Rebecca Hight
CYSE 368
Individual Reflection
December 8, 2024

# Reflection on the Risk Assessment for the City of Suffolk's SQL Database

## Introduction

The COVA CCI cybersecurity internship provided me with a unique opportunity to apply academic knowledge in a practical setting. As a member of Suffolk Team B, our project focused on conducting a risk assessment of an SQL server for the City of Suffolk using Tenable.io. This paper reflects on the project's outcomes, lessons learned, and its impact on my academic and professional growth.

## Successes and Accomplishments

One of the most significant accomplishments was the successful use of Tenable.io to conduct vulnerability scans. With guidance from our Clients, mainly, Suffolk's Senior Cybersecurity Administrator, Joshua Cox and Suffolk's Special Project Manager, Neal Miller, we identified 208 vulnerabilities within the SQL server, prioritized those vulnerabilities, and provided actionable recommendations. Another success was the clear and comprehensive deliverables, including a detailed report, a Microsoft Excel Compliance Audit, and a comprehensive Microsoft Excel Risk Assessment Findings, prioritizing all vulnerabilities and their remediations.

Collaboration played a critical role in the project's success. Effective communication with Suffolk's IT department ensured that our findings were not just actionable remediations, but

also accurate. Additionally, creating and delivering a professional PowerPoint presentation allowed our team to demonstrate our understanding of cybersecurity concepts to a non-technical audience and our Client in an executive format. This experience highlighted the importance of translating technical data into clear and concise insights for our Client and audience.

**Challenges Encountered**

Despite these successes, this project presented several challenges. Managing the complexity of 208 identified vulnerabilities required significant effort to prioritize and contextualize them. Balancing this technical analysis with project deadlines and other responsibilities was also demanding. Furthermore, the initial scope of the project lacked clarity, leading to adjustments and refinements as the work progressed. To overcome this challenge, our team held meetings with our client for clarification and maintained consistent communication through text messages. These challenges highlight the importance of clearly defining project boundaries early on and having effective time management skills.

**Lessons Learned**

Overall, the internship project with the City of Suffolk emphasized the importance of communication, prioritization, and adaptability in cybersecurity projects. Regular updates to our client and a focus on clear communication via email and scheduled Team's meetings were essential in maintaining alignment with project goals for both us and our client. Prioritizing critical vulnerabilities helped streamline our efforts and maximize the impact of our vulnerability recommendations. With the guidance from the city of Suffolk's IT department, we decided it was best to present the top three critical vulnerabilities along with the top and bottom three high vulnerabilities, offering our recommendations for mitigation. Additionally, understanding our

client's capacity for change informed the development of realistic and actionable solutions. For example, the city of Suffolk has an inventory of legacy systems, requiring time, money, and careful consideration and scheduling with other departments and system owners when implementing any mitigation strategies to their systems.

**Improvements for Future Projects**

If I were to approach this project again, I would refine the initial scope to prevent drifting into unrelated areas and allow additional time for in-depth analysis and testing, if possible. Creating a shared knowledge repository within the team could also enhance collaboration and efficiency. For example, initially finding everyone's strengths and weaknesses before getting started, having a better understanding of the Tenable.io tool, its functionality, and CIS compliance framework.

**Objectives and Fulfillment**

Our work successfully met the objectives outlined in the internship's Memorandum of Agreement. We applied risk assessment techniques by conducting thorough scans using Tenable.io and analyzing the results. The findings were communicated effectively through a professional presentation and detailed deliverables. Collaboration with mentors and peers further reinforced the practical application of cybersecurity concepts, such as our classroom lectures led by Professor Duvall, Greg Tomchick, and Dr. Baaki.

**Motivating and Challenging Aspects**

The mentorship from professionals like Greg Tomchick and Joshua Cox was a motivating highlight of the internship. Their insights into cybersecurity best practices and vulnerability

management provided meaningful growth experiences. The most challenging aspect, however, was synthesizing the technical data into clear and practical recommendations. Balancing technical analysis with project management responsibilities added another layer of complexity. Luckily, the Tenable.io platform offered strategies and resources to mitigate the vulnerabilities and we worked together throughout the project.

**Recommendations for Future Interns**

For future interns, I recommend preparing by familiarizing themselves with cybersecurity governance, risk, and compliance frameworks such as the NIST and CIS. Additionally, during the internship, maintain open communication with mentors and leadership such as Greg Tomchick, and documenting all work will streamline project execution.

**Recommendations for Course Enhancements**

To improve the course, I recommend adding more in-depth training on tools and frameworks like Tenable.io and the NIST, which will provide a structured framework for team collaboration and understanding. The hands-on mentorship and project-based learning should remain unchanged, as they were essential to the internship's success.

Through this experience, I have gained valuable insights and skills that finalized my academic knowledge and boosted my professional trajectory. The opportunity to contribute meaningfully to the City of Suffolk's cybersecurity posture has been both rewarding and impactful.

**Conclusion**

This internship was a transformative experience. I was able to bridge my academic knowledge with real-world application. The hands-on training in vulnerability management, risk assessment, and professional communication significantly enhanced my technical and analytical skills. In conclusion, this project and experience has shaped my final semester at Old Dominion University. Most importantly, it solidified my passion for working in the GovTech space. I am excited to continue building on this foundation as I begin my career with Leidos, where I look forward to contributing meaningfully and achieving success in cybersecurity and risk management.