Shawn Ziegler

CYSE 200T

Analytical Paper

4/23/25

The Analytical Paper

The Short Arm of Predictive Knowledge

(1) As discussed in the Jonas reading, there must be a balance between expecting a potential issue and remaining flexible. It is very difficult to predict what future challenges could occur. The guidelines provide a base to adapt as challenges appear. The goal is to generate regulations that highlight key priorities. Protecting essential assets, maintaining functionality, as well as ensuring that systems remain strong and are open to new modifications and information. The focus for the system is to ensure that it can undergo conditions that occur unexpectedly. It is essential to implement protection, consistent updates, and preventative barriers to enhance the durability of the system. Anyone involved within the system must receive regular training to verify that each person involved understands their role. The development of policies and guidelines should be flexible and dynamic because future risks are unpredictable

This leads me to the next topic, the CIA triad. The letters CIA stand for Confidentiality, Integrity, and Availability. The CIA triad is a model that allows organizations to guide policies for information security. These three principles are the most important components in information security. Availability entails that access to reliable information is guaranteed if

authorized. Confidentiality is a set of restrictions that regulate access to information. Integrity declares that the information is accurate and true. The CIA triad model is a fundamental framework used in cybersecurity to protect important information.

Importance of the CIA Triad

(2) Each letter within the triad represents key components within cybersecurity. The triad is a useful tool to guide the development of new products and technologies for organizations. The organization can use the triad to evaluate the needs and how value is being provided in these components. A good example of confidentiality is banks requiring an account or routing number when accessing a bank account online. This ensures that only the owner of the bank account is granted access to the account. A good example of integrity is running backups to restore affected data back to its natural state. This allows everything to be operating back to normal if an attack were to occur. Great examples of availability are making sure all hardware is immediately repairable, also making sure system upgrades are made when needed. This will ensure a properly functioning operating system. Authentication is a method used to verify a person's identity. On the other hand, the authorization method gives a person the right to access a system and its resources. The authentication process relies on credentials. A good example of this is when a person uses a username and password to log in to a computer or program. This requirement allows only authorized users to have access. Another example is when a person needs to scan an I.D. or scan their fingerprint to enter a building. This technique ensures that a stranger will not be able to enter the building without providing these credentials. Authorization relies on gaining permission to access a specific network or program. A good example of this is a company's database; the person must be authorized to be able to access any files or navigate through the

database (Kosinski, 2024). This protects the company from cyberattacks and losing important files that may contain sensitive information.

(3) When it comes to creating regulations within the company, it is important to invest in training because it is a more effective way to fight against cyber threats. In cybersecurity, it is important for employees within the company to be properly trained so they are able to do their job proficiently and be well prepared if an incident were to occur. Although many companies rely solely on technology as a safeguard, it tends to become outdated, and replacements need to be made in order to adapt to technological advancements. These technological sources usually require a lot of maintenance to ensure they are working efficiently. Investing in training is a more cost-effective investment. Investing in proper training for employees allows for the development of new skills and strengthens the skills they already have (Cyberbitsetc). If companies invested in technology, they could invest in the SCADA system, which allows the company to have real-time monitoring. The company investing in this type of system ensures that they are able to identify the problem right away, as well as try to resolve the issue right away to mitigate the risks. The company will also have security measures to make the process easier to detect cyberattacks in real time. Investing in this system allows the company to detect threats that were not detected by people within the company. This system will keep track of facility-based processes, control infrastructures, and industrial processes. Updating hardware and software, as well as procedures and policies, allows for the system to run proficiently and effectively. Developing a firewall and private network protects the company as well as reduces the risk of vulnerability (Edwards 2021).

Conclusion

The CIA triad is a very important tool to utilize within an organization, as it allows companies to have a guide for information security. Authentication and authorization are both very important because they both provide security for an organization. A company needs to invest in training its employees to ensure they are well prepared when a cyber-attack occurs. Investing in proper training allows for these employees to sharpen up their skills within their roles as well as develop new skills to ensure they are prepared for an attack that has never occurred before, and allows them to have the knowledge of new strategies to implement to fight off these attacks. Companies implementing regulations ensure that companies is able to handle situations as they occur, as predicting the future is not possible; these regulations allow for companies to be prepared. These guidelines within the company must be flexible as they make it easier to make adjustments when needed to adapt to the incident being faced. All these factors ensure that everyone involved within the company is well prepared and that the security system remains strong and runs proficiently. With the implementation of the SCADA system, companies are able to monitor facility-based processes, industrial processes, and control infrastructures. This system also allows companies to have a real-time security monitoring system to mitigate the risks of potential cyberattacks, as the company will be able to respond and adapt to attacks as they happen. As long as the company keeps hardware and software up to date, the system should run smoothly. Companies that do not have a SCADA system may not be aware of the attack taking place, and the attackers may have already done serious damage to the company's system, making recovery a lengthy process. The development of a strong firewall and connecting all operating systems to a private network could help reduce the risk of the company's vulnerability to cyber threats.

Sources

Edwards, J. (2021, February 9). *Someone is trying to take entire countries offline and cybersecurity experts say "it's a matter of time because it's really easy."* Business Insider. https://www.businessinsider.com/can-hackers-take-entire-countries-offline-2018-12

Google. (n.d.). *Cyberbitsetc - why is cyber security about human behavior?*. Google Docs. https://docs.google.com/document/d/1QplIrfcKlmkSOuKt9i0Kte72kYrukFeCm1wj9DxpnGU/edit?tab=t.0#

Kosinski, M. (2024, December 2). *Authentication vs. authorization: What's the difference?* IBM. https://www.ibm.com/think/topics/authentication-vs-authorization

SCADA systems - SCADA systems. (2018, July 25).

https://www.scadasystems.net/