Cameron Waddy

April 26, 2021

Intro to Cybersecurity, Technology, and Society

Professor Bowman

Cyber in Society

Everyday people are using their technological devices to store private information. Our credit cards, social security numbers, and other personal information float around on different platforms, apps, and websites that we use daily. What you may not realize is how vulnerable all of that information is if you do not protect it properly. Developing strong cyber security principals in both personal use and enterprise uses are essential to protecting this highly private and confidential information. If you do not, then you are at an extreme risk of losing your identity, valuables, and money of which will be extremely tiresome and sometimes impossible to recover.

I want to first give an example of what cyber technology impacts. These examples are critical infrastructure that you may not think of everyday, however they impact your day-to-day activities in some way. Cyber technology has a large impact on how systems are engineered. Without the incorporation of cyber technology into systems, they would be exposed to attacks that can steal important information, cripple systems, or cause outright economic disaster. Techniques to fortify these systems from these consequences are, but not limited to, "cyber enterprise architecture, effective implementation of North Atlantic Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements., consistent cybersecurity requirements for system procurement Requests for Proposals (RFPs), and cyber assessment for operational technology (OT) systems defining risks based on impacts to safety,

reliability, key functions, processes and compliance." If you are scratching your head wondering what I just said, I will give some more detail. NERC CIP is a “set of requirements designed to secure the assets required for North America’s bulk electric system.” (Justin Peacock) An RFP or request for proposal is a business document that announces a project, describes it, and solicits bids from qualified contractors to complete it. Some systems that are highly important to the economic infrastructure such as the electrical grid, nuclear power plants, and hydroelectric dams must be fortified in security both through physical means and technologically from all attackers. Due to information being an extremely viable asset to operations, it must be protected. Information does not just stay within the walls of these important infrastructures. It also flows to and from supervisory points or monitoring stations "off-campus" or other centralized locations. These lines of data need to be monitored and maintained using cyber technology to ensure the authenticity and reliability of the data without an unknown third-party leeching for their own personal gain. Cyberattacks can be fronted from anywhere in the world, so we must be able to protect against threats that we think we know of as well as threats that we do not see coming. The more cyber technology is implemented into these infrastructures, along with protocols to respond, and react to an attack, the more necessary it is to protect important engineering systems properly.

There are malicious cyber-related activities that directly impact businesses by their own employees called insider damage or insider threats. Insider damage is the cyber threat of employees that work within the company or have access to private company information. Cyber inside threats are normally made by individuals who are “primarily male and held highly technical positions, the majority hired with system administrator or privileged access.” This threat can arise from many situations but different types of cyber threats from insider threats are

sabotage, fraud, and theft of IP. An example of a case involving all three incidents was when "the insider quit his job following an explosive argument with his coworkers. When no severance package was offered, he proceeded to make a copy of the software he had been developing for the company, deleted the software from its systems, and stole the backup tapes. He then offered to restore the software for fifty thousand dollars." In 2020, there were 4,716 cases of insider threats where sabotage, fraud, or theft of IP occurred. For over half of insider threats reported were seen as upset due to the recent or past negative event that had affected them poorly, thus they acted out in revenge. Some of these negative events could be arguments with supervisors or coworkers, demotions or transfers to new departments, terminations, or what seems to be an inadequate increase in bonus or a decrease in pay. The best way to prevent inside threats is by incorporating a layered defense strategy. This is done by following mandated policies, procedures, as well as technical controls. However, these will only be affecting if supervisors or managers follow and enforce these defense strategies.

Two key trends in identity management are cloud access security broker and biometrics. Cloud Access Security Broker (CASB) is a security point to protect the cloud. The cloud is a very flexible and affordable place to store your data on servers where you can expand or shrink your storing capacity based on your needs. CASB, or cloud access security broker, is "an on-prem or cloud-based software that connects the cloud provider and the cloud service consumers with better security." (Hasti Valia, 2020) The CASB is regulated in accordance with Hybrid Identity Protection (HIP), California Consumer Privacy Act (CCPA), and General Data Protection Regulation (GDPR) to ensure that your data is safe from attacks on their cloud providence. The second key trend I want to talk about is biometrics. This is one of the best and most secure ways to store and protect data. Biometrics is the use of things like your voice,

fingerprint, eye, or face to secure information. The means of hacking your way into an infrastructure is near impossible with biometrics. Fast ID Online (FIDO) is not only an organization, but it is a protocol used to protect and provide stronger authentication online. FIDO uses their protocols to further protect their user's security and confidentiality by not allowing private information to be used by other online services. Also, if biometrics are used, they never leave the user's phone. If not made clear, FIDO addresses the worlds over-reliance on passwords and is making strides in moving users to a public/private key cryptography. "FIDO Authentication enables password-only logins to be replaced with secure and fast login experiences across websites and apps."

Authenticity and integrity play a big role in making cryptography a valuable means of protecting information and ensuring that it is unchanged. With authenticity in cryptography, it makes users of cryptography to properly identity an individual. This is extremely helpful especially in cases where the second party has no personal or valid knowledge that the first party is who they say they are. Having this security ensures there are no attackers trying to steal confidential information. The way this is achieved is by using digital certificates. Integrity presents itself by ensuring the information is original and unaltered in any way, shape, or form. This means that the message is received the way that it was sent. Cryptography uses a thing called hashing that creates a unique message digest from the message that is sent along with the message. After this occurs, the part receiving the first original message will then create a second digest to compare it to the original sent digest. This step is important because it helps prevent unintentional alteration to the message. Without integrity, encryption of the message itself will not guarantee privacy of content.

Reference:

Cappelli, Dawn, et al. “Common Sense Guide to Prevention and Detection of Insider Threats.” *Cylab.cmu.edu*, Carnegie Mellon University, July 2006, www.cylab.cmu.edu/_files/pdfs/CERT/CommonSenseInsiderThreatsV2.1-1-070118-1.pdf.

Peacock, Justin. “What Is NERC CIP.” *CyberSaint Security*, www.cybersaint.io/blog/what-is-nerc-cip#:~:text=North%20American%20Electric%20Reliability%20Corporation%20Critical%20Infrastructure%20Protection%20(NERC%20CIP,North%20America's%20bulk%20electric%20system.