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. Security researchers can uncover additional risks by assessing the impact of each STRIDE attack category (Kohnfelder & Garg, 1999)(Table 1).

Table 1: Cyber risk under STRIDE

|  |  |  |
| --- | --- | --- |
| Risk | Cause | Example |
| Spoofing | Failure to authenticate a resource as genuine | An email asks for a bank credential |
| Tampering | Failure to prevent resource manipulation | Changing the amount on a check |
| Repudiation | Failure to audit an operation | Disputing the cashier gave me change |
| Information Disclosure | Failure to conceal private communication | Discussing trade secrets at a restaurant |
| Denial of Service | Failure to isolate multi-tenant traffic | Hundreds of callers overloading the front-desk |
| Elevation of Privileges | Failure to enforce security policies | Alice asks her Manager to update the timeclock |

After identifying cyber risks, the organization must consider the threat impact and likelihood (Baskerville, Rowe, & Wolff, 2018)(Figure 1). If the impact is critical, the business must transfer that risk or avoid the scenario entirely.

Figure 1: Decision Matrix

Graphical user interface, application, table

Description automatically generated

For instance, foreign markets lack intellectual privacy protections, which might discourage releasing cutting-edge technology to those audiences (Krebs, 2019). In other scenarios, avoiding a hostile market or business activity is impossible, making hedging with insurance a more appropriate response. For example, it might be prohibitively expensive to have redundant manufacturing plants, while unlikely, the business could become insolvent if the building burnt down. These situations of catastrophic failure are ideal for insurance and other risk transference solutions. If the situation is less impactful, then the company might choose either self-insurance or self-protection. A self-insurance strategy might be cash reserves or options contracts to acquire resources during extreme demand or short supply.