Brayden Greenfield

Professor Duvall

CYSE 368

08 December 2024

Individual Reflection

1. basic theories and practices of digital security

With the City of Suffolk, I was able to apply cybersecurity practices. I was able to learn more about vulnerability management and compliance management. Furthermore, I could see and recommend changes that were easy to implement, and then I could research the hard-to-implement compliance settings. Tenable made it easy to read. However, you must still research the settings and understand what would affect the machine. **So we fulfilled this goal**

2. discuss the intricacies of protecting largely under-resourced organizations

I would say the city was not under-resourced in terms of software. It was more of a staffing issue. They only have one person full-time for cybersecurity. This puts a lot of pressure on Mr. Joshua Cox. Furthermore, it takes a lot of time to implement the changes. We got to see a little bit of change management for the systems. They require a lot of turnaround time. In addition, they were not meeting their service level agreements and are trying to become more compliant with their agreements. **We fulfilled this goal.**

3. the tools needed to address/manage risk. In the clinic component

We had a couple of issues with Tenable that caused slowdowns. We could not scan for about two weeks, which put us way behind schedule. Tenable did everything we needed to address and manage the City of Suffolk risk. **We fulfilled this goal.**

4. students will work in teams supervised by the Clinic staff to provide direct

cybersecurity assistance to small businesses/organizations in Hampton Roads

We did not fulfill this goal because the city is a larger organization. We did provide direct cybersecurity assistance to the organization, but as stated above. They are not a small business. If that does not matter, then we fulfilled this goal.

5. Students' clinic responsibilities will include learning about an business/organization's mission and context, assessing its vulnerabilities, and ultimately recommending and implementing mitigations to the identified security Risks.

We fulfilled this requirement. I learned how to use Tenable, read Tenable outputs, apply my understanding of compliance, and assess vulnerabilities. I did not do much assessing vulnerabilities because it was not my part of the project. I focused more on the compliance settings. I was able to research and learn more about compliance and recommend mitigations to their identified security risks.

Describe the most motivating or exciting aspects of the internship. Describe the most challenging aspects of the internship.

The most motivating and exciting aspect of the internship was using Tenable. I loved how easy it was to navigate the UI and get the data. It explained everything and allowed me to easily research what would be easier to implement and which would be hard to implement. Then, being able to easily see how they compared to CIS standards was very cool.

The most challenging aspect was getting Tenable to work. It took about two weeks to get our required scans, which definitely put us on our back foot for a little while and made more things feel rushed and unfinished. However, after the speech and hearing all the great feedback, I realized that even though we had to rush, we did great under pressure.

List your recommendations for future interns in this internship. What preparations do interns need before starting the internship?

There are a lot of recommendations. First, the valor top 10 feels like we are trying to sell his product to others. Going out for the first time was a great experience because we could see how we and others do under pressure, but any more time for our group felt like a waste.

I like the Dr. B getting out of your mind drills. They were different and fun to do. I would recommend bringing him back and having the future interns do them. They show how we think too much and how it stops us from getting to the answer.

My next recommendation is to meet with the clients a little earlier to allow for more dry runs.

Another recommendation is to have more dry runs, at least two because the first one will have the most mistakes. The next one will show the group's improvement. This would allow for more of them to get feedback and improve on the feedback because we only had one dry run, and it was finished two hours before we did it.

My fourth recommendation is to have clearly documented assignments because I got lost on a couple of assignments and did not really understand what they were. Like this one, clearly put the five learning objectives on the assignment. This makes it easier for us to understand what is required for the assignment and allows them to copy and paste an outline into a document and answer the questions in order.

Finally, interns need to have a basic understanding of cybersecurity terminology before they start. If they don't, they will be even more behind. That is my only recommendation for future intern preparation.

Conclusion:

Overall, the internship was a great experience. My key takeaways are learning vulnerabilities and compliance management. That was an enjoyable and valuable experience. This internship has allowed me to get more interviews and another internship. Moreover, I have been getting a father in the hiring process because of this internship. I hear a lot more from different companies. I am also looking at getting a full-time job soon because I have recommended that, with all this experience, I apply for full-time positions. It will influence my remaining college time by allowing me to use my newfound knowledge in other classes I will take next semester and the following semester. I put a lot of recommendations above and want to avoid relisting all of them and bloating the conclusion. There are a lot of changes, but this program can only get better each cycle. Thank you for reading, and happy holidays.