**EMCS2600: The Future of Cybersecurity: Technology and Policy**

Assignment: Module 5 Review Questions

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

Question 1: From the Defense in Depth System Security Model readings identify the two topics you consider most important and briefly say why you have chosen them (in at most 200 words).

The provocative revelation that I uncovered after reading through Defense in Depth Security Model is how it’s origins as a single solution for specific problems are a set up for future problems. There is no question that layers of defense are necessary. Prevention, Detection, and Response are critical functions of security. Furthermore, the depth of each of these functions in incredibly important to the potency of the defense. What is more important in my opinion is how these functions inform one another. For example, a SIEM doing log analysis without critical information on what devices are ***supposed*** to be on the network is pretty pointless. A SOC being inundated alerts from a SIEM with no way to formulate an automated response is equally as useless. The truth is that many organizations try to buy assurance by adding a line item in the budget for each of the layers in DID, but that doesn’t work. Defense in Depth works better when the context is shared through the layers of defense and the response in automated so security becomes more real-time rather than relying on humans that may be limited by schedules and workloads.

Question 2: Explain in a few words your views on the importance of zero-trust security and site reliability engineering using the readings on these subjects (in at most 200 words).

A comment from an anonymous YouTuber on the creator of Zero-Trust John Kindervag’s video said, “Government and military have been building IT this way, segmenting networks and building systems around information security levels for many many years ... finally, the IT-industry has also "invented" it and found a buzz word for it.” As a builder and user of government and military communications software, I must agree with the commenter. In a forwarding base, sometimes in the theater of war, “zero-trust” means taking the extra steps to normalize and mandate secure networking protocols, enforcing fine-grain access controls and logging and inspecting all network activity. For government and military IT professionals, only securing the perimeter could cost lives. Silicon Valley packaged this approach and made it into an appliance, which is useful as a way of transitioning away from tiered network structure but also trivializes the concepts of trust and verification by making it into a product. Site reliability engineering if approached as a practice cannot be limited by one concept. Our concepts around trust and verification must continue to evolve and organizations must remain responsive to the threat landscape by resisting the urge to get too comfortable in any one defense strategy.