Final Reflection

Amari Fisher
CYSE 368
Old Dominion University
12/14/2025

Final Reflection

After completing the cybersecurity internship at COVA CCI, I have gained the opportunity to apply the knowledge I have been developing over the past 3 years in a real-world context. Over the past four months, I have gained practical experience with tools such as Tenable and developed soft skills, including public speaking. Prior to this internship, I was under the impression that cybersecurity was mostly technical, although I had previously taken courses that emphasized its ethical importance. Being able to experience the importance of ethics through the sessions provided by Dr. Baki helped me better conceptualize its role in cybersecurity. Dr. Baki's sessions also helped me not overthink, as they focused on helping students get out of their comfort zones.

What Went Right, What Went Wrong, and Lessons Learned

Overall, the internship experience provided through the COVA CCI Cybersecurity internship program was highly beneficial and successful in translating classroom knowledge into practical, real-world cybersecurity practice. One of the aspects that went very well was the opportunity to work with enterprise-level tools like Tenable and to apply structured cybersecurity frameworks to a public sector organization. This allowed me to develop a better understanding of how cybersecurity decisions are made within compliance-driven organizations. One challenge I experienced during the internship was balancing technical analysis with documentation or presentation requirements. This aspect was especially difficult because I usually write a lot during the presentation, then read directly from the screen, but we were required to shorten the presentations to ensure we were actually conceptualizing the knowledge and able to present it without the screen. A major personal lesson learned was that cybersecurity is not purely technical. While technical assessments are critical, ethical considerations and governance also play an equally important role. The ethics-focused sessions led by Dr. Baki helped reinforce this understanding and encouraged professional growth by pushing students beyond their comfort zones. Additionally, I learned how to map important information into presentable questions from both Valor Cybersecurity & the CISA CPG.

Valor Importance

Mr. Tomchick primarily provided a checklist, which allowed me to better understand how to map important frameworks like NIST CSF to presentable questions to present to organizations and gain a better understanding of their current cybersecurity posture and capabilities. His top 10 checklist was an excellent tool to utilize to visualize the City of Suffolk's overall cybersecurity readiness and provided practical assistance when creating our final report.

CISA CPG

The CPG seems like an excellent tool that also maps important frameworks to presentable questions for employers, but it wasn't given as much importance as Valor and its checklist. I personally would have loved to have had more experience with the CPG apart from the NIST & CPG checklist because the tool contained vast amounts of relevant questions and information that could be asked to establish focus on certain key areas. We didn't utilize the CPG in our final reports, primarily because our focus was less on the overall cybersecurity readiness of Suffolk, but on the compliance and security of their specific database servers.

Fulfillment of Memorandum of Agreement Learning Objectives

1. Practical Application of Classroom Knowledge

This objective was strongly fulfilled. I utilized knowledge gained from the classroom regarding cybersecurity frameworks when conducting our overall cybersecurity assessment of the City of Suffolk and when conducting the compliance scans on their SQL server environment.

2. Collaboration and Communication in a team environment\

This objective was fully met. I was assigned to team B, and Mr. Cox, and the Suffolk leadership assigned us to one of their SQL database servers. My group members were excellent, and we never had any arguments or big disagreements. Whenever we considered doing something differently, either in the report or in the presentations, we would first notify each other of how it could be done better, and then make the final changes/decision once the improvements were agreed upon. We met in person and via Zoom several times before our major presentations. Overall, an excellent team experience, and I loved working with both Andy and Erik.

3. Exposure to Cyber Threat Intelligence

This objective was partially fulfilled because the internship primarily focused more on vulnerability management and compliance fulfillment; however, indirect exposure was experienced through analyzing the vulnerabilities presented by our scans on the city of Suffolk.

4. Understanding of Industries Best Practices

This objective was completely fulfilled. The internship emphasized the importance of best practices through the utilization of frameworks like NIST, CPG, and the Valor Cybersecurity checklist. These resources allowed me to translate standards into presentable questions.

5. Research and Innovative Cybersecurity Solutions

This objective was fulfilled, but the internship focused more on compliance and assessment; the overall process of identifying vulnerabilities and improvement areas required critical thinking, and the research into secure mitigation strategies/techniques.

Most Motivating/Challenging Aspects

The most motivating aspect of the internship was the experience of working with a city government and contributing to cybersecurity assessments that have real-world implications. Knowing that our work could be used to influence governing decisions within the city made the experience meaningful. The most challenging aspect of the internship was the executive portion of the final report because it required balancing technical findings with the need to communicate clear risks to executive leadership and non-technical stakeholders. This required learning how to translate complex technical information into clear, actionable, and understandable insights.

Internship Suggestions

As showcased in *Valor Importance*, Valor Cybersecurity is the established partner of the internship. I would love some focus on the CISA CPG, as it contains much more information, all pertinent to different aspects of cybersecurity. Additionally, I believe that if we had been given time to meet with our clients earlier, we would have gained a better understanding of exactly what the organization wants from the students. It would be great if there were also an established communication method and a timeframe for how often we should communicate with clients to prevent any clients from having issues with group communication.

Conclusion

My primary takeaway from this internship was the realization that effective cybersecurity requires the balancing of technical prowess, ethical considerations, governance awareness, and effective communication. Working with the city also highlighted the importance of policy-making when implementing clear cybersecurity solutions. This experience will influence the remainder of my time here at Old Dominion University by steering my future coursework toward more policy making, while continuing to foster my technical knowledge through a minor in information systems and technology. It was a valuable opportunity that any student should strive to apply for and participate in. Professionally, the internship has steered my focus on cybersecurity toward a governmental role in the public sector, or for the government in general due to its focus on critical aspects of the nation and heavy emphasis on technical and policy-making ability. I believe that the course was created exceptionally well, with distinct minds behind the introduction of the course. I listed some key recommendations in the above section, and believe that most other things should stay the same. Thank you for this opportunity!