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. Self-insurance (e.g., reserves) and self-protection (e.g., controls) are alternative strategies for less impactful events.

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.

# Applying Risk Categorizations

NCU-F wants to create a corporate culture that promotes collaboration through standard operating procedures. Reimagining the business comes with several potential vulnerabilities and risks across its political, operational, and Information Technology and Communication (IT&C) models.

## Political Vulnerabilities

When the organization introduces change, there will be internal opposition as staff becomes unclear about the future direction. During the transition period, middle managers will shift ownership and control to their peers, potentially leading to hostility and a loss of personal identity. Those leaders could deprioritize the standardization efforts for their teams. This behavior would cost NCU-F two to five additional years before transforming. Within that time, competitors could make significant advancements, and essential staff will accept new roles in different companies.

## Operational Vulnerabilities

Operational vulnerabilities will likely originate during this transformational period. For instance, today, each business manages assigns staff to support a particular hardware topology. This approach is challenging to scale and uneconomical compared to treating servers as pets versus cattle (McCance, 2012). While standardized resources (cattle) has many benefits, the migration risks losing manual edits to existing servers (pets). Presumably, those changes took place for a reason, and removing them will introduce regression risk. Specific regressions, such as seasonal processes, can remain broken for months before reporting an error. Additionally, changes in provisioning and monitoring models inherently include team ownership. When staff is unclear regarding area ownership, it creates delays escalating and routing issues, increasing Time to Detect / Time to Mitigate (TTD/TTM) latencies.

## IT Vulnerabilities

Supporting collaborative communication requires extensive changes across the IT&C ecosystem. These new pathways will expand the threat model and attack surface, necessitating additional controls and procedures. When these forces come at odds, it creates friction that either carries an undue risk or costs the business time and resources. Busby, Green, and Hutchison (2017) describe this situation through equilibrium between adversaries, users, and risk managers, whose goals are to maximize risk, maintain convenience, and minimize risk. For instance, the senior leadership can mandate complex password policies. However, beyond a certain threshold, the staff can no longer retain the random string to memory. They will either write it down or increase calls to the help desk.

## Provisions and Processes for Risk Assessment

Enterprise environments are fluid and dynamically change every day as thousands of employees make improvements. Additional churn seeps in through dependent third-party components and Commercial Off the Shelf (COTS) applications. NCU-F needs to implement formal procedures for identifying infrastructural risk at each layer, supported through automation (see Table 2).

Tool vendors often support industry-standard vulnerability scoring systems, such as the Common Vulnerability Scoring System (CVSS) (NIST, 2021). This scoring model considers several dimensions like exploitability, complexity, and prerequisite steps. For example, a vulnerability that compromises the domain controller could be a grave concern if the attacker first gains access to a secure data center. In that case, the probability does not warrant resources to mitigate the defect. However, specific requirements could impact that decision, such as the data center resides in a foreign country. Implementation teams should always gain clarity to these situations by consult with the legal, security, and compliance counterparts.

Table 2: Example Assessment Tooling

|  |  |  |
| --- | --- | --- |
| Infrastructure Component | Tooling Requirement | Description |
| Network | IDS/IPS | Packet monitoring |
| Network | Firewalls / QoS | Traffic shaping |
| Operating System | Antivirus | Malicious software removal |
| Operating System | Patch Management | Keeps software updated |
| Operating System | Systems Management | Enforces Group Policies |
| Operating System | Trusted Platform Modules | Enforces boot loader and kernel security |
| Data | Disk Encryption | Maintains hardware integrity |
| Data | Public Key Infrastructure | Cryptographic capabilities for data in rest and in-transit |
| Software | Vulnerability Scanner | Detects known issues in applications |
| Software | Change Management | Tools for versioning modifications |
| Transportation | Web Application Firewalls | Layer-7 monitoring for SQL-i and XSS attacks |
| Employees | Training | Continuously raising the bar |
| Employees | Anti-Phishing Tools | Processes to filter or highlight potential email risks |
| Employees | Work Health Indexes | Keeping a pulse on morale can surface overworked and dissatisfied staff |
| Databases | Backup Management | Point-in-time recovery solutions |

# Mitigating Vulnerabilities

There are numerous threats to the organization’s plans to modernize its communication strategy and standardize operating procedures. The business must create a prioritized list and establish policies, standards, and controls.

## Political Mitigations

Political confrontation (e.g., land grabs) results from misalignment between customer outcomes and internal rewards. Bryanr and Carr (2021) describe Amazon’s framework for forcing this alignment through its compensation model. Essentially, an employee’s base salary maxes out at $175,000. Beyond this amount, additional rewards come from company stock that vests over two to four years. Leaders merely accepting more ownership does not change their stock grants. Employees can only receive more company shares through customer results that demonstrate next-level leadership.

While significant benefits come from ensuring that leaders focus on long-term success, changing employee contracts can be challenging. In the interm senior leaders can define span and control thresholds, which the IT department implements. For instance, a manager should have no more than ten direct reports. Reporting systems can surface any violations and involve executive steering committees to make appropriate alterations.

Additionally, the business needs forums for communicating corporate decisions and debating the impact. Today, staff use external resources like Team Blind because their employers do promote these discussions. However, as the business moves toward more collaboration, it will naturally follow with more contention. Since these conversations will happen, either way, it is in NCU-F’s best interest to host a secure platform where internal secrets leak into the public internet.

## Operational Migrations

The most critical risks come from important details becoming lost, such as device and network configurations and issue routing. NCU-F can mitigate these concerns through people, processes, and products.

First, any centralized DevOps team should contain people that worked in team-specific operatins teams. These existing members have experiences and diverse perspectives that can improve the DevOps organization.

Second, existing processes must integrate into new systems where possible. Previously, policies required networking teams to use networking-{team}@ncu.f alias conventions. After converging the network support teams, these old email addresses should become forwards. Finally, automated replies should update the sender with the revised policy.

Third, the company must aggressively move resource metadata into the central repository. This store gives a consistent organizational view into its artifacts and other assets.

## IT Mitigations