**ISEC-615 - Fundamentals of Cybersecurity**

**Cybersecurity Principles Assignment No. 1.**

**Eric Webb**

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

Dr. Yair Levy

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 is. 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 Paloalto, 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 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, 2105). 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?

In your own words (no quotes, but use references), describe how each of the fundamental concepts of the cybersecurity discipline is used to provide overall system security

**:** In your own words (no quotes, but use references), describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies in organizations

**:** In your own words (no quotes, but use references), provide a conclusion that summarises the whole paper.

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/

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

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

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

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

What is Cyber Security? (n.d.). Retrieved May 19, 2019, from https://www.itgovernance.co.uk/what-is-cybersecurity