Week 5: Create a Risk Management Framework

Nate Bachmeier

TIM-8190: Computer Science Policy and Strategy

October 3, 2021

Northcentral University

# Create a Risk Management Framework

Traditional businesses have a smaller attack surface from well-understood sources, such as inventory management, performance management, and petty crime. In contrast, cyber risk is dynamic and constantly evolving (Grobler, 2018). NCU-F’s Chief Risk Officer (CRO) must define policies and procedures that address cyber risk through cyber security. 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 from malicious and negligent scenarios, degrading confidentiality, integrity, and availability of our service offerings.

## Categorize Potential Vulnerabilities

When categorizing these risks, a taxonomy needs to consider the incentives and origin of the risk (Li & Liao, 2018). Incentives of malicious and negligent behavior are drastically different and require unique approaches. Kosub (2015) proposes the terms cyber-risk (negligence) and cyber-crime (maliciousness) to distinguish between these scenarios. For instance, technical support staff wants to follow the cultural norms set by their employer and minimize any friction in completing their assignments (Weston, Conklin, & Drobnis, 2018). Meanwhile, malicious actors seek to exploit espionage, sabotage, and subversion attacks (Matsubara, 2014). While policies and training can reduce the impact of erroneous technicians, those solutions do not apply to external criminals.

The next level of the taxonomy includes specific situations involving various people, processes, and products. Privacy and cyber risks to a process can come from insufficient authorization and auditing controls. For instance, failure to maintain accurate inventory records can cause inaccurate accounting of the corporate position. Another example might come from a weak authorization policy that allows low-level employees to reboot mission-critical systems. In contrast, cyber-crime might leverage repudiation attacks against a process such as requesting a refund before completing the purchase.