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

Translating the protection requirements into security implementations has a wide range of maturity levels that could follow a good, better, best approach. Ideally, Hi-Tech would only follow the most strict guidelines. However, that is not as practical due to unacceptable costs both financially and in terms of user experience. For example, the business uses many IoT devices that lack remote firmware upgrade capabilities. It might be acceptable to have the operations team manually upgrade each device annually—the labor costs are too high for monthly cadences. Though it is important to remember that security investments are not binary, and can support shades of gray (Gordon, Loeb, Lucyshyn, & Zhou, 2015). This approach could divide the upgrade task into subgroups based on the criticality, like safety systems versus temperature sensors. Each subgroup can feed into the prioritization discussion, perhaps resulting in safety systems landing on a quarterly upgrade cycle, and the less critical sensors remain on an annual cycle. This decomposition of large bodies of work keeps the costs down and enables more focused efforts.

Vulnerabilities exist at the intersect of three conditions. “(1) system susceptibility, such as a design or implementation flaw; (2) threat accessibility, such as system access points or services; (3) threat capability, such as an opponent with the knowledge and resources to discover, access, and exploit a flaw.” (Baskerville, Rowe, & Wolff, 2018, p. 35) Often, it can be more economical to address one of the other criteria than the underlying problem. For instance, the IoT temperature sensors have a well-known remote command execution defect in the File Transfer Protocol (FTP) daemon. If Hi-Tech does not rely on this functionality, then merely blocking access at the network switch level removes the issue. Another vulnerability exists in the Telnet daemon communicating in plain-text. Similarly, the administrators can place those interactions on a Virtual Local Area Network (VLAN) to limit access.

There can be political pushback that some protections come with a cure worse than the disease. Hi-Tech would desire that leadership signs off on every work order, which is not feasible given the competing demands for time. Some staff members are aware of the override code to bypass this requirement and get the invoices out the door. While the rule intends to ensure that invoices are complete and promote accountability, but it also causes a bottleneck that impedes timely delivery. On the one hand, the security team could remove the bypass feature, but this introduces additional for the team. Approaching the prioritization of these scenarios requires a gentle touch, as security enables the business, not the other way around (Dai Zovi, 2019). Instead, a conversation could begin with senior leadership to understand if the previous decision makes still make sense. If the idea is valid, perhaps minor tweaks can maintain the central concept under more amenable terms.

Another challenge comes from balancing security over the rapid development of new features (Lam, 2016). Hi-Tech follows a three-month Water Flow Release Cycle that plans, implements, stabilizes for three, six, and three weeks respectively. Once the planning is complete, it can be challenging to introduce additional work as it requires an expensive reset. If the security team is divorce from this cadence, there is a high risk to existing business commitments. While the senior leadership team might be willing to accept those scheduling challenges, it puts unnecessary stress on the teams. For instance, postponing the release might delay a big customer onboarding into the platform. Ultimately these decisions are trading one set of risks for another.

## Disaster Recovery Priorities

The operations and security teams at Hi-Tech 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.

For example, an employe’s workstation becomes infected with ransomware. If the helpdesk can respond by reinstalling the operating system and downloading a recent backup of personal information, then the cost is minimized. Alternatively, if the automation does not exist or backup processes are not consistent, then the losses are magnified. Given the frequency of these types of situations, it makes economic sense to devise a generic repeatable solution upfront. Meanwhile, other disaster recovery scenarios are prohibitively expensive to even approach from a technical or process perspective. Imagine that 80% of manufacturing takes place at the headquarter location, and a meteor crashes into the building (e.g., black swan event). These risks require a transference to third-party insurance providers.

# References

Astani, M., & Ready, K. (2016). Trends and preventive strategies for mitigating cybersecurity breaches in organizations. *Issues in Information Systems, 17*(2), 208-214. Retrieved May 9th, 2020, from https://iacis.org/iis/2016/2\_iis\_2016\_208-214.pdf

Baskerville, R., Rowe, F., & Wolff, F. (2018, February). Integration of information systems and cybersecurity countermeasures: an exposure to risk perspective. *Special Interest Group on Management Information Systems (SIGMIS) Databases, 49*(1), 33-52. doi:https://doi.org/10.1145/3184444.3184448

Dai Zovi, D. (2019). Every Security Team is a Software Team Now. *Black Hat USA.* Las Vegas, NV, USA: Black Hat. Retrieved May 9th, 2020, from https://www.youtube.com/watch?v=8armE3Wz0jk

Elifoglu, H., Abel, I., & Tasseven, O. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business, 38*(2), 61-73. Retrieved May 9th, 2020, from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=bth&AN=129631258&site=eds-live

Galinec, D., & Steingartner, W. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience. *14th International Scientific Conference on Informatics.* Poprad, Slovakia: Institute of Electrical and Electronics Engineers. doi:https://doi.org/10.1109/INFORMATICS.2017.8327227

Gordon, L., Loeb, M., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment. *Journal of Accounting and Public Policy, 34*(5), 509-519. doi:https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Grohmann, A. (2018). Evolution of the cybersecurity framework. *Information Systems Security Association, 16*(7), 14-18. Retrieved May 2nd, 2020, from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=tsh&AN=130572679&site=eds-live

Hunt, T. (2019). Hack to the Future. *NDC Conferences.* Minnesota: NDC. Retrieved May 9th, 2020, from https://www.youtube.com/watch?v=qCOefMiakps

Kilgallon, S., De La Rosa, L., & Cavazos, J. (2017, September 18-22). Improving the effectiveness and efficiency of dynamic malware analysis with machine learning. *Resilience Week.* Wilmington, DE, USA. doi:https://doi.org/10.1109/RWEEK.2017.8088644

Lam, W. (2016). Attack-prevention and damage-control investments in cybersecurity. *Information Economics and Policy, 37*, 42-51. doi:https://doi.org/10.1016/j.infoecopol.2016.10.003

Paller, A., Mahalik, H., Skoudis, E., & Ullrich, J. (2020). The five most dangerous new attack techniques and how to counter them. *RSA Conference.* RSA. Retrieved May 9th, 2020, from https://youtu.be/xz7IFVJf3Lk

Proctor, R., & Chen, J. (2015, August). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Human Factors and Ergonomics Society, 57*(5), 721-727. doi:https://doi.org/10.1177/0018720815585906

Valiente, C. (2017, October). Addressing malware with cybersecurity awareness. *Information Systems Security Association, 15*(10), 16-22. Retrieved May 9th, 2020, from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=tsh&AN=125478200&site=eds-live