.

# Regulatory Requirements

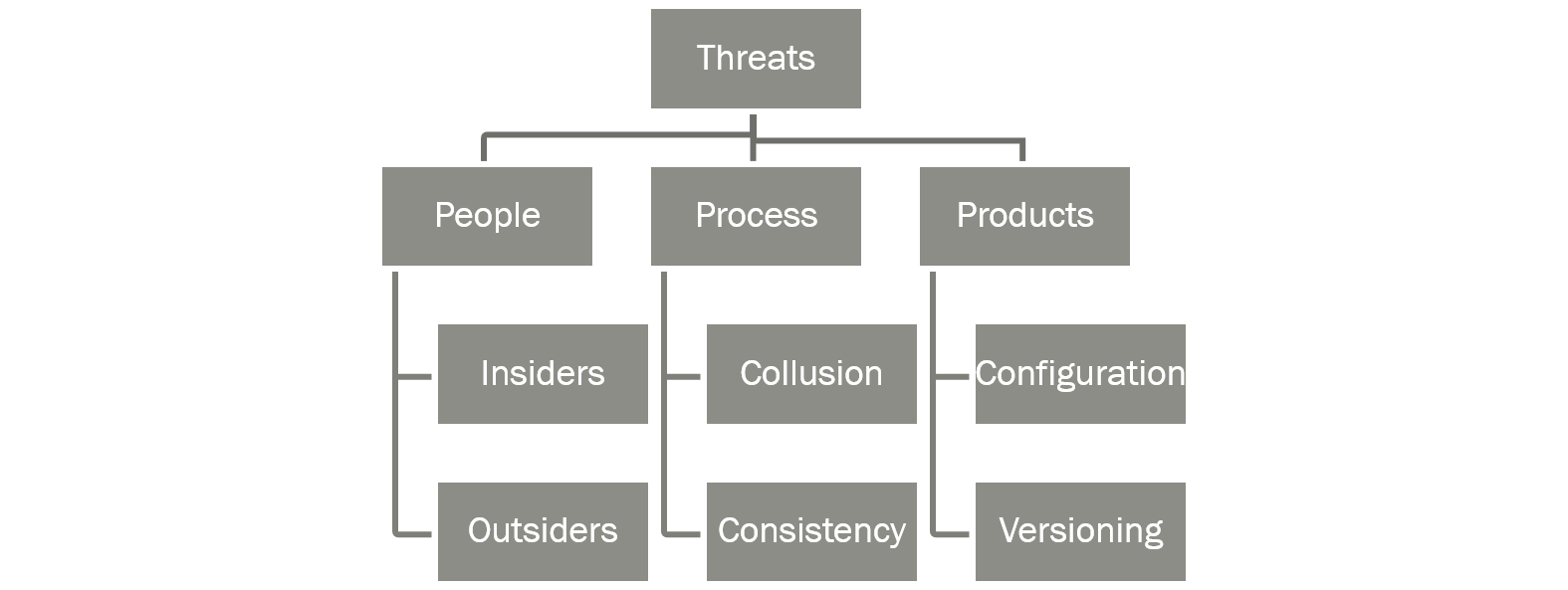
Financial institutions need to maintain the confidentiality, integrity, and availability of customer data (Brown, 2015). When these expectations are not maintained, then it results in embarrassment and economic loss.

Various regulatory boards have established policy baselines that must adhere too.

* *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 2: Taxonomy



A taxonomy represents a hierarchical system for entity classification (see Figure 2). NCUF uses this approach to group related items together, to convey the context of each task and enable prioritization conversations.

# 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.

# Misconfiguration Networks

The misconfiguration of service policy can result in security incidents like outages or device compromise.

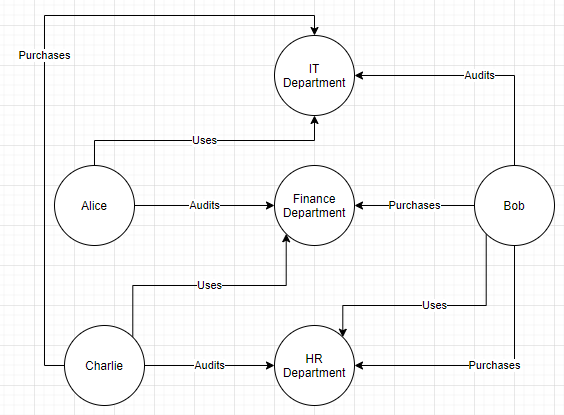
NCUF’s network topology spans five sites, and this introduces challenges keeping configuration settings coherent. For instance, the reuse of MAC addresses causes erroneous routes and inconsistent transmissions. There are several different solutions to this problem, such as partitioning the address space, where the first byte in the MAC address 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 SoD protections.

One solution is to assign responsibility such that cross-validation occurs (see Figure 3). 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. This cross-validation solution also helps to minimize the number of employees for cost-saving purposes.

Figure 3: 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 that 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 the intrusion. That could involve changes to access controls, patch and quota management, or a broader mitigation strategy effort.

# References

Baskerville, R., Rowe, F., & Wolff, F. (2018, February). Integration of information systems and cybersecurity countermeasures. *Special Interest Group on Management Information Systems (SIGMIS) Databases, 49*(1), 33-52. doi:https://doi.org/10.1145/3184444.3184448

Brown, T. (2015). A Primer on Data Security. *CPA Journal, 85*(5), 58-62. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=ofs&AN=102909750&site=eds-live

Combass, T., & Shilling, A. (2016). Integrating cybersecurity into NAVAIR OTPS acquisition. *Institute of Electrical and Electronics Engineering AUTOTESTCON*, (pp. 1-5). Anaheim, CA. doi:https://doi-org.proxy1.ncu.edu/10.1109/AUTEST.2016.7589632

Dai Zovi, D. (2019). Every Security Team is a Software Team Now. *Blackhat USA.* Black Hat. Retrieved May 2020, from https://www.youtube.com/watch?v=8armE3Wz0jk

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM Journal, 23*(4), 367-376. doi:http://dx.doi.org.proxy1.ncu.edu/10.1108/17542731111139455

Hennig, N. (2018). Privacy and Security Online: Best Practices for Cybersecurity. *Library Technology Reports, 54*(3), 1-37. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=ehh&AN=128707555&site=eds-live

Kohnfelder, L., & Garg, P. (1999, April 1). *The threats to our products*. Retrieved June 7, 2020, from Microsoft Security Blog: https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/

Lee, J., Moon, S., & Park, J. (2017, July). CloudRPS: a cloud analysis based enhanced ransomware prevention system. *Journal of Supercomputing, 73*(7), 3065-3084. doi:https://doi-org.proxy1.ncu.edu/10.1007/s11227-016-1825-5

Mickens. (2018, August 16). *Why Do Keynote Speakers Keep Suggesting That Improving Security Is Possible?* Retrieved from YouTube: https://www.youtube.com/watch?v=ajGX7odA87k

Valiente, C. (2017, October). Addressing Malware WITH Cybersecurity Awareness. *Information Systems Security Association Journal, 15*(10), 16-22. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=tsh&AN=125478200&site=eds-live