Section 2: Week 2: The Human Aspect

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

April 12th, 2020

North Central University

# The Human Aspect

## Framing a Security Message

It can be challenging to communicate the criticality of security to a broad organizational audience 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. They are sophisticated adversaries that will stop at nothing to exploit your website and exfiltrate the data. From the employee perspective, this sounds far fetched premise to a Michael Bay film, and 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 implicitly and explicitly accept. Many risks exist within technology, though a more alarming number originate from the employees. 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. How we prevent and recover from these negligent incidents, is fundamental to communicating why one should care and how it impacts them.

## What is the Goal of Security

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. 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 or lossy. Security protections, like Transport Layer Security (TLS), can detect the hardware failure through checksums that are visible at the application layer. A product defect might cause a surge of traffic, and without traffic-shaping technologies result in overloading the downstream services. Another 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 organization.

## How has the perception evolved

The attack surface of an organization has drastically evolved over the last twenty years, from a focus on attackers and technology to centering around people and processes. Previous, the administrators could sleep comfortably, knowing that only a few people with physical access could interact with their networked topologies. Over time the needs of these topologies grew to support complex communication systems that interact with employees, contractors, and also anonymous guests. Some of these anonymous guests want to attack the corporate network, though this is another evolving area. 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. Now, anyone with a few dollars and an open-source vulnerability scanner can programmatically multiple network segments. Substantial effort goes into protecting these platforms, but little attention has considered on the other side of the equation—all of these people. Modern enterprise networks have hundreds of users that are authorized to perform tasks. When those users fail, it can be very challenging to detect, mitigate, or even control the blast radius. This realization creates the need for security engineers to design programs that center around awareness and skepticism.

## Why are people now the focus

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 can remove nearly half of the attack surface and strengthen business continuity. 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. It is too late to discuss service redundancies and fail-over technologies after the service is offline. Similarly, it is too late to discuss the least privileges after a support technician accidentally corrupts customer data.

## Where do we need to protect people

Before the Internet, the attack surface was limited to criminals breaking down the front door and stealing the safe. Now businesses are highly connected through always-on technologies that interact with the outside world. Critical infrastructure, like DNS and LDAP, also resides outside of the corporate firewall creating a more abstract notion of where the network ends.

Networks need to consider the impact of heterogeneous devices, that are not entirely under the control of the administrators. How many employees use VPN and communication services from their phones? How many work laptops also surf the public Internet? Each of these devices is only weakly protected but allowed direct access to sensitive resources. Though these are not the only mechanisms to interact with the employees, they also receive emails, snail mails, voice calls, and video chats. Each of these mediums invites attack vectors where scammers can attempt to slip unauthenticated messages. If an attacker can manipulate support staff with a 55 cent stamp and one-page letter, then why bother with a more complex assault?

## Understanding STRIDE Categorizations

Demystifying security begins with a framework of categorizing different attack vectors. STRIDE enumerates these vectors as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges. While countless examples result in these scenarios, having an awareness of their existence, causes humans to look for them.

|  |  |  |
| --- | --- | --- |
| Risk | Cause | Example |
| Spoofing | Failure to authenticate a resource as genuine | An email asks for bank credential |
| Tampering | Failure to prevent resource manipulation | Changing the amount on a check |
| Repudiation | Failure to audit an operation | Disputing the cashier gave me change |
| Information Disclosure | Failure to conceal private communication | Discussing trade secrets at a restaurant |
| Denial of Service | Failure to isolate multi-tenant traffic | Hundreds of callers overloading the front-desk |
| Elevation of Privileges | Failure to enforce security policies | Alice asks her Manager to update the timeclock |

## Using threat modeling here

It can be challenging to enumerate the threats against an abstract system of interactions, and this creates the need for a more methodical approach. This process could begin with first enumerating the different entities and resources within the system. For instance, the coffee shop has staff, managers, point of sale systems, and coffee machines. Next, consider the different endpoints that exist to communicate with these systems. Customers can talk with the staff, provide loyalty reward cards, escalate to management, and use different payment technologies. There are implicit and explicit trust boundaries between the customers, staff, and management that allows communication to flow in various contexts. As customers buy coffee, there is an unspoken protocol that begins at the register, waits in line, then gets the cup a few minutes later. The venue has various security systems such as locks on office doors, cameras, and personal watching the customers.

## Applying these ideas to getting free coffee

After listing the different resources and interactions, some of the threats against the coffee shop become more clear. Consider the purchasing protocol and ask what enforces the sequence of events? A customer could skip the cashier and insist their order was lost, or reuse their receipt to get a second cup. Many loyalty programs use punch cards to track the tenth cup is free, and run the risk of tampering. Perhaps the chain offers free coffee to employees, and a customer claims they are a new hire from a different branch. Some establishments allow customers to get free refills but do not authenticate they purchase the first cup. How about complaining to management about the service, and demanding a free cup?

Are these attacks specific to coffee shops? No, these low-tech attacks are reliable across many human-interactions due to a lack of skepticism. Why would the customer try to scam me? That is something that happens to other people, not me.

## Creating a Security Aware Culture

When an organization makes security a core pillar of their design methodology, it reduces risks and provides more reliable services. Integrating this mindset requires a culture shift where the employees are skeptical and ask questions about “how they will ensure meeting specific performance and reliability metrics.” For instance, how are parameters validated and authenticated? What mechanism is authorizing the specific action? How will we record the action that took place? These questions are not limited to technical systems, and also apply to interpersonal interactions. For example, when an email comes into the accounting department and requests updates to the payment information, what confirms the message is not spoofed? Does the secretary have the authorization to make the filing change, or does it require management approval? How will an external auditor trace this change, legitimate or not? Perhaps even 9 out of 10 times, the message is genuine, but consider the impact of a typographical error on their side. Now, payments are going to the wrong place, and the business needs to work with the bank to get their money back. “To err is human,” negligence is all around us, so we need to remain skeptical and confirm the accuracy of all information.

## Credential Management

The notion of a password made sense in the dark ages of MIT mainframes, where a dozen people shared a room-sized computer. However, as the availability of digit resources has grown, the concept has become outdated. Not wanting to let a bad idea die, password complexity policies arose requiring symbols and numbers, along with requirements to rotate passwords on a regular cadence. End-users replied by reusing these secure passwords across multiple sites, doing minor translations such as “o” to “0,” and writing them on post-it notes. The challenge comes from passwords are inherently difficult for humans to remember. Instead, a security-aware culture should consider using passphrases and short sentences, as these are difficult for computers and easy for humans to remember. Introducing Multi-Factor Authentication (MFA) protects against credential theft. When the system confirms not only something the user knows but something they have, are, do, and location. In essence, it increases security guarantees through additional dimensions of authenticity.

Single Sign-On (SSO) and Open Authentication (OAuth) both remove and create problems for the organization. On the one hand, having a consistent identity allows the user to remember fewer passwords and increase the centralization of credentials. However, these digital identities can accumulate baggage, as we mindlessly click through websites. For example, a review of my personal Google account shows that three websites are authorized to access location data. From the end-user perspective, these OAuth approval messages are more noise that is getting in the way of reading this cat article. Perhaps the should be a national review of our OAuth Day. However, until then, training and communication about the impact of these decisions need to take place.

## Device Management

Mobile apps can accumulate dangerous levels of access to our devices. Like the OAuth approval messages, users do not understand what these mean, why would a flashlight app be malicious? While many of these apps are binane, others are trojan horses that will exfiltrate our contacts and other personal information. This scenario is particularly concerning since many professionals also keep emails and sensitive documentation on the device. Some IT departments even allow Virtual Private Network (VPN) connections, creating a direct route from the Google Playstore to the back office. Yikes. Network security policies need to be skeptical of these devices and quarantine what they can access, but this only addresses half the puzzle. The rest comes back to training and awareness that *free* apps and *private* data do not mix. Patch management plays a vital aspect in preventing malicious automation from attacking our devices. There needs to be repeated guidance to apply patches promptly. Despite the relative simplicity of weaponizing a patch, users do not understand the risks and see it as an inconvenience. As in many related scenarios, when security competes with convenience, there is natural friction that requires additional attention.

## Phishing Sites

Users interact with spoofed resources through cold-calling or name squatting scenarios, such as forged emails or netflix.com.evil.com. Previous security messages tell the user to look for details, like misspellings, as evidence of being fake. 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. Without a consistent and reliable method to determine that a resource is genuine, the only alternative is skepticism. For instance, when “your bank” calls to get 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, and scroll 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.

## Doxing

Facebook and social media create significant risks to privacy and identity management. Consider the requirements to recover a password to financial institutions; date of birth, grandparents’ names, city of birth, which school did you attend. These facts are highly discoverable through social graphs. Even if we do not directly share these details, our friends report metadata about themselves, and that tends to be highly correlated. Public records also report big-ticket transactions, such as property deeds and marriage certifications, that detail other aspects of our lives. While it can be tempting to think that my information is not essential, why would anyone target me? This perception is inaccurate because automation allows third-parties to aggregate the information across a broad population. From this vantage point, they can identify clusters of high-probability targets and go after all of them. These attacks lead to personalized advertisements that have a higher click-through rate.

## Untrusted Networking

A modern enterprise network has abstract borders, with users connecting from untrusted sites like coffee shops. As the gateway to the Internet, these open hotspots are free to monitor and manipulate any unencrypted traffic that flows through them. For instance, the provider could inject malicious JavaScript into the returned webpage, or steal credentials as they are uploaded. Malicious hotspots can attack other protocols, such as Simple Mail Transport Protocol (SMTP) and Domain Name Services (DNS), to spy on private emails and influence routing to external sites. These changes can be subtle and difficult to notice. Alternatively, training needs to communicate the necessity for VPN technologies as a mechanism for creating an encrypted tunnel into a trusted service. Untrusted networks are not limited to those that run on switches and routers, but also include public areas. For example, if two employees are openly discussing trade secrets at the coffee shop, the next table over can hear them. Other scenarios might center around lost mobile devices in the real world. If they are not encrypted, then any information on the device is lost into the public. Through an awareness program, users need to understand these are information disclosures vulnerabilities. It does not matter that the data leaks from the mouth and not the ethernet; there is an equal potential for damage.

# Conclusion

Traditional framing of a security message has focused on the notion that a lone hacker is out to get us. This approach leads employees across the organization to question the accuracy of that message and the guidance associated with it. A modern vantage point argues that security is a collection of processes that reduce and contain risk. These risks exist from both malicious and negligent sources, and both introduce challenges towards business continuity. Hardware fails, technicians will corrupt customer data, engineers will write defects, and administrators will misconfigure services. If the system approaches these scenarios methodologically, then incident responses can fail-over traffic or perform necessary backup and recovery operations. Security is only partially about stopping malicious actors; the rest is about stopping erroneous actions from legitimate sources. In many scenarios, manipulating humans proves to be easier than attacking the machines. Mitigating these risks requires a security-aware culture that understands the different attack vectors and is cognisant of those interactions. While identifying risk in an abstract system is challenging, a methodical approach that enumerates communication flow across an environment can help to identify those threats. Consider the coffee shop and the number of assumptions that exist in the payment and transaction protocols. These threats are not unique to a café, and with minor tweaks apply to any other establishment. Additional specific challenges exist, such as phishing, doxing, credential management, and utilizing untrusted networking that requires awareness. Despite these ideas seeming foreign and complicated, having an understanding of the risks will reduce the attack surface and keep the employees safe.