ISEC-615 - Fundamentals of Cybersecurity

Cybersecurity Principles Assignment No. 1.

Due: 6/2/2019

Eric Webb

[ew774@mynsu.nova.edu](mailto:ew774@mynsu.nova.edu)

Dr. Yair Levy

Cybersecurity Definitions…………………………………………………………..3

Principals of Cybersecurity…………………………………………………………4

Overall Security………………………………………………………………….....5

Secured Operations………………………………………………………………....6

Conclusion………………………………………………………………………….7

Work Cited……………………………………………………………………….....8

Certificate of Authorship……………………………………………………………9

As the world continues to advance into the Digital Era the topic of cybersecurity becomes a more prevalent force. Now-a-days cybersecurity threats are an ever increasing risk for Government, Business, and for the consumer. Every day malicious forces are trying to adapt and overcome these cybersecurity defenses for either financial or political gain. But, what is cybersecurity?

The [National Initiative for Cybersecurity Careers and Studies](https://niccs.us-cert.gov/) defines cybersecurity as **“**The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.”(Niccs Glossary, 2019). Cybersecurity is a pretty unanimous term across all regions and are neighbors to the east in the United Kingdom define Cybersecurity as “a subset of information security. It specifically focuses on protecting computer systems and their components – including hardware, software and data – and digital infrastructure from attack, unauthorized access or being otherwise damaged or made inaccessible. Data centers, websites, programs, servers, or accounts can all be exploited through a cyber-attack.”(ItGovernanceUK, 2019). As from government entities to the corporate sector, the term cybersecurity also has it commercial definitions on what cybersecurity needs to be. Paloalto networks defines cybersecurity as “a set of techniques used to protect the integrity cyber networks, programs and data from attack, damage or unauthorized access.”(What is Cybersecurity? , 2019.)

Across the board cybersecurity seems to be in basic line of protecting networks and hardware from malicious forces and implementing guidelines to help offset these attacks.

In Cybersecurity there is the basic principles of CIA, confidentiality, integrity, and availability. These principles all intertwine and directly correlate all with each other. To introduce the relationships between these principles we must first understand what each of them mean. To begin, Portland based Software Company Tripwire describes confidentiality as “The correct level of access should be given to only those people and processes that need it to complete their duties. If no access is required then none should be given.” (EdonNov, P. 2015). Essentially, nobody should be able to see what they have no business in. That brings us to the concept of integrity, IT education platform Techopedia states that integrity is “This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.” (Staff, T. 2017.) For example if you and a colleague both request the same document from an internal resource, but both get back different documents. How would you know which is the correct document? Integrity solves this issue. Lastly this brings us to availability, it has been said that availability is “data that can be accessed when needed. A problem such as a hardware failure or a hacking attack might prevent access to data. Security professionals must have solutions to ensure data can be accessed when a problem such as one of these occurs. ” (Lavendaer, L. 2019 pg47) . For instance, if you have access to important data through a server and that server goes down how else would that important data be available? That is why you need to take into account how available information can be.

As you can see all three definitions of the security triad CIA have their own respective components to each forming the whole triad. Confidentiality, keep things on a need to know basis. Integrity, makes sure information has not been changed incorrectly. While Availability brings to the question, how can you access this and what ways?

Earlier we discussed the text book definitions of CIA, but now let’s discuss how these fundamental concepts are used to provide system security.

To begin Confidentiality allows data to be sent and seen by only those who are on a need to know basis. Only those who are meant to see the document or data will have access to it. You do not want unauthorized users to access your data. Some practical ways to enforce confidentiality are Unix file permissions. (Such as chmod/chown) and Access Control Lists to limit users permissions. You can also use encryption to hide data that has been compromised and will need a key to decrypt it. This adds another layer security to confidentiality.

Integrity is more of a guarantee that your information / data is correct without being tampered with and if it has been changed then a digital footprint is established for accounting. A better example would be if two doctors looked up the cure for a disease on the central online library and both search results produced a different set of instructions for the cure. Which would be the correct answer? Integrity can provide confidence that a result set has not been changed by using hashing algorithms. You can use a hashing algorithm (Such as Sha-1 or md5sum) to establish a digital fingerprint so that if you run the exact copy of the file/data through the same algorithm you will get that same digital fingerprint. Even as much as adding few spaces or periods will provide a completely different outcome.

Availability brings to question data redundancy along with how permissions will affect the efficiency of the environment. If something goes wrong can members still access the data a second way? If you set to many permission controls, work starts to get redundant and inefficient for the everyday worker. How can we keep things efficient and stream line while maintaining a well-balanced security posture? That is what availability brings into question.

In this section we will go into detail on how the CIA triad allows for the development of security mechanisms that can implement desired security policies in organizations

For Confidentiality we typically have the case that hackers are always trying to get access to what is intended to be classified data. Because of this organizations typically have good implementation of security policies involving access control lists and other policies to better enforce data on a need to know basis.

Integrity is important because you want to make sure your data does not contain any malicious content or has been changed for nefarious reasons. Because of this hashing has been developed to verify data hasn’t been altered. Such policies like creating digital signatures before a restore or when first recovering data from a crime scene have been implemented.

In the case of importance on availability, we need data to be redundant but also secure. Because of this, organizations might implement policies about disaster recovery plans and data redundancy fail safes.

From this we can see how the CIA triad aids to security and has helped develop concepts that lead to stronger implementation of security policies.

As you can see this document focused on the definitions of cybersecurity along with the CIA triad.From this we now can grasp that cybersecurity is the concept of keeping your digital assets secure electronically and physically from malicious intent.

We now know the definitions of Confidentiality, Integrity, and Availability.

We also know how they provide overall security along with how these concepts have led to the development of more strategic security policies.

To conclude, Cybersecurity and the CIA triad are very important terms and concepts that have deep impacts on security. It is important to remember the role of all these in maintaining a strong security posture.

EdonNov, P. (2015, November 30). The Three Principles of a Secure System. Retrieved May 19, 2019, from <https://www.tripwire.com/state-of-security/security-awareness/the-three-principles-of-a-secure-system/>

ItGovernanceUK (n.d.). Retrieved May 19, 2019, from <https://www.itgovernance.co.uk/what-is-cybersecurity>

LAVENDER, L. (2018). *PRINCIPLES OF CYBERSECURITY*[1st]. Retrieved May 19, 2019, from <https://www.g-wonlinetextbooks.com/principles-of-cybersecurity-2020/47>

Niccs Glossary. (n.d.). Retrieved May 19, 2019, from <https://niccs.us-cert.gov/about-niccs/glossary#C>

Staff, T. (2017, May 19). The 7 Basic Principles of IT Security. Retrieved May 19, 2019, from <https://www.techopedia.com/2/27825/security/the-basic-principles-of-it-security>

WHAT IS CYBERSECURITY? Palo Aloto Networks (n.d.). Retrieved May 19, 2019, from <https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security>



Certification of Authorship of Assignment

Submitted to: Professor Yair Levy.

Student’s Name: Eric Webb

Date of Assignment: 6/2/2019

Title of Assignment: Assignment 1 - Cybersecurity Principles

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this course.

Student's Signature: ERIC WEBB