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

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 full of Boogiemen who live in basements dressed in hoodies (Bruijn & Janssen, 2017). These sophisticated adversaries will stop at nothing to exploit our websites and exfiltrate the data. This situation sounds far-fetched to users and reminiscent of a Michael Bay film from the employee perspective. 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, requiring a backup and restore operation. Fundamentally, conveying these risks results in the awareness and forming strategies around both prevention and recovery. Perhaps more importantly, it addresses “why should I care?”

## What is the Goal of Security

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

## How has the perception evolved

An organization’s attack surface has drastically evolved over the last twenty years, from a focus on attackers and technology to centering around people and processes. Previously, the administrators could sleep comfortably, knowing that only a few people with physical access could interact with their networked topologies (Hunt, 2019). Over time the needs of these topologies grew to support complex communication systems that interact with employees, contractors, and anonymous guests. Attacks from these anonymous guests are another evolving area. Where former hackers would carry out manual attacks, those with botnets could use automation to increase their leverage. However, the ubiquitous availability of cloud and high-speed networking removes these artificial constraints in the modern world. Now, anyone with a few dollars and an open-source vulnerability scanner can programmatically cluster targets and attack the signature as a whole (Dai Zovi, 2019). Substantial effort goes into protecting these platforms, but little attention considers the other side of the equation—all of these people (Blythe & Coventry, 2018). Modern enterprise networks have hundreds of users that are authorized to perform tasks. When those users fail to detect, mitigate, or control the blast radius can be very challenging (Elifoglu, Abel, & Tasseven, 2018). 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 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 J. , 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 until sufficient awareness, and team members understand the damage that follows their actions. If we can stop the good guys from doing bad stuff, the organization will be in a much better position.

## Where do we need to protect people

Before the Internet, a more limited attack surface could focus on more traditional criminals’ threats, like someone breaking down the front door and stealing the safe. Now businesses are highly connected through always-on technologies that interact with the outside world. The network boundary is now abstract with critical infrastructures and resides outside of the corporate firewall (Paller et al., 2019). Many enterprises outsource systems like Domain Name Services (DNS) and Lightweight Directory Access Protocol (LDAP) instead of self-hosting. With the notion of connectivity spanning multiple contexts, network operators need to consider the interactions from heterogeneous devices that are not entirely under the control of the administrators. How many employees use Virtual Private Networking (VPN) and other phone communication services? How many work laptops also surf the public Internet? Each of these devices is only weakly protected but allowed direct access to sensitive resources. Outsiders can also communicate with employees through emails, snail mails, voice calls, and video chats. Each of these mediums invites unique attack vectors where scammers can attempt to insert unauthenticated messages. If an attacker can manipulate support staff with a 55-cent stamp and one-page letter, why bother with a more complex assault?

## Understanding STRIDE Categorizations

Demystifying security begins with a framework to categorize different attack vectors. STRIDE enumerates these vectors as spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges (Kohnfelder & Garg, 1999). While countless examples result in these scenarios, awareness of their existence provides a basis for people even to consider them.

|  |  |  |
| --- | --- | --- |
| Risk | Cause | Example |
| Spoofing | Failure to authenticate a resource as genuine | An email asks for a 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, creating the need for a more methodical approach. This process could begin with first identifying the different entities and resources within the environment. 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 brewers, 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 allow communication to flow in various contexts. As customers buy coffee, an unspoken protocol begins at the register, followed by waiting in line and receiving a cup shortly afterward. 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 confirm that the first cup was purchased. Maybe, complaining to management about the service results in free Joe. Are these attacks specific to coffee shops? These low-tech attacks are reliable across many human interactions due to a lack of skepticism (Mickens, 2018). Why would the customer try to scam me? That is something that happens to other people, not me (Valiente, 2017). Given the permutations of these scenarios, it is not possible to explicitly training employees, and there needs to be a high-level consciousness of business risks. This transformation requires a complete culture shift toward security awareness.

## Creating a Security Aware Culture

When an organization makes security a core pillar of its design methodology, it reduces risks and provides more reliable services. Integrating this mindset requires a culture shift where the employees are skeptical and ask how implementation and execution will ensure specific performance and reliability metrics. For instance, how are request parameters validated and authenticated? What mechanism authorizes 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 either side. Now, payments are going wrong, and the organization needs to follow complex banking policies 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 accessibility 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 and 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 (Hunt, 2019). The challenge comes from passwords that 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 by confirming 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 (Jonathan et al., 2017).

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 centralizes the storage of credentials. However, these digital identities can accumulate baggage as we mindlessly click through websites (Paller et al., 2019). For example, my personal Google account review shows that three websites are authorized to access location data. From the end-user perspective, these OAuth approval messages are noise that prevents their access to cat articles. Organizations need to augment training programs with periodic reminders that end-users review access and periodically trim the fat.

## 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 or how could a flashlight app be malicious (Hunt, 2019). 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 personal devices. 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 that team members 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, natural friction requires additional attention when security competes with convenience.

## Phishing Sites

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. Training has also told users to look for the security icon when users connect to websites, but this only means the traffic is encrypted (Hunt, 2019). The only alternative is skepticism without a consistent and reliable method to determine that a resource is genuine. 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 authentic site. While none of these methods are fool-proof, they increase the odds of ending at the correct 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 (Paller et al., 2019). These facts are highly discoverable through social graphs. Even when we do not directly share these details, our friends report metadata about themselves that tends to be highly correlated. Public records also report big-ticket transactions, such as property deeds and marriage certifications, detailing 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 (Blythe & Coventry, 2018). From this vantage point, attackers can identify clusters of high-probability targets and go after all of them. These attacks lead to personalized advertisements with a higher click-through rate to an annoying or malicious website.

## 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 can monitor and manipulate unencrypted traffic that flows through them (Paller et al., 2019). 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 convey the necessity for VPN technologies as a mechanism for encrypted traffic tunneling across the hostile Internet to a trusted location. Untrusted networks are not limited to those that run on switches and routers but also include public areas. For example, if two employees openly discuss trade secrets at the coffee shop, they can hear the table next. Other scenarios might center around lost mobile devices in the real world. If they are not encrypted, any information on the device is lost to the public. Users need to understand these are information disclosure vulnerabilities through an awareness program. 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. Security is only partially about stopping malicious actors; the rest is about stopping erroneous actions from legitimate sources, with both introducing challenges to business continuity. Hardware fails, technicians will corrupt customer data, engineers write defects, and administrators will misconfigure services. If the business approaches these scenarios methodologically, incident responses can fail traffic or perform necessary backup and recovery operations.

In many scenarios, manipulating humans is more effortless than attacking 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 in the payment and transaction protocols (see Week 1). These threats are not unique to a café, and 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, understanding the risks will reduce the attack surface and keep the employees safe.

# References

Blythe, J., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviors. *Computers in Human Behavior Volume 87, October*, 87-97.

Brown, T. (2015). A Primer on Data Security. *CPA Journal May Volume 85, Issue 5*, 58-62.

Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly Volume 34, Issue 1, January* 1-7.

Dai Zovi, D. (2019). Every Security Team is a Software Team Now. *Blackhat USA 2019.*

Elifoglu, H., Abel, I., & Tasseven, O. (2018). Minimizing Insider Threat Risk with Behavioral Monitoring. *Review of Business. Vol. 38, Issue 2*, 61-73.

Hennig, N. (2018). Privacy and Security Online: Best Practices for Cybersecurity. *Library Technology Reports. April, Vol. 54, Issue 3*, 1-37.

Hunt, T. (2019, May 20th). *Keynote: Hack to the Future*. Retrieved from YouTube: https://www.youtube.com/watch?v=qCOefMiakps

Jonathan et al. (2017). Security system with three-dimensional face recognition using the PCA method and neural networks algorithm. *4th International Conference on New Media Studies, Yogyakarta, Indonesia, 8-10 Nov*.

Kohnfelder, L., & Garg, P. (1999, April 1st). *The threats to our products*. Retrieved from Microsoft Security Blog: https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/

Mickens. (2018, August 16th). *Why Do Keynote Speakers Keep Suggesting That Improving Security Is Possible?* Retrieved from YouTube: https://www.youtube.com/watch?v=ajGX7odA87k

Mickens, J. (2015, September 9th). *Not Even Close, The State of Computer Security with Slides*. Retrieved from YouTube: https://youtu.be/tF24WHumvIc

Paller et al. (2019, March 7th). The Five Most Dangerous New Attack Techniques and How to Counter Them. *RSA Conference.* Retrieved from YouTube.

Proctor, R., & J, C. (2015). The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace. *Human Factors Aug; Vol. 57 (5)*, 721-727.

Valiente, C. (2017). Addressing Malware WITH Cybersecurity Awareness. *ISSA Journal. Oct, Vol. 15, Issue 10*, 16-22.

Whitty et al. (2015). Individual differences in cybersecurity behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior And Social Networking Jan; Vol. 18 (1)*, 3-7.