Asher Embry

CYSE 368 – Cybersecurity Clinic

Spring 2026

Professor Teresa Duvall

TA Jade Hines and Carla Belfiore

Final Reflection Paper

Introduction

The COVA CCI Cyber Clinic serves as a way for ODU students to provide cybersecurity assistance to local small businesses and nonprofit organizations. I had the pleasure of working with the Boys and Girls Clubs of Southeast Virginia (BGCSEVA), a nonprofit youth-serving organization. Over the course of the Spring 2026 semester, I learned about industry standards, design thinking, professional relationships, and many other skills.

What Went Well

Overall, most of the lessons taught before meeting our client went well, as well as the entire experience working with BGCSEVA. From the start of the course, we got lessons on how to think creatively, industry cybersecurity frameworks, and other strategies for performing a cybersecurity assessment for our clients. I especially enjoyed the design thinking sessions from Dr. Baaki, they were quite strange and atypical for a lesson in a cybersecurity course, but they taught us how to think outside the box and build upon other's ideas to create a better result. The lessons also taught the class as a group that we have to actively work together to produce a good product rather than let others do the heavy lifting.

The other instructional sessions like learning the NIST Cybersecurity Framework and the CISA Cybersecurity Performance Goals featured guest speakers and different locations around campus and in Norfolk. I really liked this aspect of the course where we got to learn topics from experts in their field rather than be given a boring PowerPoint lecture like in previous courses I have taken.

The whole process of meeting and working with our client and team also went great. Isaiah and Ryan were my group mates, and we worked well together to get our final products done and meet the appropriate deadlines. Barring a few minor mishaps (the 'WELCOME' sign saying 'MELCOME'), there were no issues with our client. We conducted our meetings with Ken Lamay, the Director of Administration for BGCSEVA. Their primary concern was setting up content filtering for club members and preparing for unknown cybersecurity standards upcoming from the national organization. Most of their IT equipment and systems are managed by a local MSP, Mode 5. From talking with other groups in the Cyber Clinic, this was an atypical scenario, where most other clients were starting from minimal digital protections and practices in place and groups could provide a comprehensive list of what to improve and how to do so.

In our client meetings my group worked well together to ask clarifying questions with Mr. Lamay and develop ideas to better improve BGCSEVA's cyber posture for the final report and presentation. We worked well together drafting the report and presentation to recommend the following to BGCSEVA;

- Securely store physical PHI documents at club locations
- Manually configure ISP content filtering
- Implement routine staff training on cybersecurity best practices

- Implement a cybersecurity incident response plan

Our final presentation went great and was well received by Mr. Lamay. It was a great culmination of the semester's work, and the whole team was glad that it was completed. I appreciated the time to do dry runs of the presentation so we could get better practice with presenting and to refine the content of the presentation itself.

What Could Have Gone Better

Other than a terrorist attack on campus right before spring break, there were not many things that went poorly over the course of this internship. I think the only part of the course that I felt could use some improvements was the sessions with Valor Security and "hitting the streets." The idea of the sessions with Valor and Greg Tomchick were great, to get us thinking about cybersecurity assessments, what we want to do in our career, and doing a few short assessments as well. However, I feel like there was not as much actually gained by the students as there could have been. In those sessions, it seemed like Mr. Tomchick was more interested in giving us some statistics and promoting Valor's *Legacy in Cyber Program* and other services for businesses. It felt like we were being given a marketing pitch for Valor to be salespeople for the company and their services when we hit the streets.

As a group, the hitting the streets activity had a mixed reaction. It is a great idea to have students go out and ask local businesses about their cybersecurity practices to get them thinking about cybersecurity and making sure that they are secure. I am used to meeting and conversing with new people, but I did not enjoy this experience. It was an odd feeling walking into a business as a random college student asking about cybersecurity and being met with a similar reaction to someone selling gutter cleaning services. For how much this segment of the class was

talked about and hyped up, I did not enjoy it. Afterwards, it seemed like the assessments completed with local businesses were forgotten about until after the client presentations were done. We took the scores from businesses and compiled their weaknesses into a report document to deliver to them. At time of writing, we have not received printed reports to deliver to businesses. The core idea of the sessions with Valor was helpful, but it felt like Valor gained more from the experience than the students did.

Lessons Learned

Many of the lessons I learned over the course of this internship were soft skills like conducting business meetings, and thinking creatively with others to solve cybersecurity problems, among other skills. Over the years I have learned some of these skills in other ways, but it was helpful to put them to use in an academic setting. I appreciated a course where the atmosphere was relaxed and all the students were highly motivated and knowledgeable in the field of cybersecurity. Perhaps the newest skill I learned was acting in the role of a consultant for a client, something I had some experience with in being the client, but it was helpful to experience the other side of that relationship.

Course Recommendations

As mentioned above, I think my biggest friction point of this course was with Valor Cybersecurity. I think the best way to improve the course when working with Valor is to have lessons that better explain the importance of a cybersecurity assessment and provide immediate results for companies when we ‘hit the streets.’ It would be helpful to teach how to interpret results from the assessments done with the *Top 10 Checklist* and translate them to policy recommendations.

Another recommendation for the course is to include a tentative schedule for the course in the syllabus and use Docusign or onboarding forms formatted to use digital signatures to make the onboarding for the course easier. To better prepare the students for giving their presentation and public speaking in general, it would be helpful to include a 10–15-minute lesson with good tips for public speaking like to face the audience and not the screen, speak with your diaphragm, have confident body language, etc.

Conclusion

Overall, I enjoyed the Cyber Clinic program. I think that its current state is very well defined in the goal and purpose of the program both for the students and for the client organizations. While there are some aspects that could use some improvement, the professors and TAs running the program are very passionate about making sure that everything goes as smoothly as possible and continuing to improve every semester. I think this experience with the Cyber Clinic will spoil me in the sense of having high performing classmates as well as instructors motivating me to do well in my last semesters at ODU. In my professional career, this experience will help me to better understand working in a corporate environment to be able to explain complex technical concepts to a managerial audience.