Atticus Emilsson

CYSE 368

Cybersecurity Internship

February 25, 2025

Reflective Journal #3

This reflective journal marks the third 50-hour period of work I have completed under the context of the CYSE368 Cybersecurity Internship course. The focus of this segment of time has shifted heavily when compared to my previous reflective journals. This period of work has been incredibly hands-on with with products/services such as Windows, BitLocker, Active Directory, and everything in between.

I was recently granted increased administrative privileges, inherently broadening the scope of work in my capacity. This has included a lot of troubleshooting relating to Windows and the relevant system's security. Many of the corresponding systems are constituents of an Active Directory domain, which had advantages and disadvantages. I had taken courses on Active Directory in the past; however, they were not particularly hands on so much of the information was merely theoretical or abstract. In this instance, I was thrown into the deep-end where I had to act accordingly. Of course, no changes were made without a second opinion considering my relatively basic experience with AD; however, I learned a huge amount relating to AD access and security controls.

I have also gained more experience with BitLocker enabled devices, as I have handled quite a few this past 50-hours. Handling BitLocker identification and recovery keys opened my eyes to the complexities that exist in terms of the secure storage of large quantities of information of this nature.

This issue is a great example for considering the CIA (Confidentiality, Integrity, Availability) triad. This information must not reach the hands of the wrong parties, as this would threaten the confidentiality of the user's data. The integrity must be maintained in order to ensure that the encrypted contents or necessary keys are not corrupted. Availability must be considered for cases where troubleshooting and repairs must be carried out. Failure to consider proper availability when developing a solution for securing this information can interfere company operations on both ends.

Another recently encountered issue that requires consideration of the CIA triad is disaster recovery and business continuity. During this 50-hour period, my employers requested that I attend a class for these concepts. In the class which I attended on February 25, 2025, I learned how to implement backup and recovery solutions which enable entire systems/servers and/or specific data/services to be recovered with ease.

In summation, I have found this 50-hour segment of work under the context of the CYSE368 Cybersecurity Internship course to be incredibly valuable towards both my education and career. These issues highlighted areas in which I can improve, both internally (education, analysis, etc) and externally (administration, operations, etc).