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

* Collection of mechanisms and processes that constrain risk to business systems
* Prevent erroneous conditions from negligent and malicious sources
* Ensure confidentiality, integrity, and availability of our products and services

## How does security enable the business

* The core objective of the business is to deliver its mission as effectively as possible
  + 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, that efficiency comes from consistency and iterative releases, versus wild swings of productivity due to high risk and high reward scenarios.
* When we apply risk management, it reduces the blast radius of any single decision. It limits the draw-downs from factors that might not be entirely within our control.
* Hardware dies, traffic is finite, data becomes corrupt, and these incidents necessitate a methodological approach that minimizes the time to detect and recover (MTTD/MTTR).

## 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.
* Instead, the message should center around the risks that our software and business processes accept-- both implicitly and explicitly. Many risks exist within technology, though a more alarming number originate from the employees

## Applying a framework to security

* There is an abundance of standards and frameworks available to determine if decisions consistently made.
* Frameworks like ISO, NIST, COBIT, and RMF make trade-offs in terms of guidance versus mandatory expectations.
* Despite internal differences, each of these frameworks follows a similar cycle of “plan, act, assess, revise.” This approach helps ensure that the business is looking for the highest priority risks and addressing them appropriately. Previous decisions also require periodic re-evaluation to confirm they are still meeting the needs without adding undue pain across participants.

# 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 system commands.
* This group also represents the “good guys” that are even trying to “do the right thing.” If we come up with awareness strategies for this audience, it has the most considerable potential impact, and they can become incentivized for change.
* 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.
* While there are benefits to rich profiles that contain deep context, it also introduces privacy concerns along the edges where the context becomes entangled. For instance, Google and Facebook provide simplified user enrollment but blend the person’s personal and professional information. This scenario creates challenges, such as trackability across platforms.
* Our employees have access to critical systems as a requirement of their role. If their behaviors are left unchecked, then it results in erroneous actions, even embezzlement, and theft.

## Processes

* Protecting against foreign and domestic risks requires augmenting business processes and asset lifecycle management. These insights might come from formal processes like threat modeling.
* The legal protections across that lifecycle can be highly dynamic, especially as different aspects of the value-chain sprawl different jurisdictions. For instance, California and Delaware have stronger privacy expectations than American federal requirements—and the European Union is arguably even stricter. Meanwhile, intellectual privacy is more of a footnote to some authoritarian nations like China and Russia.
* We need to assess the influence of confidentiality and integrity checks failing, and how to minimize those challenges by design and contract—not implementation.
* Time can add an entirely new dimension of complexity to our processes, especially as they become distributed across multiple physical locales. 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.

## Products

* There can be multiple locale-specific risks that need to influence our release strategies. When intellectual privacy (IP) like source code ships to customers, they can reverse engineer those secrets. Dealing with foreign nations might also require forced hand-off of IP and discourage releasing certain features into those markets.
* Product expectations is a two-way street, and those foreign markets might have legal and cultural norms that prevent certain features. For instance, having insufficient encryption or storing user information in unsupported physical boundaries can result in litigation.
* As the scope of our products and solutions grows, so too does the usage of third-party technologies. If those systems have issues, then they effectively become our issues.
* 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. We need to be mindful of where the incentives exist when building or purchasing products.

# Whom are we defending against

## Negligence

* When we step back and look at the numbers, half security incidents come from employee negligence. Their interaction with hostile automation, e.g., phishing attacks and malicious mobile apps, along with trying to find the path of least resistance for completing their job—bypasses safety protocols.
* Another critical challenge comes from the access that users require to perform their job. The company is always one lousy database command away from executing a disaster and recovery procedure.
* Users tend to be more vulnerable than technology. It makes economic sense for attackers to target them specifically. Statistically, this is where the risk comes from because they will make the most authenticated and privileged decisions across the system.
* These situations all culminate in security awareness training is essential for the survivability of the business.

## International actors

* Incentives exist for international actors to carry out cyber espionage, sabotage, and subversion against our businesses. Stealing our hard work or knocking it off the Internet is often cheaper and easier than competing.
* The jurisdiction also becomes very fuzzy, and that creates limitations of legal protections across these different boundaries.
* Another set of challenges centers around the lack of transparency across different regulatory boards. In some regions that do not have strict audibility requirements, there can even be punishments from the industry for being the only transparent player in the space.
* Essentially there are different political values at play, and that causes distinct trade-offs between government control, social freedoms, and international actors’ rights. If a foreign competitor can steal and cheat impunity-- why would they not?

## Scammers, Spammers, and Robots

* Where former hackers would carry out manual attacks, those with botnets could use automation to increase their leverage. However, in the modern world, the ubiquitous availability of cloud and high-speed networking removes these artificial constraints.
* Through that leverage, the attackers can focus on market segments instead of specific individuals and play a game of large numbers. No longer do they target us because we are *special*.
* Scammers and insiders can appear at any level of the organization, to acquire assets and property for personal gain. These vectors can be difficult to catch as they are becoming more sophisticated over time.

# How are they attacking us

## Ransomware and Malware

* Malicious software, or malware, are applications that compromise the confidentiality, integrity, or availability of a system.
* One specific attack that is gaining popularity is ransomware, which are applications that encrypt user data and then offer to sell the decryption key.
* 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.
* Since malware comes from different vectors with varying objectives, detecting and preventing all scenarios is nearly impossible.

## Patch Management and Zero Days

* Zero-day black markets allow governments, criminals, and researchers to transact in weaponized exploits.
* However, the more likely scenario is compromise form a known vulnerability that is at least one year old. Luckily, patch management is very solvable and addresses the 80% scenario.
* Addressing patch management requires two components; first notification to employees that updates are available and second training to apply them. Through security training, the staff can be made aware of why the updates are necessary and the reasons for the timely application.

## Phishing

* Users interact with spoofed resources through cold-calling or name squatting scenarios, such as emails directing them to netflix.com.evil.com.
* Attackers have become very sophisticated with these attacks because they are cheap, highly effective, and most users do not understand them.
* Traditional protections have centered around looking for unencrypted websites and spelling errors. However, this has also trained those users that the inverse makes it not a scam.

# Where are they attacking from

## Abstract Borders and XaaS

* The network boundary is no longer a crisp line and instead abstractly blends across multiple third-party systems.
* Legacy controls systems, such as edge firewalls and vulnerability scanners, are no longer sufficient because attackers focus on the richer landscape of application-level attacks. In many situations, these protocols allow anonymous communication directly with service endpoints.
* Another growing trend of the XaaS is that even internal systems often become distributed across public and private clouds.
* 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.

## Globalization

* 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
* These competing requirements cause national security policies to make trade-offs between government control, societal freedoms, and rights of international actors.
* 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.

## 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, defending that bridge is challenging due to the deficiencies of authentication, authorization, and auditing protections in the devices. According to Gartner, the trend of weak authentication controls impacts nearly 50% of all IoT vendors.
* Incidents like the Mirai malware that compromised 500 thousand devices using a small dictionary file. Despite these issues, the industry is broadly not taking the necessary actions to prevent these challenges in the first place.

# Prioritizing Risk Management

* Implementing security often comes with a good, better, best set of solutions. While it would be ideal always to choose the best option, that is not realistic. The business has a finite amount of resources. It needs to consider the impact in terms of schedule and existing commitments.
* Vulnerabilities within the system exist at the intersection of (1) the system is susceptible, (2) the threat is accessible, and (3) the actor is capable. In many scenarios, one of these facets is cheaper to mitigate, and that enables a good enough approach to make a risk acceptable.
* In other situations, the security issue might be too enormous to tackle. When this occurs, then a strategy must determine how do decompose the work into an iterative solution. Perhaps upgrading all workstations is prohibitively expensive, so they are divided by department, and accounting and finance devices receive the first round of improvements.
* While purists want to address all risks to the organization, the business will need to live with a set of them. However, it is important to remember that security exists to enhance the business, not the other way around.
* If the economic or impact on productivity too costly, then other solutions need to exist. For instance, perhaps the business purchases insurance or finds another risk transference mechanism.
* As security professionals, our responsibility is to communicate the risks and propose mechanisms to reduce the blast radius. It is the responsibility of the executive leadership to internalize those decisions and make the final cost-benefit conclusion, given that guidance.