Elliot Mason

12/01/2024

CYSE200T

Who Should Cybersecurity Rely On?

There is no doubt that the line between humans and technology in the cybersecurity world is very frayed. While humans can cause human errors and technology can shut down due to outdated tech systems or even just weather, neither is perfect nor can completely run our cybersecurity systems. One may work better than the other for certain types of companies and businesses in their personal information systems and cybersecurity, but neither should overtake the other. We cannot completely rely completely on one or the other to control all systems. Both have risks, both have mass benefits.

The Human Factor in Cybersecurity

Everyone knows humans have errors in almost everything. It just so happens that in the cybersecurity world, that can have a massive impact. I believe the human factor and prioritizing maintaining it as well as enforcing training to prevent it, is overlooked greatly. Humans have a large impact on cybersecurity whether it is part of their job to maintain it, or they just work under the same network as information systems. Human error can be as simple as clicking on a phishing link or as intentional as a planned cybersecurity breach. However, due to how unreliable technology can be by itself, humans are the ones who can physically reset, update, fix, and restore these systems.

The Technology Factor in Cybersecurity

While the use of technology is inevitable, as yes humans can't have firewalls and the ability to run servers and motherboards, it changes frequently and has its own issues. When working properly, technology can help run servers and networks smoothly, send alarms, when possible, threats are detected, and have helpful data for companies and businesses that otherwise humans would take too long to gather. However, with more technology, comes more risks. Hackers use technology to commit cybercrime attacks, cyber fraud risks are heightened, and technology isn't always reliable. With newer technologies, more updates and setting up those systems arise…these require the work of humans. Technology and systems working in a cybersecurity framework can also be affected by random shutdowns, power outages, and even weather-related damages.

Human Training or More Technology?

Both training and cybersecurity technology are crucial in mitigating risks and lowering human risks. Technology can be strong and most of the time predictable to normal shutdowns and reboots. Humans, meaning employees, however, are unpredictable when it comes to cybersecurity. Human error is a huge risk in cybersecurity. Companies should allocate a good amount of funds and time into human training to limit and mitigate human error and risk. These trainings should include training on the cybersecurity technology, training on how to control threats and how to recover from attacks if they so happen.

Human risk and error are almost always the most likely to occur and extremely unpredictable. This is why human training should be extremely important in the cybersecurity world. Errors and mistakes occur, but in cybersecurity it can create a larger issue than just a little

mistake. Technology that can defeat and prevent outsider threats and keeping those systems updated are also extremely important. Technology changes and requires updates to continue to function properly. Human training and individual research can help to stay up to date with technology systems and therefore put in the work to keep systems running properly with the help of technology. Systems don't have brains, eyes and can research, humans can. Humans can then put forth that training and research with the help of the technology they have at their hands. The more technology, the more updates, unknown problems, workarounds, and more things to try to handle.

How They Can Work Together

Like mentioned at the beginning at this paper, cybersecurity should not rely on one or the other, there should be some kind of balance to have a proper and secure system in place. There are many critical infrastructure systems in the world of cybersecurity that are at risks of attacks. There are systems like SCADA that are put in place to help reduce attacks, these systems are a good example of how humans and technology work together to secure our critical infrastructures.

Critical Infrastructure Systems

Critical infrastructure systems such as power grids, water supply, communications systems and more are subject to being at risk of cybersecurity attacks. These critical infrastructure systems hold high vulnerability for cybersecurity attacks and systems need to be put in place to protect them from such. These infrastructures are crucial to society and governments and the risk they pose puts not only the systems in jeopardy but the government and possibly society as well. Outdated systems, failed mechanisms, weak signals, unsecure accessing is all things that pose risk due to vulnerability. There are also natural threats such as natural

disasters that could weaken or damage these systems. The main cybersecurity threats are those of human threats such as terrorism attacks and cyber-attacks (International Journal of Control and Automation pg.17-20).

SCADA System

Many of these critical infrastructures now are secured and controlled by controlled systems such as SCADA. SCADA stands for Supervisory Control and Data Acquisition. It is used to control some of these critical infrastructure systems such as water treatment facilities pipelines, wind farms and more. The SCADA system however does not directly control these processes in real time but instead controls and coordinates with the processes. There are many parts to SCADA systems that enable it to control and process data to keep these infrastructure systems operating. These systems communicate with the equipment of these infrastructures to enable it to run properly while also having Human Machine Interface (HMI) that gives data processed form this infrastructure communication back to a human operator. In a sense, SCADA is the middleman for operations (SCADA Systems pg. 1-4).

Overall having SCADA systems in place for these critical infrastructures gives control and some more security then if they weren't controlled all together. Real time monitoring and communication with human operators ensures that if anything fails and goes wrong, someone can acknowledge it and hopefully fix it before it opens vulnerability to the infrastructures. SCADA also helps control who has access and is authorized to be in any sort of access or control of these infrastructures. SCADA systems can also place incident response commands and therefore work to combat a cyber security attack or other threat before it becomes detrimental. SCADA systems are important to have in place for these critical infrastructure systems to reduce risks and vulnerability.

The Balance

So yes, both the human factor and the technology factor are important in the cybersecurity world. Both have their risks; however, both also do things that are critical that the other cannot perform. They both also have the ability to check each other. Humans help maintain the physical aspect of technology as well as updating systems while technology continues to change. Technology also has similar ways of checking humans and more so employees within companies, it does this by putting up firewalls, helping prevent phishing links from being accessed, and sending detection alarms when possible threats arise.

A balance should be found within the world of cybersecurity, both human factor and technology are incredibly crucial for cybersecurity frameworks and to keep data safe and our infrastructure systems running. Humans and technology working together form a strong shield against cybersecurity attacks, natural threats, and other human threats, as well as having plans to recover in the event an attack or threat arises. Finding a balance for the two to work together is the best way for the human factor and technology to exists in the cybersecurity world. This creates the safest route for confidential information, critical infrastructure systems, and anything else.

Works Cited

"The Human Factor in Cybersecurity." SecurityScorecard, 1 July 2024, securityscorecard.com/blog/the-human-factor-in-cybersecurity/. Accessed 01 Dec. 2024.

"Risks of Emerging Technologies in Cyber Security: RiskXchange." Riskxchange.Co, 30 Aug. 2024, riskxchange.co/1007713/risks-of-emerging-technologies-in-cyber-security/#:~:text=How%20has%20technology%20advanced%20cybersecurity,elaborate%20and%20complex%20cyber%20attacks. Accessed 01 Dec. 2024.

Robles, Rosslin, et al. " Common Threats and Vulnerabilities of Critical Infrastructures." International Journal of Control and Automation, citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7098a29a404f8561c7f3c66801b6e1f36f88b7b7 .

"SCADA Systems." SCADA Systems, www.scadasystems.net/. Accessed 29 Nov. 2024.

Technative. "Why Cybersecurity Is Also a Human Issue, Not Just a Technology One." TechNative, 23 June 2024, technative.io/why-cybersecurity-is-also-a-human-issue-not-just-a-technology-one/. Accessed 01 Dec. 2024.