Section 3: Week 8: Corporate Risk Management Plan

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

July 26, 2020

North Central University

# Corporate Risk Management Plans

NCU Financial (NCU-F) operates on a finite budget and must prioritize investments into features and services. On the one hand, the business would like to spend all available resources delivering its core mission, enabling personalized investing. Allocating time and money into other projects might even appear to detract from this mission and feel like a waste. However, along the journey are risks from a litany of sources that can derail progress, cause financial hardship, and harm the organization’s reputation (Erickson & Neilson, 2018). Using a security framework, such as COBIT or NIST Cybersecurity, formalize processes for identifying and approaching threats from these risks (Devos & Van de Ginste, 2015). It would be economically prohibitive to remove every threat against the organization. Instead, a prioritization discussion must delineate between threats and vulnerabilities.

Assessing and addressing vulnerabilities requires a mixture of proactive and reactive controls that constrains the blast radius of malicious and negligent people, processes, and products. Meeting that expectation requires a corporate strategy that minimizes risks using mitigation, avoidance, and transference strategies (Baskerville, Rowe, & Wolff, 2018). Deciding the appropriate solution is contextually sensitive and can also require tooling and redundancies. For example, data loss can occur from ransomware, hardware failure, or accidental deletion. While the reasons vary, the resolution is too perform a disaster recovery process. If the business accounts for that situation ahead of time, then systems will already exist and impact to service continuity is curtailed.

Lastly, the most brilliant risk management plans are ineffective without processes to verify and disseminate across the team members. Over time business priorities and technologies change, necessitating the need to confirm these procedures continue being accurate.

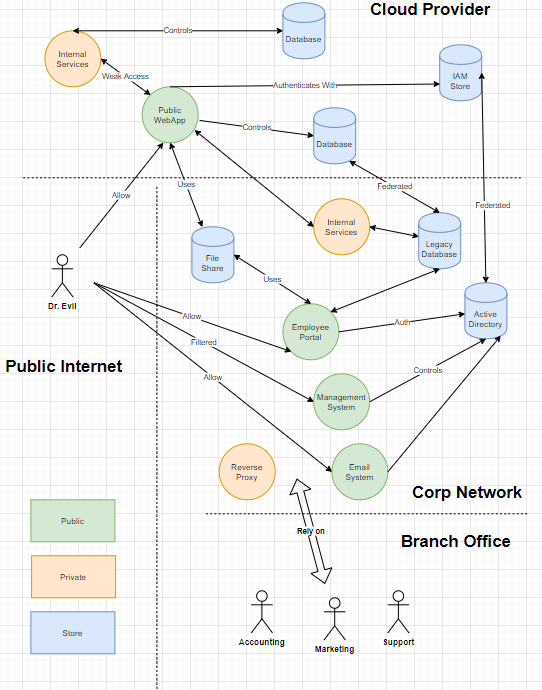
# Section I: State of the Organization

Before building a risk management plan is to assess the state of the organization. This introspection process evaluates the existing system and applications, along with identifying challenges that come with the business model.

## Corporate management of systems and applications

NCU-F has significant investments in its private data center resources, which hosts several legacy and business-critical systems (see Figure 1). There are fifty branch offices across the country that transact with the corporate network using Virtual Private Networking (VPN). Around four years ago, the business began transitioning to a hybrid cloud model with plans to decommission the private data center eventually. Most recently, the global pandemic has forced most employees to work remotely, using a combination of personal equipment, mobile devices, and employer-purchased hardware.

Figure 1: NCU-F Network Topology



The network administration team must define policies and procedures for ensuring the consistency of these different environments. This requirement is challenging because resources ownership extends over multiple parties, and technology stacks range drastically. For instance, the cloud solution uses a mixture of Infrastructure, Platform, and Service as a Service (IaaS, PaaS, and SaaS) platforms. Meanwhile, client technicians must support Microsoft Windows, Apple iOS, and Google Android. Further complicating matters, the applications that run on these systems execute with varying levels of isolation and trust. While the business can mandate anti-virus products and patch management, there is still a high probability that these machines will become infected with malicious software.

## Threats Every Organization Faces

Traditional threat discovery processes focus on technical management using filter and barrier products, such as firewalls and Intrusion Detection and Prevention Systems (IDS/IPS). A more modern and mature process includes information governance and compliance concerns within the model (Bobbert & Mulder, 2015). These additional considerations include policies, continuity planning, ethical norms, and legal expectations.

CyberSecurity policies and controls refer 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 (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.

## Organizational Chart

Table 1: Stakeholders

|  |  |
| --- | --- |
| Team/Role | Primary Concerns |
| Customers and other end-user | Privacy, reliability, usability, and available |
| Security Engineers | Confidentiality, integrity, and availability |
| Software Engineers | Reliability, observability, and performance |
| Program Managers | Functionality, predictability, and extensibility |
| Support Engineers | Observability and supportability |
| User Experience (UX) | Convenience and performance |
| Legal and Compliance | Privacy and confidentiality |
| Marketing and Sales | Functionality and consistency |
| Accounting and Finance | Economical and profitable |
| Senior Leadership | Connects with the broader company strategy |
| Technical Writers | Consistency and explainability |
| Network Security Engineers | Authentication, authorization, and auditing |
| Operations | Observability, reportability, and discoverability |

Implementing enterprise software solutions requires teams of professionals from across multiple disciplines, each with a unique perspective. Alignment and inclusion of these different perspectives are critical, or it results in distortion, leading to political confrontation and critical misses. These diverse ideas originate from industry norms that seek to improve consistency, accuracy, and efficiencies for different aspects of the business (see Table 1). While there are advantages for teams to operate in vertical silos, such as the speed of decisions, an integrated framework draws on the expertise across the company (Nicho, Khan, & Rahman, 2017). When all stakeholders can participate in the process, it culminates in releasing the right product at the right time.

# Section II: Objectives of Risk Management Plan

The fundamental purpose of a risk management framework is to identify and prioritize threats, plan and correct those issues, and finally verify and monitor those changes (Gillies, 2011). While it is possible to mitigate specific scenarios pre-emptively, other challenges require reactive compensation. For instance, anti-virus software can reduce the chances of ransomware corrupting a mission-critical database. However, an extensive catalog of reasons could conclude at the same point (e.g., application defect or drive failure).

NCU-F has finite resources and cannot address every vector that results in a loss of confidentiality, integrity, and availability. Instead, the risk management plan must specifically address a subset of circumstances and default to general recovery procedures for other cases. These decision trees need to consider the influence of both asset classification and failure reasons. For example, if an employee’s workstation becomes unresponsive, the support office might follow a ‘retry-reboot-reinstall-replace’ workflow. Meanwhile, a legacy mainframe might be too costly to touch and need a concise remediation process.

# Section III: Business Impact Analysis

No one likes to think about negative situations, and this causes organizations to under-estimate the likelihood and cost of a security incident (Eling & Wirfs, 2019). In reality, most data breaches cost millions of dollars, with high profile instances reach substantially more (Brown, 2015). The economic impact comes from many sources, such as class action lawsuits, regulatory fines, digital forensics, productivity loss, and additional public relations campaign expenses (Erickson & Neilson, 2018).

# Section IV: Plan of Action and Milestones

# Section V: Risk Reduction for Mobile Device Management

Legacy network environments heavily rely on centralizing information into a single mainframe or data warehouse. Network security teams could protect these resources through border security solutions, such as firewalls and other network access controls. However, this model lacks the convenience and data portability that users expect (Astani & Ready, 2016), leading to the adoption of Master Data Management systems (MaDaMgmt).

The objective of MaDaMgmt is to enable the sharing of business entities and related feeds across the organization (Rivas, Caballero, Serrano, & Pattini, 2017). Now that employees could locally cache information on their corporate laptops and workstations, productivity increased, but ensuring data confidentiality and integrity became more complex. Deploying client management tooling (CMT) allows the administrators to enforce security policy across these edge devices (Tarzey, 2018). However, these CMT products tend to specialize in specific platforms and scenarios, which limits the device supportability matrix for corporate Information Technology (IT) departments. Due to these restrictions, rigid homogenous topologies became the norm instead of allowing the best tool for the job.

Modern networks believe that IT enables the business, not stifles innovation. The emersion of the Bring-Your-Own-Device (BYOD) makes this perspective front and center (Lamolle, Menet, & Le Duc, 2015). With employees are free to use the best tool for their role, it results in highly diverse environments that span multiple technology stacks, like Windows, iOS, and Android. That freedom improves productivity, at the cost of sensitive business information resides on devices not controlled by the organization and partially trusted at best.

## Addressing these issues

Client management tools give the system administrators the ability to define policy centrally and then target groups of workstations. Effective device management needs a similar mechanism that accounts for platform-specific variations. Unified Endpoint Management (UEM) addresses these issues by creating an abstraction layer that can translate corporate governance and policies into device-specific configurations (Tarzey, 2018). For instance, the administrator can mandate the installation of all critical operating system patches. The implementation of this action varies between Windows desktops, Apple iPhones, and Android Chromebooks—though the intent remains consistent. In addition to desired configuration and patch management, UEM platforms can perform operations like remotely wiping the device or requesting inventory reports. These actions enable the administrators to address specific challenges like the lost and stolen device scenarios. Advanced solutions like Microsoft Intune and MobileIron, support sandbox technologies that prevent mixing personal and corporate data (Soseman, 2019; MobileIron 2020). The data context tagging also opens the door for smarter remote wipe scenarios that do not touch personal data like family pictures.

# Section VI: Tooling Recommendations

In addition to standard solutions, such as anti-virus and patch management, the business should also consider intrusion detection systems that rely on signatures (Mehresh & Upadhyaya, 2015). These technologies confirm that the system meets cryptographical proofs that tampering has not occurred. For instance, the operating system can use a Trusted Platform Module (TPM) to confirm the integrity of the boot loader and other critical components. An argument exists for network traffic anomaly detection and HoneyPots (Westcon-Comstor, 2018). However, these tools can report false positives and be challenging to configure correctly.

## Security Information and Event Management

Modern business topologies are dynamic and interconnected, containing components that originate from internal teams, external contractors, and third-party providers. Overtime priorities shift and follow economic incentives to churn out new products and features, causing bitrot to neglected services and new features that lack sufficient security controls (Li & Liao, 2018). Eventually, service failures occur within this complex environment leading to the natural question, “so what happened?” The cost associated with solving this mystery is dependent on the quality of the auditing information.

Half of these moments come from employee negligence, a quarter from system errors, and the remainder from malicious sources (Valiente, 2017). According to this breakdown, there is significant value is auditing all change across every business process. In addition to these failure scenarios, there must also be considerations around industry norms and regulatory requirements. Not if, but when customers file litigation against NCU-F, the business must have documentation that corroborates the truth (Keel, 2015). Otherwise, misconstruing facts could force the business to admit fault erroneously. Likewise, if the mandatory audit trails are not available, then regulatory boards can seek damages for non-compliance.

However, a trade-off exists between performance, storage, and observability, which might limit NCU-F’s ability to collect and persist such an enormous volume of data (Adedayo & Oliver, 2015). When choosing what information to keep, a one-size-fits-all solution does not exist. Instead, the administrators need to categorize the potential value of these various events in terms of needs for experimental and retrospective reconstruction.

While there are many benefits to having a formal SIEM product, it is not a magic box and only provides insights into integrated systems. For instance, NCU-F exposes a public enrollment portal that follows a standard three-tier architecture (see Figure 1). If monitoring exists only for the database, then it can be perplexing to investigate the reason behind specific alerts. Perhaps a careless technician is servicing a request against the wrong server. Alternatively, the inclusion of router and switch logs could detect this traffic anomaly. Unfortunately, SIEM providers often follow the “more for more” mantra and charge higher licensing fees for additional coverage. The support of different technology stacks can also depend on the focus areas of the SIEM platform (see Table 1). Before choosing a provider, the organization needs to assess the most concerning scenarios and acceptable costs. For example, a simple branch office that already uses McAfee anti-virus will likely find McAfee Security Manager a great fit.

# Section VII: Privacy and Risk from Cloud Environments

## Abstract Borders, Cloud, and XaaS

Traditional cybersecurity solutions focus on hardening the network parameter with firewalls and vulnerability scanners. However, this approach is no longer sufficient as attackers center their efforts on the application layer (Astani & Ready, 2016). By design, anonymous users can interact with the organization through public interfaces, such as web services and email. When malicious actors exploit Structured Query Language Injections (SQLi) or embed ransomware into mail attachments—it bypasses these network barriers and allows unauthorized access to information. Further complicating matters, the boundary of the network is becoming more abstract due to the notion of “everything as a service” (Paller, Mahalik, Skoudis, & Ullrich, 2020). For instance, 40% of enterprises are in the process of uplifting mission-critical services, like identity and authorization, into third-party providers (Galinec & Steingartner, 2017). Shifting ownership to these provides does not mean transferring the responsibility of risk. Users do not care if DropBox or Amazon owns the physical server—they entrusted the stewardship of their data to HTM and will blame them for negligent handling. Modern businesses need to evolve their controls to meet the challenges of these application-specific vulnerabilities using strategies that encompasses people, processes, and products.

# Section VIII: Incident Response Process

The attack against the NCU-F application interface has enabled international actors to install multiple strains of malware onto the network. The administrative team must devise a response plan to contain the infestation and restore business continuity. While the number of critical issues can be overwhelming, the organization must follow a methodical approach to remediate the situation. The remediation strategy should follow industry best practices, like the guidance from COBIT and NIST Cybersecurity Framework.

## Corporate Network

This mitigation approach must use Identify-Plan-Do-Check feedback loops, which prioritizes assets and objectives that are the most critical first (Radhakrishnan, 2015). Ransomware has corrupt the mission-critical database and payroll department. Without access to that database, NCU-F cannot continue any operations. Meanwhile, the accounting department can temporarily resort to more mechanical processes or offload to third-parties. After identifying the most critical systems, planning needs to stop the bleeding before drilling into a longer-term solution. For example, deploying the most recent backup of the database, upgrading the software patches, and installing new malware definitions might be an acceptable first step. However, later cleanup will need to revisit configurations and additional access controls.

## Branch Offices

The network administration team will need to quarantine systems that fail to meet specific conditions. One solution is to use System Health Validation (SHV) to confirm the compliance of an endpoint with intranet policies (Microsoft, 2018). These policies can include checks that virus signatures and system patches are recent. A risk exists that the attack could rely on zero-day exploits that can reinfect the machines, though, in practice, this is less likely to occur. Nearly 99% of all malware attacks use public vulnerabilities that are over a year old (Galinec & Steingartner, 2017). This behavior is partially due to reliable zero-day vulnerabilities being worth tens of thousands of dollars on the dark web, versus public exploits are often free (Emery, 2017). However, nation-states and other well-financed actors might have economic means for using such a weapon.

## Cloud Technologies

NCU-F uses VPN technologies for extending the corporate network into the cloud infrastructure (see Figure 1). Operating a hybrid cloud creates many efficiencies but can introduce single points of failure. For example, during the malware attack, the public web application is offline due to dependencies on private datacenter systems. Instead, replication technologies could maintain copies of those private resources within the cloud, constraining the blast radius to the intranet’s edge. The company should also consider the inclusion of anti-malware technologies at various strategic points in the topology. For example, incoming files for the public web application need to stage the content for static and dynamic analysis through tools like ClamAV and Cuckoo (Kilgallon, De La Rosa, & Cavazos, 2017).

## People

One of the byproducts of modern networks having abstract borders is that the rampant malware does not stop at devices owned exclusively by NCU-F. Instead, it continues onto personal devices, which triggers automated backup systems and social media services to further propagating across friends and family members (Balupari & Singh, 2017). At a minimum, the organization has an ethical obligation to guide team members and provide anti-virus licenses. Depending on the specifics, the company could also be liable for any damages to employee property.

## Coming Back Stronger

After addressing the initial crisis, the business must come up with alerting and monitoring enhancements to become more proactive against future attacks. One reason that this attack will be tedious to recover and very expensive is because of the extensive infestation across the entire topology. Using endpoint protection software would give the administrators more forewarning that this issue was becoming uncontrollable. While the business might lack the expertise to handle that scenario, it could have begun seeking external consultants and third-party experts.

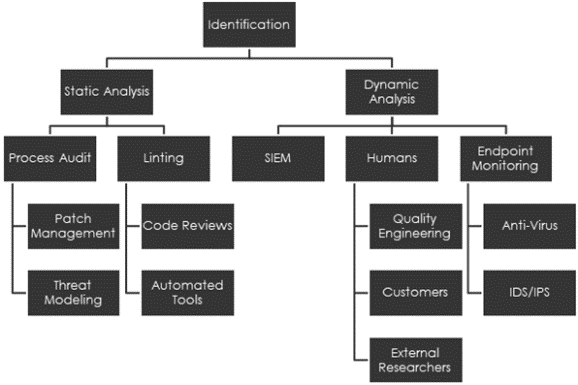
# Section VIII: Vulnerability Assessments

A vulnerability occurs at the intersection of (1) system susceptibility; (2) threat accessibility; and (3) threat capability (Baskerville, Rowe, & Wolff, 2018). Nullifying any of these predicates mitigates an attacker’s ability to compromise the confidentiality, integrity, and availability from that specific threat. The costs to address these predicates range substantially and are highly scenario specific. For instance, the legacy mainframe lacks support for modern network encryption and authorization protocols. Upgrading or replacing the system are not feasible solutions, though moving the server to a private network disconnects the threat’s accessibility. Another configuration, such as a public web application, might experience the opposite problem where patching the software defect is a more natural path forward. Over a long enough period, all vulnerabilities are discovered and exploited (McLane, 2018). Processes need to combinations of proactive and reactive defenses to defuse these timebombs before they explode.

## Identification

Detection of the vulnerability might come from static (offline) or dynamic (online) analysis (see Figure 3). Static Analysis Tools (SAT), such as SonarQube and Checkmarx, parse the source code into graph-like structures and then run queries to find defects in the application. While there is the potential of encountering false positives and false negatives, these lint checks are effective at catching problems in proprietary systems. Dynamic Analysis Tools (DAT) use telemetry to monitor for security-critical events, making it ideal for black-box situations and discovering unknown unknowns. Outside of tooling, periodic process audits and patch management solutions can surface that a problem exists.

Figure 3: Identification Strategies



## Plan

The full impact of a vulnerability might not be immediately visible, as engineering teams often copy-paste existing code and infrastructure into multiple locations. During the planning phase, the senior leaders need to agree on a communication strategy and proposal for introducing the new changes. Consider a scenario where insufficient controls exist for a shared database. Arbitrarily adding defenses will break downstream processes and cause a production outage. Like other software projects, an iterative design must occur that seeks the maximum immediate value (Lam, 2016). Though not ideal, the security team needs to weigh the potential schedule risk that comes from doing everything upfront. Perhaps this means only protecting against one of N situations initially and returning to the others later.

## Mitigation and Verification

Mitigating the vulnerability could be a trivial change to a configuration file or require massive changes to the infrastructure. These changes present multiple risks to the organization, such as degrading performance (e.g., encryption or verbose logging) or creating new failure points (e.g., surfacing broken code). In parallel to standard regression automation, the quality assurance teams need to confirm other permutations of the exploit are unsuccessful. For example, a cross-site scripting defect existing in the enrollment portal (see Figure 1) via the query string. Any mitigation validation plan must also review the other page parameters.

## Respond

Many factors influence NCU-F’s requirement to respond publicly about the vulnerability, such as legal and compliance requirements (Fonseca & Ramaswamy, 2014). Where regulatory mandates do not exist, the company must weigh the ethical obligation to customers and stakeholders that expect full transparency. If the business attempts to cover up the mistake, only to find details leaked to the media, removes substantial trust, and might irrefutably harm its public image. Given the numerous landmines that may exist, the security team should involve members of senior leadership and other stakeholders (e.g., general counsel or public relations).

# Section IX: Disaster Recovery

The operations and security teams at NCU-F seek to reduce risk to the minimum level possible. However, many risks are unavoidable or only partially mitigated due to resource constraints. For instance, an ultra-secure laptop that restricts user access to a finite set of functions could still experience a hardware failure. Lightning could strike the building, and it immediately burns to the ground. A global pandemic could halt international supply chains and force all works to shelter-in-place. There is virtually an unlimited number of scenarios that did not meet the bar for proactive mitigations and will require reactive compensations.

The compensation strategy will need to follow a procedure that restores service. If the procedure is poorly defined or not implemented, then the Mean Time to Recovery (MTTR) can be unacceptably long, creating new risks to the business. These risks need a prioritization discussion that chooses which ones become self-protected, self-insured, transferred, or deferred (Baskerville, Rowe, & Wolff, 2018). Those conversations will need to consider the likelihood and potential costs under a deferment.

## Remote Locations

## Inventory Management

## Backup and Recovery

There are dozens of scenarios that result in data becoming corrupt or inaccessible, such as hardware failures, ransomware, accidental deletion, and application corruption. Mitigating these situations requires controls that backup digital business artifacts and provide capabilities to restore that information promptly. This control needs to extend beyond sensitive documents to handle circumstances like reimaging workstations and servers. After creating the archives, the business needs a strategy around the encrypting and hashing to ensure confidentiality and integrity. When this does not occur, then malicious actors could acquire secrets or tamper with historical records (e.g., repudiation) from the copy.

## Remote Site Fail-Over

# Section X: Plan Verification

## Implementing Drills

## Assessing Drills

# Section XI: Dissemination

## Plan Distribution

The adoption of any process requires sponsorship from executive leadership and proper communication to the troops (Weston, Conklin, & Drobnis, 2018). When either the top or bottom of the organization lack agreement in the solution, it will not become a priority, and team members will sidestep it. Instead, having a cultural alignment ensures that the standard operating procedure makes safe decisions that minimize risk and privacy concerns. For instance, NCU-F’s intrusion began with a phishing attack. Security awareness training could reduce the likelihood of that scenario but not eliminate it (Hunt, 2019). Through a similar mechanism, RSA became compromised via malicious emails, automatically triggering a zero-day exploit in Adobe Flash (Leyden, 2011). After slipping past the firewall, many enterprise environments lack defense-in-depth controls allowing lateral movement across the network (Stevens, 2018). Removing these auxiliary threats requires a fundamental shift in approach that centers around zero-trust and an assume breach mindset. Promoting such a shift is only possible under a shared vision of success and collective agreement that change is necessary.

## Awareness Training

Negligence from employee actions accounts for nearly half of security incidents in enterprise environments (Proctor & Chen, 2015). This group represents both people that want to do the right thing and the most significant slice of the pie. Controls need to exist through compliance training that communicates the expectations and rationale of HTM. For instance, flagging email as originating from an untrusted source provides little value when the employee does not understand the meaning of the flag. Usability studies consistently find that security-critical markings on resources fall on deaf ears when the audience is non-technical (Hunt, 2019). Training corporate norms can also discourage dangerous behavior, such as installing unauthorized software of company devices or using weak passwords. However, many of these concepts are easier said than done, as users will seek the path of least resistance to accomplish their goals. Administrators need to provide familiar integrations that become a natural part of the workflow, not an overwhelming burden on the side.

## Formation of Emergency Committee Personnel