Section 1: Week 2: Importance of Risk Mitigation Strategies

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 14, 2020

North Central University

# Importance of Risk Mitigation Strategies

## Process for categorizing risks for privacy and 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 due to both malicious and negligent scenarios, degrading the confidentiality, integrity, and availability of our service offerings.

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. 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 same vectors do not apply to external criminals.

The next level of the taxonomy includes specific situations involving various people, process, 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 attack processes through repudiation attacks, such as requesting a refund before completing the purchase.

Bit-rot is technical jargon for describing a product that is not consistently maintained. Over time a lack of attention to patch management and policy updates results in fragile systems that are less secure and increase the risk to data privacy. For instance, malware predominately targets vulnerabilities that are over one year old (Emery, 2017). Another common challenge comes from abandoning partial state on these devices, allowing unintentional access for malware and other intruders.

## Importance and value of corporate data and the cost of ownership

## Process of risk assessment or analysis

## Risk management strategies and countermeasures

## Definition of each information security role

## Relationship between roles and role of cybersecurity professional