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 are simply broken. 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 |

## Applying these ideas to getting free coffee

## Using threat modeling here

## Creating a Security Aware Culture

## Credential Management

## Device Management

## Phishing Sites

## Doxing

## Untrusted Networking

## Challenges with Internationalization

## Conclusion