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

The core objective of NCU Financial (NCUF) is to deliver on its mission of world-class banking services. Meeting that expectation requires a corporate strategy that minimizes risks using mitigation, avoidance, and transference strategies (Baskerville, Rowe, & Wolff, 2018). When the business chooses to remove a vulnerability, that decision requires resources and detracts from the core mission. The corporate risk management program (RMP) needs to address both ‘when and how’ these threats are resolved (Dai Zovi, 2019). Those answers typically come from a feedback loop of identity, assessing, prioritizing, mitigating, and revising vulnerabilities (Gillies, 2011).

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.

# Section I: State of the Organization

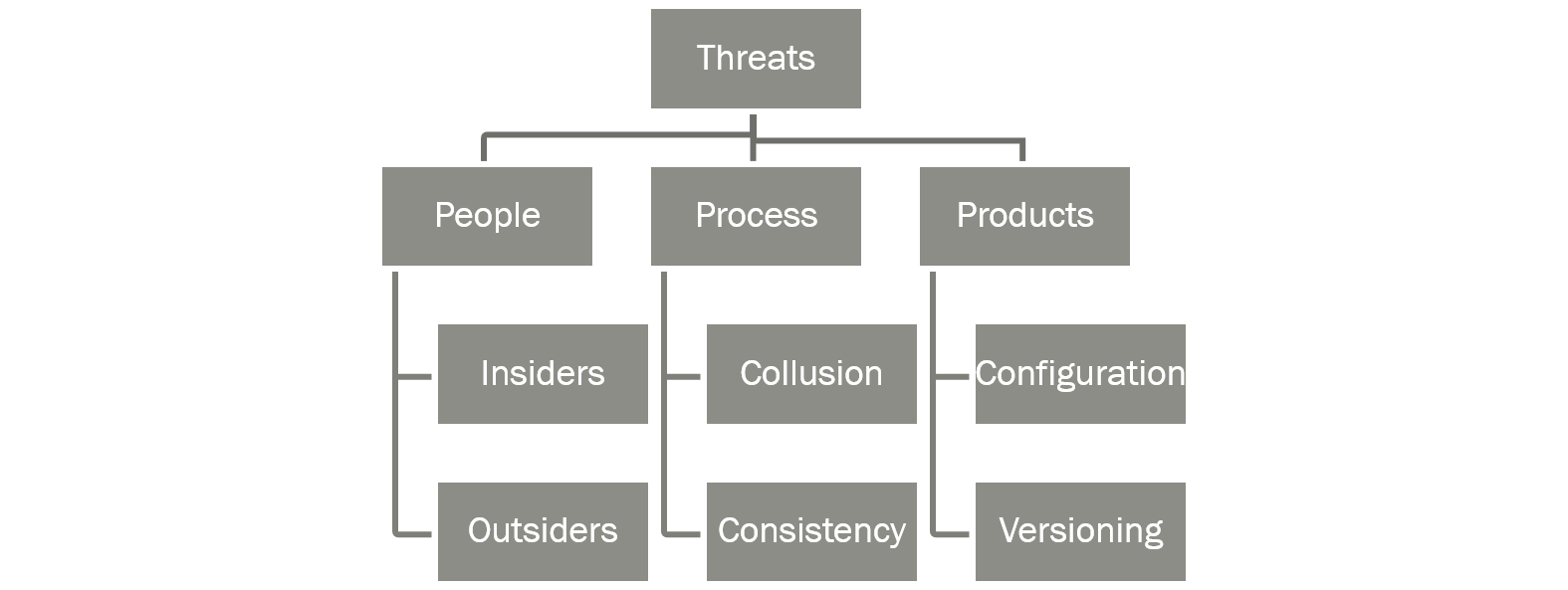
## Corporate Management of Systems

## Threats Every Organization Faces

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 (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.

Figure 1: Sources of Risks



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 like 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 to discover.

## Organizational Chart

Multiple security personas work in tandem to deliver a consistent and coherent risk management strategy that encompasses all people, processes, and products. If that strategy lacks sponsorship from the executive-level or does not resonate with the troops, then it is unlikely to succeed (Weston, Conklin, & Drobnis, 2018). Instead, having a cultural alignment ensures that the standard operating procedure makes safe decisions that minimize risk and privacy concerns.

The Chief Risk Management Officer (CRMO) and Chief Information Security Officer (CISO) set the stage by determining which risks are acceptable to business continuity. While smaller organizations combine these roles, the CRMO focuses on general risk versus the CISO is more concerned with the subdomain of information confidentiality, integrity, and availability (Grobler, 2018). Their broad policies and expectations form the corporate vision and guidelines that the Director of Information Security (DIS) must meet. For instance, the CISO might require customer data protections are Health Insurance Portability and Accountability (HIPAA) compliant. The DIS would break that down into a series of process changes and define a roadmap for achieving this goal. Incrementally delivering on the roadmap comes from teams of security engineers, that decompose problem statements into specific work items and validate policy decisions.

Last, but not least is everyone else, as it is security-critical that policies enable the business versus create artificial blockades (Weston, Conklin, & Drobnis, 2018). If the other team members lack insights into the intent of a policy, they will follow the specific ask, not similar permutations of the rule. For example, the timely installation of operating system patches reduces the risk of malware spreading through the organization. While no one asked for similar updates to Java, Flash, and Adobe reader are equally vulnerable. Only through associating the request to policy to the roadmap to the vision are these auxiliary risks addressed.

|  |  |
| --- | --- |
| Role | Description |
| Chief Risk Management Officer | Reduces the blast radius of process failures across the corporate strategy |
| Chief Information Security Officer | Accountable for the corporate strategy that protects business technology assets |
| Director of Information Security | Defines the policies that enact the corporate security strategy |
| Director of Privacy and Compliance | Ensures following of regulatory requirements around the handling of data |
| Security Engineer | Validates the implementation details of the security policy decisions |
| Everyone Else | Interacts with those policies and is critical for their successful execution |

## Network Diagrams

# Section II: Objectives of Risk Management Plan

## Risk Statement

When an organization begins with technological solutions, they are likely to devise incomplete protection strategies (Stevens, 2018). Instead, Hi-Tech needs to methodically begin with identifying and classifying what internal and external factors create the risk, then determine an appropriate response (Baskerville, Rowe, & Wolff, 2018). Due to resource constraints, it is not possible to address all issues under every scenario. The classification results can act as a mechanism for prioritizing the concerns and recognizing any non-starters upfront.

## People

The most crucial resource of an organization are the employees, and any plan for success needs to begin here. Valientes (2017) estimates that nearly half of security incidents result from employee negligence, like interacting with phishing attacks and fat-fingering system commands. Businesses that focus on security awareness training can reduce these statistics and create more reliable systems. This awareness needs to touch on foreign policy expectations, like European customer data, cannot leave Europe. However, even domestic policies differ, such as California and Delaware having stricter privacy laws than federal legislation. Initially, these expectations appear arbitrary, but communications the geographical nature of the Internet presents general consistencies and best practice patterns. It also leads to an understanding of how various levels of legal enforceability influence release schedules of new features and innovation into new markets. That training can guide all levels of the organization to reach out to subject matter experts because they are aware of the inherent complexity.

It can be helpful to think of customer identity as a user profile that contains collections of historical choices, stated preferences, user roles, and known associations (Wachter, 2018). When our services understand the context of the user’s profile, the experience can be customized and produce more desirable experiences. The payment for access to these inferences and decision processes comes from personal information, such as calendars, contacts, and routines (Mickens, 2018). This trade creates privacy concerns that can be subtle and can go unnoticed for some time. For instance, numerous platforms integrate into open identity provides like Google and Facebook as a mechanism to simplify enrollment. However, is that the job the user intended to hire (Dai Zovi, 2019)? Through an exchange of convenience, the user becomes trackable across multiple sites and web services (Paller, Mahalik, Skoudis, & Ullrich, 2020). While the physical person wants a single sign-on experience, they also desire distinct virtual profiles across those providers (e.g., LinkedIn versus PornHub). Traditionally users have encountered these entanglements of context on their mobile devices, but these are not the only scenarios. Asking personal assistants, such as Siri, Alexa, and Google Home, if they spy on us, results in recommendations to review the privacy policy (Haselton, 2018). That response can be misleading since these policies exist as a liability disclaimer, not for the direct benefit of the user (Wachter, 2018).

## Processes

Protecting against foreign and domestic risks requires augmenting business processes and asset lifecycle management. Hennig (2018) recommends starting with a threat modeling to identify what resources need protection and under which contexts. During this exercise, each step needs to consider any integrity, confidentiality, and availability risks that might exist. For instance, a prerequisite of deploying web services into authoritarian nations datacenters might involve exchanging sensitive communications with a foreign company. Interception of those conversations by nation-states will occur—either across the wire or from an official subpoena. These challenges require design decisions that focus on disposable resources (e.g., one-time access tokens) and end-to-end encryption. Many real-world processes span cross-corporation and require communication across asset production, installation, operationalization, and retirement (Busdicker & Upendra, 2017). Identifying and repairing vulnerabilities across this lifecycle needs to be an iterative process that seeks feedback and incorporates it.

Manufacturing facilities are evolving into massive CPS ecosystems through Industrial IoT devices feeding into complex event processing systems (Babiceanu, 2016). This approach reduces costs by increasing automation efficiencies. Reliance on automation also increases the opacity of decision-making processes and introduces additional risk vectors (Mickens, 2018). For example, an increase in network latencies might cause decision processes to act on outdated information. When perspective distortion exists between the cyber and physical structures, then accidents can follow, like autonomous vehicles failing to stop or safety systems not initiating soon enough (Frodigh, 2018). CPS technologies can enter into this erroneous state due to Denial of Service states (DoS) caused by malicious actors, malware, and negligent administrators. Process designers need to minimize these risks by evaluating the impact of time sensitivity on their implementation.

## Products

The products released into a market need to consider the security assertions of both the foreign market and the domestic organization. For instance, authoritarian nations will steal innovations and share those trade secrets with foreign competitors. The inverse can also be true, where products lack the security assertions of the foreign market and are not permissible. Recently Kaspersky Anti-Virus was banned from several American institutions because of concerns that Russia could maliciously control the software (Krebs, 2019). This trait is not unique to authoritarian nations, as specific New Zealand products have been ban from France for not meeting privacy norms (Hunt, 2019). When a product does not meet the expectations of either the producer or the consumer, then a decision around acceptable risk needs to take place. Those decisions might result in bundling fewer features into a smaller version or blocking the deal entirely.

There is an economic incentive for businesses to churn out new products and devices with more innovative, instead of investing in security protections for those features (Li & Liao, 2018). For many retail markets, the customer makes purchasing decisions predominantly on which product has the most features at the lowest price. Meanwhile, devices such as 8-bit micro-controllers, lack the computing resources necessary to support authentication, authorization, auditing, and transport encryption (Weber & Studer, 2016). Even when there are sufficient resources available, security protections can cause interoperation (interop) challenges, which leads to customers assuming that the product does not work. If the customer believes that the offering is faulty, they leave bad reviews online, contact support, and request replacements—all of which cost the business money.

# Section III: Business Impact Analysis

When choosing a risk management strategy, the organization needs to consider the threat impact and likelihood (Baskerville, Rowe, & Wolff, 2018). If the impact is critical, then the business will need to either transfer that risk or avoid the scenario entirely. For instance, foreign markets lack intellectual privacy protections, and this might discourage releasing cutting-edge technology to those audiences (Krebs, 2019). In other scenarios, avoiding a hostile market or business activity is not possible, making hedging with insurance a more appropriate response. For example, it might be prohibitively expensive to have redundant manufacturing plants, while unlikely, if the building burnt down, then the organization would go out of business. 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. For most other scenarios, the business needs to rely on controls that detect and react to failures promptly (Kosub, 2015). These might include technologies such as anti-virus and Intrusion Detection/Prevention Systems (IDS/IPS).

Another strategy is to form tighter integrations between the system components as a mechanism to reduce the attack surface (Baskerville, Rowe, & Wolff, 2018). For instance, if the network topology requires a user to maintain five accounts with different password complexities, the security of those passwords will decrease to offset the lost convenience (Busby, Green, & Hutchison, 2017). Instead, exposing Single Sign-On (SSO) capabilities improve the user experience and encourages more desirable credential management. Another technical gain comes from the removal of redundant components, each with the potential to contain incorrect application code or configuration settings. Removing redundancies also aids in more consistency through centralized policy management and enforcement.

# 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.

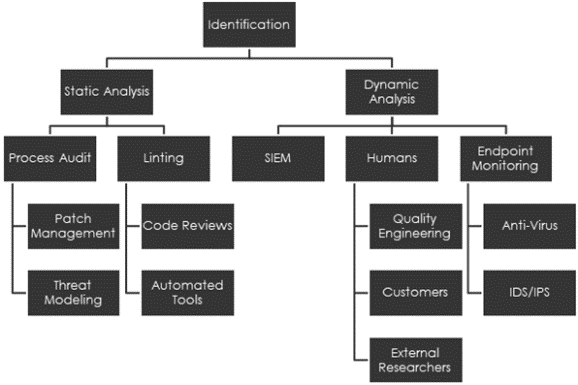
# Section VIII: Vulnerability Assessments

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