Taylor Ball
12/10/2023

What can we do to help with the 'Short Arm' of predictive knowledge?

Introduction

1}With the increase in technology the knowledge we have as a society is always changing. Due to this, we have a lack of knowledge to the foresight of the consequences for the actions that are taking place today. All the different policies and infrastructures we make is also always changing and we can't predict what it is going to be like in the future, but we can always guess. There are things I think we can do to at least lower the 'short arm' of the predictive knowledge. Having flexibility will help because cybersecurity is always changing. The certain things I think that can help us better understand the short arm in predictive knowledge are possibly human factor especially research and training, maintaining the upkeep of the CIA Triad, and also implementing SCADA Systems.

The Human Factor in Cybersecurity

The human factor is a critical component of cybersecurity, it refers to different situations when human error results in a successful data breach. Human error is the leading cause of cybersecurity breaches. In 2021, it was found that human error was responsible for 95% of different breaches according to the "IBM Cyber Security Intelligence Index Report" (Tech, 2022). Training is important to help decrease that amount of security breaches being held due to human error. There are certain reasons why I think human error is important to lower the short arm in predicting knowledge.

3}Training can help lower the risk of being cyber-attacked and making the people change their software all the time. It will also help the people in those trains know of to protect themselves and identify the risks. Investing in ongoing training programs for cybersecurity professionals can keep them updated on the latest different threats, technologies, and the best practices to avoid cyber-attack risks. Training can also help us with flexibilities in the cybersecurity business. Cybersecurity needs to be flexible because the field is always changing. Training can be customized to the needs of any kind of organization to help them better understand what is going on in cybersecurity.

The human factor in cybersecurity, I think needs to be fixed because there are too many security breaches due to human error, so I think training is something that can us learn. We need to learn how to protect ourselves and other people for the upcoming future in cybersecurity even though we will never know for certain what is coming. Due to that, I also think we need to be flexible due to all the changes that are and will happen in the field of cybersecurity.

The CIA Triad

Currently, the CIA Triad is one of the most prominent models for guiding information security policy in any organization. When a cyberattack occurs to a organization, I can be sure that at least one of these principles had been violated (Philip, 2022). I think the upkeep of the CIA Triad will help the short arm of the predictive knowledge will help us focus on the future of cybersecurity by helping protect the present and when it is attacked it can help us fix the software and improve it.

The CIA Triad is short for Confidentiality, Integrity, and Availability. The CIA Triad is a model designed to guide policies for information security within an organization (Chai, 2022). The CIA can be broken down to the three key concepts. Confidentiality is basically the equivalent of privacy. Measures are designed to prevent sensitive information from unauthorized access attempts (Chai, 2022). Integrity is the consistency and trustworthiness of data for a long time. The data that is given cannot changed or altered. Availability means that the information that was given is always accessible for authorized users. The CIA Triad is important because it can guide the development of security policies for organizations. Some examples of the CIA Triad are User Ids and passwords, user access controls, and firewalls.

2}The CIA Triad can be slip up into different part which include confidentiality, integrity, and availability. Confidentiality is security, integrity is constant, and availability is being able to access something at all times. The upkeep of the CIA Triad can help us with the short arm of the predictive knowledge of the field of cybersecurity because it stops certain cyberattacks and it can help us predict the outcome of the cyberattacks and help fix the software for future references.

The SCADA Systems

The SCADA (Supervisory Control and Data Acquisition) is a system of software and hardware elements that allow industrial organizations to control and monitor industrial processes locally or at remote locations. I think the SCADA is trying to help infrastructure improve so we don’t so many human error is the workplace and it also, gives real-time data status of the various devices, it we can make the equipment better for the future.

Critical Infrastructure are those systems and assets that are so vital that their incapacitation or destruction would have a debilitating effect on security, the economy, public health, public safety, or any combination (CISA, 2023). Critical infrastructure has various threats and vulnerabilities that can compromise its functionality and security. The vulnerabilities can be intentional or unintentional, natural, or man-made, physical, or cyber. The most common sources of vulnerability are natural disasters, public health emergencies, malfunctions, cyber-attacks, and terror attacks (Johnson, 2019).

4}Supervisory control and data acquisition is an automation control system that is used in industries that may use energy, oil, gas, water, power, and a lot more (Krambeck, 2015). The SCADA System does not control the processes in real time it usually refers to the system that coordinates the processes in real time. The HMI (Human Machine Interface) is linked to the SCADA system’s databases to provide the diagnostic data and manage information and tending

information. It also helps with maintenance procedures and troubleshooting guides. Programmable logic controllers (PLCs) control the flow of cooling water, which will set off alarms if the systems change and be recorded and displayed. Remote terminal unit connected to the physical equipment, by converting and sending the electrical signals to the equipment, like closing/opening a value or setting the speed of a pump.

Conclusion

In conclusion, I think there are many ways to lower the short arms of predict knowledges. The human factor in cybersecurity especially training, the upkeep of the CIA Triad, and implementing the SCADA Systems can help us better understand what we can do in the future to help us have more knowledge of the field of cyber security. Training helps us lower the risks of cyberattacks due to human error and it helps us protect ourselves and others from breaches of our information. The CIA Triad and SCADA Systems helps us understand what we can do to improve the software and hardware so we can protect ourselves from attacks. If CIA Triad is hacked we can see what principle was weak to have it hacked, so we can strengthen it. Also, the SCADA System gives us real-time data status, we can improve the equipment to do the different jobs to help the company or organizations.

References

Chai, W. (2022). What is the CIA Triad? Definition, Explanation, Examples. 1-7.

CISA. (2023, November 5). *Critical Infrastructure Systems*. Retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems

Johnson, B. (2019, December 31). *CISA Confronts 2020's Top Critical Infrastructure Threats*. Retrieved from COUNTERTERRORISMEMERGENCY PREPAREDNESSFEDERAL GOVERNMENT: https://www.hstoday.us/federal-pages/dhs/cisa-confronts-2020s-top-critical-infrastructure-threats/

Krambeck, D. (2015, August 31). *An Introduction to SCADA Systems*. Retrieved from All About Circuits: https://www.allaboutcircuits.com/technical-articles/an-introduction-to-scada-systems/

Philip, L. T. (2022, November 29). *Understanding the CIA Triad: A Comprehensive Guide to the Three Pillars of Information Security*. Retrieved from Lipson Thomas Cyber Security: https://lipsonthomas.com/cia-triad/

Tech, T. (2022, November 10). *Human Factors in Cybersecurity: Protect Yourself*. Retrieved from https://telefonicatech.com/en/blog/human-factors-in-cybersecurity