**Module Two Journal – Defense in Depth**

Joseph Veneski

Department of Computer Science, Southern New Hampshire University

CS-405 Secure Coding

Professor Kaan Esendemir

March 17, 2024

**Module Two Journal – Defense in Depth**

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

Defense in Depth (DiD) strategies will vary by situation. There is a tradeoff between increasing security by adding additional complexity and decreasing usability and increasing costs. Considering embedded devices where resources are limited, more complex Defense in Depth strategies may not be feasible. The value of assets being protected must be considered and weighed against the costs of more complex defense strategies. The key is finding a balance between mitigating security risks without excessively burdening the system, organization, or stakeholders.

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

Implementing and maintaining a DiD strategy can be time-consuming. Each layer requires planning, implementation, and maintenance. The more layers of security there are, the more hindrance to user access there will be. Each of these layers has a monetary cost as well in the form of technology, equipment, paying personnel. Skilled security professionals may be required as security becomes more complex, which will significantly raise costs (Korolov, 2015).

An investment in a well-implemented DiD strategy can be a benefit to a company’s reputation by demonstrating a commitment to security. Again, the more complex the strategy and implementation becomes, the more of a hindrance it becomes for user experience. A very slow unresponsive system that is bogged down by security overkill can bring diminishing returns on security versus productivity.

It is important to account for scalability in DiD strategies as organizations grow. Frequent security audits and risk assessments should be used to maintain and improve security. Additionally, incorporating a security mindset and security training for personnel can have a significant impact on risk mitigation. A security strategy is only effective if properly utilized. A disaster recovery strategy and its testing is also part of DiD which can help in mitigating potential cost and reputation damages (“What is Cybersecurity Risk? Definition & Factors to Consider in 2024”, 2024).

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

Other considerations for DiD strategies include the potential risk for an organization, possible regulations, asset value to be protected, and technology environment utilized. There is inherently less risk for small businesses compared to multimillion dollar companies and the defense measures should reflect that. Some organizations will need to adhere to regulatory requirements often due to the risk profile and nature of data being handled which will naturally require more complex DiD to remain in compliance (Miller, 2023). The technology environment will also dictate the level of DiD that can be implemented, such as with embedded devices which generally have power and memory constraints.

**References**

Korolov, M. (2015). *The Dark Side of Layered Security*. CSO. <https://www.csoonline.com/article/553599/the-dark-side-of-layered-security.html>

Miller, J. (2023). *Cyber Compliance 101 – What It Is and Why It’s Needed.* Indiana Cybersecurity Hub. <https://www.in.gov/cybersecurity/blog/posts/cyber-compliance-101-what-it-is-and-why-its-needed/>

*What is Cybersecurity Risk? Definition & Factors to Consider in 2024*. (2024). SecurityScorecard. <https://securityscorecard.com/blog/what-is-cybersecurity-risk-factors-to-consider/>