Section 2: Week 6: Mitigation, Continuity, Controls, and Disaster Planning

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

May 10th, 2020

North Central University

# Mitigation, Continuity, Controls, and Disaster Planning

Hi-Tech Manufacturing (HTM) operates electronic car assemblies plants across North America, Europe, and Asia. Their organization faces many cybersecurity risks to its data and services confidentiality, integrity, and availability (CIA). These potential vulnerabilities require security controls that constrain the blast radius of negligent and malicious actions through authentication, authorization, and auditing mechanisms (AAA). A finite resource budget exists to provide these mechanisms creating the need for effective investment prioritization. Choosing the right controls within the budget requires consideration beyond technology also to consider the influence of people and processes.

# Section I: Mitigation through Controls

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 attachments, it bypasses these 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, such as 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 a strategy that encompasses people, processes, and products.

## Control: 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 biggest 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 to non-technical audiences (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.

## Control: Auditing of Failure

Malicious employees represent risks to the business that can be difficult to detect. Often accessing sensitive documents and facility locations is part of that person’s role. Managing these expected behaviors creates the need for control mechanisms that specialize in anomaly detection and auditing. When these systems catch intentionally malicious behavior, it rarely escalates to the legal system (Elifoglu, Abel, & Tasseven, 2018). However, increasing the probability of catching the mischievous action can be an appropriate disincentive for specific scenarios. For other scenarios, security logs and video footage provide the necessary tools for external auditors to determine what happened after the fact. Proactive solutions are generally preferred, though having a reactive system is better than nothing.

## Control: Patch Management

Gartner estimates that 99% of successful vulnerability exploits target a known defect older than one year (Galinec & Steingartner, 2017). HTM can address these challenges through patch management strategies that follow a timely cadence. There can be political challenges to enforcing these policies because they come at odds with potential service disruptions. Mission-critical systems might only have a few scheduled maintenance windows each year. Resistance also comes from traveling employees that are unwilling to risk an outage on the road. The business needs to prescribe the expectations for typical usages and treat exceptions and unique items.

## Control: Recoverability

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.

# Section II: Mitigation, Continuity, and Disasters

Hi-Tech 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, building the best electronic vehicle. Allocating time and money into other projects might even appear to detract from this mission, and feel like a waste.

However, investments in other aspects of the organization reduce risk and improve continuity. It can be challenging to choose efficiently prioritize risk reduction because it compares an immediate real cost against a hypothetical future expense (Gordon, Loeb, Lucyshyn, & Zhou, 2015). For instance, licensing anti-virus software might cost the business one million dollars a year. If during that year, the company was lucky and did not encounter any malware, then the insurance was not used. In contrast, ransomware spreading across the intranet could easily exceed several million dollars (Astani & Ready, 2016).

Along with continuity solutions, the business also requires disaster recovery and response solutions to handle both known and unknown assaults. The threat landscape continues to evolve with adversaries, continually gaining leverage through decreasing costs to issue the attack, versus the cost to the defender protecting their resources (Lam, 2016). This asymmetry naturally occurs because the attacker only needs to send packets versus the defender must parse and act on those requests. Malware authors are also publishing over one million strains every day (Kilgallon, De La Rosa, & Cavazos, 2017). Given the sheer volume, there is a high probability that anti-virus fails to prevent an infection. While these malicious actors can wreak havoc on the corporate network, few forces are as damaging as employee negligence (Valiente, 2017). If a support technician issues an erroneous database command, it can cascade into a critical outage. Even after protecting against these sources, a hurricane or fire can cause irreparable damage.

## Establish Important Protections

The National Institute of Standards and Technology (NIST) Cybersecurity Framework suggests that effectively establishing protections uses a feedback loop of identification, protect, detect, respond, and recover (Grohmann, 2018). Previous efforts have worked to identify the most high-risk assets to including employee safety systems, intellectual property, and supply-chain management.

Employee safety blends across the cyber-physical boundary from risks on both sides. For instance, unauthorized persons cannot walk into the manufacturing area as this could result in injury or death. Instead, physical security officers need to confirm the identity of everyone on the premises. When these employees come into their work stations, they require the equipment to operate predictably, or they will lose productivity. This equipment includes laptops, various Internet of Things (IoT) devices, and potentially heavy machinery.

Intellectual property exists in the source code repositories and internal design documents. If the confidentiality of these assets becomes lost, then the competitive advantage of the Hi-Tech would be diminished. Safeguards need to exist to confirm the identity of the requestor and audit the request. Using encryption technologies like Digital Rights Media (DRM) can be effective for protecting design documents, but are harder to associate with source files. For those scenarios, the business might require that the volume containing uses Microsoft Bitlocker or a similar product.

Enterprise Resource Management (ERM) systems are responsible for the end-to-end supply chain order flow. If the system is inaccurate or unresponsive, then the business cannot make timely decisions nor process invoices. It is mission-critical that the system is available through fail-over replicas that understand the current state of the business. A series of checks and balances also exist to confirm that only appropriate roles can approve the final sign-off of work.

## Balancing Business Impact