Introduction to Security

Gregorio Marrero

[Institutional Affiliation(s)]

Author Note

Defense in Depth and Threats to INFOSEC

Defense in Depth and INFOSEC

Defense in Depth is an emerging concept in the world of cybersecurity. It is about the placement of a series of defensive mechanisms that placed in layers to protect important data or information (Kakareka, 2013). This method of cybersecurity is often equated with the art of “Castle Defense”, as it is just like the security mechanisms of a medieval castle, where the battery of assault needed to go through a series of walls, draw bridges, keep and numerous other defenses to win the battle. This is very important as no organization can protect its IT systems by a single layer of security. There are always backdoors in the system that are found by the hackers and exploited for their malicious aims. There are different components of the placing Defense in Depth mechanism in your workplaces. Some of the common elements of the Defense in Depth are Network Security via traffic controlling mechanism such as firewalls, installation of Antivirus Software that is used on individual work stations, analysis of data integrity for marking suspicious files and Behavior Analysis that is used to halt data breaches that are in progress.

This Defense in Depth is of great importance, especially during the contemporary threats to Information Security (INFOSEC), that are growing with the progress of time. Cybercriminals are discovering new ways every day to hack the most complex and sensitive networks in the world, especially after the invention of the Dark Net, which has made this easier than ever before. Many cybercriminals used social media to describe complex "water holing" attacks that infect all the websites the victim visits in his browsing sessions. Some of the emerging threats to INFOSEC are Mobile Malware, Third-party entry points, Outdated Security Software (mostly antiviruses), Social Engineering and inadequate security technology that are often employed by companies to cut costs related to the much-ignored threat of cyberattacks (Ledesma, 2019).

# References

Kakareka, A. (2013). What Is Vulnerability Assessment? *Computer and Information Security Handbook (Third Edition)*, 483-494. DOI:10.1016/B978-0-12-803843-7.00031-4

Ledesma, J. (2019, February 07). Cybersecurity Threat Trends: What Should Be On Your Radar Part 2. *MIS Training Institute*. Retrieved from https://misti.com/infosec-insider/2019-cybersecurity-threat-trends-what-should-be-on-your-radar-part-2