Dylan Coulter January 19, 2025

[Dylan.coulter@snhu.edu](mailto:Dylan.coulter@snhu.edu)

ID# 1896062

CS405

**Assignment 2-1 Defense in Depth Activity**

**How deep is too deep, and what’s the tradeoff?**

When considering Defense in Depth (DiD) and what may be too deep we need to understand that it is a cybersecurity approach that is focused on building layers of security controls to protect data, networks and systems from attacks. It can be a challenge to find what may be too many layers and not having enough can allow for attackers to exploit and find vulnerabilities. More layers mean more complexity making it harder for attackers to find a way to breach the system. More layers also mean more cost and time which may not be a big deal to some depending on what they are protecting, but to others the amount of layers can be much and unnecessary. In the end it is important to understand what we are trying to protect to understand what can be considered too deep.

**What are some time, money, reputation, and operational considerations?**

Implementing Defense in Depth will involve several considerations which would include the amount of time and money, and the reputation and operational impact. When multiple layers are implemented, it can be very time-consuming and is especially true as the systems become more complex and involve a lot of configuring and maintenance to keep everything secure. An attack on a company that causes a large data breach can have a major impact on that company’s reputation. In the past we have seen companies’ stock collapse after a data breach. On the other hand, a company with strong security measures will have a stronger reputation especially if they are handling extremely sensitive data. Another area that would need to be looked at is the financial impact a more complex system may have. Just like with a lot of this the more complex something is the more it will cost to keep it operating and up to date.

**What are some additional aspects of DiD that make it unique for each situation?**

Defense in Depth has aspects that make it unique in each situation because it can be adapted to many different situations such as certain threats, needs and vulnerabilities of the organization. The Defense in Depth strategy will be influenced by many different factors and some of these include budget, type of data that is being protected, and the industry to name a few. A hospital or health care organization would have different needs of security than a financial institution in some cases as they may have different forms of regulations such as a health care organization would need to comply with HIPPA. It is important to understand the potential for attacks and the risks faced to allow for the proper adjustment to how we implement Defense in Depth.