Joshua Russell
CYSE 368
Teresa Duvall

CM Technology and the Finer Details

Reflection #3

Currently, we are in the research and development phase of our internship which is incredible complex and strenuous. In the third set of 50 hours, we have devoted all our time to communicating with organization leaders John Beahm and Frank Rose, assessing the concerns of CM Technology, and formulating strategies for cybersecurity compliance. This is research intensive and requires in-depth analysis of the frameworks to provide CM Technology with the best possible recommendations that meet their needs, and the requirements desired.

In this phase, we are implementing NIST CSF 2.0, NIST CSF Small Business Guide, and NIST 800-171 Cybersecurity Maturity Model Certification (CMMC) to assess CM Technology and their cybersecurity postures. These frameworks provide a roadmap that allows us to analyze current business practices regarding cybersecurity and create an action plan to address needs conveyed by the organization. The crucial issues CM Technology possesses are having a lack of clear employee training and awareness programs, increased attack vectors, threats with malicious intent, and a goal of becoming CMMC compliant to obtain Department of Defense (DoD) contracts in the satellite communications (SATCOM) industry. In addition, CM Technology has goals of establishing a continuity of operations plan (COOP), an incident response plan (IRP), and methods of deploying new cybersecurity tools and services. This can be a massive undertaking, but the frameworks outline guidance as to how to accomplish these tasks.

Joshua Russell
CYSE 368
Teresa Duvall

This portion of the internship also demands extensive teamwork and leadership because work is becoming increasingly detail driven. Everyone has a role to play, and all roles are important to the overall mission. As the research lead, my job is to analyze answers from the Valor Top 10 Cybersecurity Checklist and the Client Intake Questionnaire I created, consolidate the data collected, and research methods, services, and tools to help CM Technology become successful in their cybersecurity efforts. At this stage, it is imperative that communication is clear, feedback is constructive, and all members of the team feel that their contributions are making a difference.

Overall, I feel confident that we will provide CM Technology with recommendations that will exceed their expectations. Through use of the NIST frameworks and exhaustive research, a continuity of operations plan, an incident response plan, and employee training and awareness plan will be developed. It has been incredibly enjoyable working as a team to address the concerns and needs associated with CM Technology; it is a complex organization that requires collaboration, communication, problem solving, and critical thinking. This internship clinic has been very insightful in providing me experience as to what I will be dealing with in my future cybersecurity career.