Name: Jacob Pelletier

Instructor: Christopher Bowman

Course: CYSE200T/Spring2025

Date: 04/26/2025

Systems and Humans: Which is more important?

Introduction

Technology is ever evolving, it has become integrated into nearly every aspect of our daily lives from social media, banking, medical records, even grocery shopping. Of course there is no point in arguing that society has benefited from the implementation of technology and continues to do so. However, because of its systemic implementation, have we become complacent in recognizing our role in maintaining its integrity? As technology has advanced, so has the need for systems and malware to be developed in order to maintain these systems. Furthermore, as these systems and evolved in complexity, so has the defensive systems put in place to secure them. We rely heavily on the use of technology driven systems to protect and maintain technology itself. Though there are several functions that cannot be done as efficiently by a human being as it can be by some form of computer system, that doesn't necessarily reduce the human factor in cybersecurity.

Cybersecurity is a finely turned dance that occurs between the system and the user. In this dance, both the system and the user must work together in order to produce maximum efficiency. If one falls behind, then the other element weakens significantly producing a break in continuity within security chain. A great example of how these elements of cybersecurity must coexist and are of equal importance can be found when analyzing SCAD, also known as, Control and Data Acquisition systems. These are important systems used in large-scale infrastructure for data collection and control. It is composed of remote terminal units that gather information from various locations and feed it back to a central system, which is viewed by an operator through a human-machine interface that contains real-time data being collected. These systems can be found in a variety of settings, including power plants, waste centers, smart buildings, public transportation, and many more. There is no argument to be made that SCADA systems are effective when functioning correctly. However, though Supervisory Control and Data Acquisition systems have been, and continue to be implemented into modern infrastructure, the system does have a major vulnerability in its ability to be effective and efficient. One of the most obvious vulnerabilities of these large and complex systems, is not its susceptibility to systems malfunctions, or technology based failures. The most vulnerable aspect of these systems can be found in the rather minuscule role that the user, or operator plays within these systems. Though it may not be where the most complexity or productivity is found, the user (human) of this system holds a

significant amount of importance in maintaining the integrity of this system and the information that it houses. In many cases, and SCADA systems are no exception, security breaches can often times be traced back to some form of human error. Something utilizing an unsecured network could be held responsible for potential large-scale data compromise resulting in billions of dollars. Because SCADA systems utilize human-machine interface, many aspects of the system, including Remote Terminal Units (RTUs) and Programable Logic Controllers (PLCs), can be accessed remotely via various applications. Using these applications, especially on unsecured networks, could provide a weak point in the security system, allowing attackers to gain access through those applications. When it comes to mitigating vulnerabilities in a SCADA system, the National Institute of Standards and Technology created standard practices to help reduce the risk of security breaches. Some examples of these practices include using virtual patching to help manage updates and patches, applying network segmentation, using adequate security measures between the ICS network and corporate network, properly managing authorization and user accounts, and using endpoint protection on engineering workstations connected to SCADA for device programming and control adjustments. Though there are systems and policies in place to reduce the risk, and effectively maintain incidents of security compromise, are we downgrading the importance of the human element of cybersecurity. The reality is, regardless of how advanced and complex technology becomes, the first, and weakest

element of the security chain will always rest with the user. Ironically, the most insignificant and involved element of technology, is also the most important.

Solution

So the question is how to we address the problem that is human error within the cybersecurity field? The projected global funds allocated towards cyber security are set to reach as high as $459 Billon in 2025. Only a projected $10 Billion is estimated to be allocated towards cybersecurity awareness training. Though $10 Billon is a substantial amount of allocated resources, it is hard to argue where the priority lies within the cybersecurity industry. There needs to be a shift in thinking regarding the importance of the human element within Cybersecurity. Governments and corporations need to prioritize human defenses as it is not only the most cost effective, but because it also remains one of the weakest links in the cybersecurity system. It is simply not enough to provide annual training to employees and expect them remain proficient, as well as vigilant in regards to safe cyber practices. The mindset that the responsibility of cybersecurity within the work place is the sole responsibility of IT specialist is simply not a viable practice. The reality of the situation it that non-IT individuals play the most important role in prevention while IT specialist play a more involved role in incident management/mitigation. apply a significant portion of the budget to cybersecurity awareness training. Furthermore, while technology

driven systems and programs are extremely beneficial and lack the potential for human error and complacency, it does not replace the need for a strong foundation in cybersecurity awareness and safe practices at the employee level.

Conclusion

As technology evolves and becomes more integrated into aspects of society, so is the need for cybersecurity awareness to evolve. We cannot expect the system to operate effectively when a large component of the system is not held as equally important as others. Regardless of how advance technological systems become, the reality is that the human element will never be completely removed. Because we cannot remove the human element, the potential for human error will always be present. It is our responsibility to acknowledge the significance of human beings both positive, as well as negative, and the impact that we play in cybersecurity.

Sources cited:

Trend Micro Research. *One Flaw Too Many: Vulnerabilities in SCADA Systems*. Trend Micro, 16 Dec. 2019, https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems.

Morgan, Steve. *Boardroom Cybersecurity Report 2024*. Cybersecurity Ventures, sponsored by Secureworks, 5 Nov. 2024, https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024.