Analytical Paper

Madelene McFarlane

4/19/2022

Details

In modern society more and more people rely on technology for reasons that they are not fully present minded of. Most people will think about shopping online, bank account information, or posting on social media. Though there is a greater impact that technology has in the background of present-day society. The groundwork of these systems are the CIA triad, SCADA systems, and finally using the example of the legal system of the struggle and benefit of growing technology in regards to cybersecurity.

Starting off, the CIA triad is an information model that is valuable within the information security field. The CIA triad contains three core principles which make up the initials of the model's name. These principles being Confidentiality, Integrity, and Availability. Implementation of these principles offer professionals the challenge of creating priorities within the policies that they create.

The first principle of the CIA triad is confidentiality. Confidentiality gates data in a way that only people within authorization and processes can access and modify the data. Often times laypeople will view the general term of cybersecurity as 'anything that restricts access to data' (Fruhlinger, Josh). Though overall that mindset is within the guidelines of confidentiality. An example of CIA triad confidentiality is public-key cryptography which is an infrastructure that includes both Authentication and Authorization.

Information security refers to the two terms of authentication and authorization as the two big As. Authentication is a layer of security in order to confirm the user as who they say they are. The users identify being able to be confirmed by the use of biometrics, security tokens, and passwords. Authorization, however, determines who is granted the ability to access the data. For example, just because a student has logged onto their college website does not grant them sensitive information regarding grades, finances, or future assignments.

The second principle of the CIA triad is integrity. Integrity holds that data should be upheld properly so that ill-modification cannot occur. An example of integrity is that certain files can be read and accessed by certain users. Though those same users are not able to modify them. Therefore, the data is being upheld to only be modified by those granted the authorization to do so, but the other users are still able to access the data to look over.

Lastly, the third principle of the CIA triad is availability. Availability is authorized users being able to access the data and modify it as needed when the data is requested. This being shown when a user is keeping their system's hardware up to date that way, they can maintain access to the needed data. The ability to access needed data is very important in the overall system of operation and maintains a key point in the triad. If something were to go astray with availability users would notice right away such as a denial-of-service attack.

The CIA triad is a core model to information security. Within the model there are three principles being confidentiality, integrity, and availability. The three principles within the triad allow for professionals to measure priorities within a system. Then from the priorities the professionals are able to enforce policies in order to maintain proper upkeep following the CIA triad.

Next off is SCADA systems and how important protection is to these systems for modern day life. SCADA, supervisory control and data acquisition, systems are systems that control infrastructure processes, facility-based processes, and industrial processes. Processes such water treatment, airports, production. SCADA systems also involve the help of subsystems as well. The subsystems that are normally present in SCADA systems being remote terminal units (RTUs) and Programmable logic controller (PLCs).

While SCADA systems provide efficient workplace environments and remain helpful to society. There are security issues that can arise due to the systems vulnerabilities and applications. SCADA systems as mentioned previously control key processes to society and therefore makes SCADA systems potential targets of cyberterrorism/cyberwarfare attacks. Due to SCADA systems having a great impact in modern society through traffic lights, gas transportation and many more. These key functions of everyday life making SCADA systems security 'extremely important because the destruction of the systems would have very bad consequences' (SCADA Systems).

When it comes down to threats against the SCADA system there are two main variations. There is the first kind of threat of unauthorized access to the SCADA system software. Then there is also the second kind which is tied with packet access to the network that host SCADA devices. Both of these threats being detrimental to the SCADA system and the inspiration behind security methods to keep these threats at bay.

The first threat of unauthorized access can be in two different forms. The first form being human access meaning actual people physically coming into the system and causing damage. Then the other form being a more digital sense of unauthorized access. This form containing intentionally inflicted damages, virus infections to hardware/software, along with other methods that can affect the control host machine in the SCADA system.

The second threat being related to packet access. There is a lack of security on the actual packet control protocol. Therefore, this leads to a massive vulnerability because the user that is sending packets to the SCADA device is in control of the device. The small blanket of protection that a VPN provides is not enough to protect the system against physical access attacks to devices within the SCADA system. Network switches for example of a device.

SCADA systems are a key part of modern society. These systems provide many beneficial essentials to everyday people and some of which rely heavily on the production. Therefore, the security in SCADA systems remain very important to society. While protection measures are in place there are still vulnerabilities within the interworking's of the system that need to be revised.

Lastly, when it comes down to new technology advancements some find themselves eager to learn about the new processes. While others prefer to stick with what they know and do not feel the need for change. This is a matter of preference but due to the growing change within the legal system new practices are needed to better the flow of the congested legal system. The methods to better implement the new technology in the legal system will take effort, but after the curve the benefits will over way any hardships.

The world of technology is constantly evolving and 'is changing the way that legal services are delivered'(Ryan.F). Therefore, it might be difficult to fully keep up with the progress when in a non-tech field. However, having teams or weekly updates concerning necessary announcements would help the information to be more palatable to a non-tech employee. Along with keeping them updated on important factors that they should be aware of. While avoiding the clutter of technical talk that they might block out due to a learning curve.

Another way to implement new technology in the legal system is by providing hand-on training when needed. For example, if a new program or update was released and it was said to save time on processing legal files this would be a benefit to the system. Though many employees would need guidance throughout how the program works to avoid setbacks and untrained bias to the outdated models.

The legal system is our only legal system. The technology used within the system is not the key factor in delaying the congestion that the legal system faces. Untrained and biased employees of the legal system are sticking to what they know and feel confident in. Without

knowing the benefits of programs that would help the flow of their everyday lives. The main bridge between the two that needs to be enforced being education and training. Why walk when you can learn how to drive.

Within society there are main surface level risks that one may think about when they look at cybersecurity and technology. Though the risks and protection needed to keep modern day technology running goes far deeper then social media passwords and text messaging. Cybersecurity is needed on many levels such as SCADA systems. Along with workers needing to update ways that systems function in order to better their company's workflow. All of this while still remaining true to the CIA triad and keeping people and their systems secure.

References

Broussard, C., Brown, K., Cordova, D., & Mauldin, S. (2017). *Teaching Legal Technology*. New York Law School. Retrieved April 4, 2022, from https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=1917&context=fac_articles_chapters

Fruhlinger, J. (2020). The CIA triad.pdf. The CIA triad: Definition, components and examples. Retrieved March 8, 2022, from https://drive.google.com/file/d/1Mn3icTLG5X3W7tJjuDaohW8OscHdLOQI/view

Firdaus, Zakuan & Jamil, Norziana & Qassim, Qais & Rusli, Mohd & afar, Norhamadi & Daud, Maslina & Hasan, Hafizah. (2018). A Study on Security Vulnerabilities Assessment and Quantification in SCADA Systems. Journal of Engineering and Applied Sciences. 2018. 10.3923/jeasci.2018.1338.1346.

Nweke, L. O. (2017). Using the CIA and AAA models to explain cybersecurity activities. Using the CIA and AAA Models to Explain Cybersecurity Activities. Retrieved March 9, 2022, from https://pmworldlibrary.net/wp-content/uploads/2017/05/171126-Nweke-Using-CIA-and-AAA-Models-to-explain-Cybersecurity.pdf

Mir, Suhail & Quadri, Syed. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security. 07. 185-194. 10.4236/jis.2016.73014.

Ryan, F. (2020). *Rage against the machine? incorporating legal tech into legal education*. Taylor & Francis. Retrieved April 4, 2022, from https://www.tandfonline.com/doi/abs/10.1080/03069400.2020.1805927

SCADA systems. SCADA Systems. (n.d.). Retrieved March 14, 2022, from http://www.scadasystems.net/

Van Der Ham, J. (2020). Toward a better understanding of "cybersecurity" toward a better understanding of "cybersecurity". Toward a Better Understanding of "Cybersecurity". Retrieved March 8, 2022, from https://dl.acm.org/doi/fullHtml/10.1145/3442445

Yadav, G., & Paul, K. (2021, April 8). *Architecture and security of SCADA systems: A Review*. International Journal of Critical Infrastructure Protection. Retrieved March 14, 2022, from https://www.sciencedirect.com/science/article/abs/pii/S1874548221000251

Zakharova, M. V. (2022, March 1). *Training of academic lawyers for implementation of high-tech research projects*. Journal of Physics: Conference Series. Retrieved April 4, 2022, from https://iopscience.iop.org/article/10.1088/1742-6596/2210/1/012016/meta