Section 3: Week 8: Additional Content and Quotes

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

June 7, 2020

North Central University

# Additional Content and Quotes

# 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, NCU-F 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.

## Privacy

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 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.

## 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 VIII: Incident Response Process

After a security incident transpires, the administrative team must devise a response plan to contain the incursion 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). For instance, 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, updating 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

## 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).