Section 3: Week 8: Integrating Strategic Cybersecurity

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

May 23rd, 2020

North Central University

# Setting the stage

## What is Cybersecurity

CyberSecurity refers to a collection of mechanisms and processes that constrain risk to business processes by ensuring they are meet performance and consistency expectations, even under erroneous conditions (Mickens, 2018). These erroneous conditions arise due to both malicious or negligent scenarios. For instance, when two services are communicating across a private network, numerous risks to their continuity exist, such as the switch could become faulty and lossy. Security protections, like Transport Layer Security (TLS), can detect the hardware failure through checksums that are visible at the application layer. A second product defect might cause a surge of traffic, and without traffic-shaping technologies results in overloading the downstream services. A third defect might incorrectly combine data with commands, such as a single quote that triggers a SQL injection and crashing the application. From the perspective of the end-user, it does not matter if our services fail because of hardware, configuration, weak quota management, or incorrect application code. They care that the system works. These scenarios hurt the reputation of the service operators and weaken the competitive position of the business.

## How does security enable the business

## Framing a Security Message

Communicating the criticality of security to a broad organizational audience is challenging because too many experts have poorly framed the conversation in the past. Traditional approaches describe the Internet as being full of Boogiemen, that live in basements dressed in hoodies (Bruijn & Janssen, 2017). These sophisticated adversaries will stop at nothing to exploit our websites and exfiltrate the data. From the employee perspective, this sounds far fetched and reminiscent of a Michael Bay film. They do not understand why they should care. Admittedly, our data is not attractive, so why would anyone bother to attack us? Instead, the message should center around the risks that our software and business processes accept, implicitly, and explicitly. Many risks exist within technology, though a more alarming number originate from the employees (Valiente, 2017). The employees have access to customer data, production services, and other sensitive assets. When they fat-finger a database command, there is a chance of data corruption, and that will require a backup and restore operation. Fundamentally, conveying these risks results in the awareness and the formation of strategies around both prevention and recovery. Perhaps more importantly, it addresses the question, "why should I care?"

## Applying a framework to security

There is an abundance of standards and frameworks available to determine if decisions are being made consistently across the industry. Four common incarnations are the Risk Management Framework (RMF), ISO2700x, NIST Cybersecurity Framework, and COBIT v5. Each of these approaches follows a similar cycle of plan-act-assess-revise across different aspects of the stack (e.g., authentication, authorization, and auditing). However, there are differences between the degree of enforcement versus guidance. The origin of the standard also has a significant influence on the framework designers' perspective, such as COBIT deriving from IT auditing then expanding with industry commonalities.

While each of these frameworks possesses a similar structure, they differ in terms of prescriptive guidance versus generalizations. For instance, ISO2700x has stringent requirements that necessitate a cultural shift for many businesses, and this is difficult to scale to an enterprise environment (Gillies, 2011). In contrast, the NIST Cybersecurity Framework describes various common scenarios then offers a good, better, best approach for the implementors (Grohmann, 2018). While there is a time and place for everything, introducing schedule risk to inflight commitments through abrupt policy change will always encounter political push back (Dai Zovi, 2019). For many businesses like HTM, having the flexibility to adopt a framework and then iteratively mature their processes over time reduces that risk and is an easier sell to leadership. Arguably, this is not the utopian course during the interim. However, movement in the right direction is better than no action.

# What are we protecting

## 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 database commands. Businesses that focus on security awareness training can reduce these statistics and create more reliable systems. This awareness needs to touch on cultural expectations, such as European customer data, cannot leave Europe. 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 foreign markets. This training applies to all levels of the business, such as how technicians assist international customers, and how executives bundle products for international distribution.

It can be helpful to think of identity within IoT as a profile of historical choices, stated preferences, user roles, and known associations (Wachter, 2018). When the device understands the context of the user's profile, the experience can be customized and produce more accurate predictions. 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 (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 global 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. Those conversations are likely to be intercepted and also viewed nation-states, either across the wire 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. Leadership teams need to prioritize building these intra-team trust relationships through combinations of social outreach and bug bounty programs.

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.

## 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.

According to Gartner, the trend of weak authentication controls impacts nearly 50% of all IoT vendors (Galinec & Steingartner, 2017). The Mirai malware was able to span half a million devices using a small dictionary file to brute force access (Gamblin, 2017). Although its source code has been available for several years, and its particularly noisy approach to gaining entry are discoverable, variations are still thriving (Kolias, Kambourakis, Stavrou, & Voas, 2017). While these programs should have encouraged a movement toward security by default, the broad industry has failed to act against even this rudimentary attack.

There is an economic incentive for businesses to churn out new IoT 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 device does not work. If the customer believes that the equipment is faulty, they leave bad reviews online, contact support, and request replacements—all of which cost the business money.

## Information

## Customers

# Whom are we protecting against

## Negligence

When we step back and look at the numbers, half of the attacks target technology assets explicitly, such as probing for cross-site scripting bugs in our websites. The next quarter comes from humans interacting with hostile automation, e.g., phishing attacks and malicious mobile apps, and the final quarter from erroneous behaviors. These figures suggest that creating a more security-aware culture could remove nearly half of the attack surface and strengthen business continuity (Valiente, 2017). For instance, when network engineers understand risk management, they create features that consider scalability and availability during the design versus after the solution has failed (Mickens, 2015). It is too late to discuss service redundancies and fail-over technologies after the service is offline, or least privileges after a support technician accidentally corrupts customer data. These challenges will continue to occur until there is sufficient awareness, and team members understand the damage that follows their actions. If we can at least stop the good guys doing bad stuff, the organization would be in a much better position.

## International actors

## Hackers/Hacktivist

# How are they attacking us

## Ransomware and Malware

Malicious software, or malware, are applications that compromise the confidentiality, integrity, or availability of a system. These programs infect systems via email, file-sharing services, browser vulnerabilities, spoofed resources, and misconfigured services (Lee et al., 2017). It can be challenging to contain the spread through an organization due to homogeneous configurations of the devices. For instance, a branch office will likely run the same software packages on each workstation and share documents through central repositories. The objective of the malware can vary from scenarios such as remote command-and-control, data exfiltration, and denial of service scenarios. One specific attack that is gaining popularity is ransomware, which are applications that encrypt user data and then offer to sell the decryption key (Busdicker & Upendra, 2017). Since malware comes from different vectors with varying objectives, detecting and preventing all scenarios is nearly impossible. Even with protection against all known scenarios, criminal social networks have easy access to exploitation packages and zero-day vulnerabilities across the dark web (Ericsson et al., 2018). Given the availability of exploitation software, organizations need to consider these scenarios as part of their risk management planning. Addressing these unknown unknowns requires defense-in-depth mindsets that expand beyond edge firewalls to include more robust Intrusion Detection and Prevention Systems (IDS/IPS).

## Zero Days

## Phishing

Users interact with spoofed resources through cold-calling or name squatting scenarios, such as emails directing them to netflix.com.evil.com. Previous security messages tell the user to look for details, like misspellings, as evidence of being fake (Proctor & J, 2015). However, this implicitly implies that perfect grammar infers being real. When users connect to websites, training has also told them to look for the security icon, but this only means the traffic is encrypted (Hunt, 2019). Without a consistent and reliable method to determine that a resource is genuine, the only alternative is skepticism. For instance, when a banker calls for account information, hang up and call them back through the main switchboard. If the call were real, there would be a note on the file, and another representative will assist. Along those same lines, if netflix.com.evil.com, needs an update to your information, start at Bing and search for Netflix login, scrolling past the advertisements to the real site. While none of these methods are fool-proof, they increase the odds of ending at the right location.

# Where are they attacking from

## 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.

## IoT

The Internet of Things (IoT) represents the next evolutionary step in communication and system connectivity. Naïve outsiders see this industry as a series of gimmicks, Apple watches, and smart toasters. Those statements are true, but more importantly, it also creates the missing bridge between cyber and physical systems (CPS). This capability comes from sensor and input networks that emit telemetry into ubiquitous cloud computing and machine learning platforms. Using physical motors and actuators, artificial intelligence and big data solutions can then reach back into manufacturing and safety systems. As information and decision processes transact across this bridge, it enables organizations to execute expert workflows autonomously and prevent costly failures. However, many challenges exist around ensuring the confidentiality, integrity, and availability (CIA) of all participants of this system.

# Globalization Considerations

## Geography and Sovereignty

The premise of the Internet is an open communication system that connects people from around the world, enabling commerce and ideas to flow freely. However, nation-states also want to protect their sovereignty and enforce laws around these interactions (Inkster, 2015). These competing requirements cause national security policies to make trade-offs between government control, societal freedoms, and rights of international actors (Kovacs, 2018). Since the values of democratic and authoritarian nations vary substantially, it is unrealistic to assume a unified set of policies can exist that appeal to all countries. Instead, nearly all nations legislate laws that target the Internet infrastructure that resides within their state (Matsubara, 2014). These decisions create geography that influences the protective capabilities and behavioral norms. For instance, the European Union (EU) believes that building a digital economy begins with user privacy (Kovacs, Cyber Security Policy and Strategy in the European Union and NATO, 2017). While the EU's Global Data Protection Regulations (GDPR) mandates severe penalties for negligence, like data breaches, authoritarian countries such as Russia are more laisse-fair. These value differences appear in other aspects like the transparency to share evidence or assist with criminal investigations.

## Cyberespionage

Businesses that operate solely within the United States have access to a legal system that enables seeking damages for malicious third-party behavior. For instance, when Uber stole intellectual property from Google, it was sued for $250M in damages (Bensinger, 2019). When the same theft occurs across international borders, jurisdiction becomes less clear and is more challenging to enforce. Participants in these hostile markets need to be aware that espionage comes from various sources, such as individual hackers and nation-states (Krebs, 2019). International law does not prohibit these nation-states spying, Article 51 of the United Nations charter even allows it under the disguise of self-defense (Banks, 2017). Some states argue that different rules should exist for monitoring public and private institutions. However, this perspective employs a very Western view. For socialist countries, the distinction is fuzzier than a purely capitalist society as the boundary between the industries lacks a consistent definition.

## Cyber sabotage

Using technologies like ransomware, malicious software that encrypts digital devices, nefarious actors can force an organization to purchase decryption keys before restoring service (Busdicker & Upendra, 2017). Attackers also send high volumes of network traffic into corporate websites as a mechanism causing Denial of Service (DoS) scenarios. When these cyber sabotage events occur, it disrupts business continuity and impacts the credibility of the victim. American companies have traditionally relied on deterrence, such as the Computer Fraud and Abuse Act (Fischerkeller & Harknett, 217). Technological solutions like deploying applications across multiple Public Cloud Service Provider (CSP) data centers can minimize the influence of DoS attacks. However, these same legal protections do not uniformly exist across the globe, and regulations around data placement can limit the accessibility of flexible fail-over solutions.

## Subversion

The international community does not agree on the strict definition of what constitutes a cyber-attack (Fischerkeller & Harknett, 217). These differences influence auditing and compliance requirements between countries and prevent direct comparisons across policies or statistics (Matsubara, 2014). The political values of nations contribute to the disparity, such as Europe prioritizing end-user safety versus authoritarian governments preferring to save face. When requirements around transparency do not fully exist, then even legitimate partners are unlikely to tell the whole truth. Being the only business that is forthcoming creates a competitive disadvantage, as customers only see "A" claims to be more secure than "B." Without a carrot or stick, how can a domestic company ensure security incidents are timely and accurately communicated? Imagine the challenges with less reputable entities, if these are the risks with legitimate partners.

# Prioritizing Risk Management

Finite resources Translating the protection requirements into security implementations have 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—though the labor costs are too high for monthly cadences. In many scenarios, choosing a security investment is not binary (do everything versus do nothing). Instead, the purchase can be in the middle and follow a phased release (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 an 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, 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 work for the team. Approaching the prioritization of these scenarios requires a gentle touch, as security enables the business, not the other way around (Zovi, 2019). Instead, a conversation could begin with senior leadership to understand if the previous decision still makes 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 divorced 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.