Reflective Essay: Developing Key Cybersecurity Skills through Interdisciplinary Learning and Practical Experience

A'shya Reynolds

Old Dominion University School of Cybersecurity

IDS493- Electronic Portfolio Project

Professor Andrews

March 04, 2024

Introduction

As a student majoring in Information Technology and Cybersecurity at Old Dominion University, my academic journey has given me a broad skill set that combines technical and analytical disciplines. I have acquired three crucial abilities through education and practical experiences: technical competency, problem-solving, and analytical thinking. My preparation for a job in cybersecurity, especially with government organizations like the Department of Justice (DOJ), has been greatly aided by these abilities. My education's multidisciplinary focus, especially in IDS 300W and my cybersecurity internship in CYSE 368, has molded my capacity to tackle cybersecurity issues from several angles. This essay will examine how these abilities have been enhanced and how my practical and academic experiences have helped me become more prepared for the workforce.

Analytical Thinking

Artifact: IDS 300W Workshop 1 Assignment

Analytical thinking is crucial in cybersecurity, where professionals must assess risks, interpret security threats, and make data-driven decisions. One of the key experiences that helped me develop this skill was my IDS 300W Workshop 1 assignment, which required creating a visual depiction of the 10-step interdisciplinary research process. The purpose of this assignment was to help me understand the process better by applying visual metaphors. The 10-step interdisciplinary research process I did can be effectively visualized through a crime scene investigation metaphor, with each step symbolized by key actions in an investigation. The process begins with defining the problem, represented by an investigator identifying the crime scene. Next, information is gathered, akin to collecting evidence, followed by identifying various expert perspectives, mirroring how different investigators contribute to solving the case. Data

analysis is symbolized by forensic examination, while the generation of questions mirrors the process of interrogating witnesses to gather more insight. Evaluating methods involves assessing the tools available, similar to detectives reviewing their investigative techniques. Hypotheses are created like theories developed by investigators, and testing them is represented by experiments or simulations. As new evidence emerges, conclusions are refined, just as an investigator revises their theories based on fresh findings. Finally, the research process culminates in the communication of findings, like the final report prepared for presentation in court. This metaphor not only highlights the logical flow of research but also illustrates the collaborative, evolving nature of interdisciplinary work, where different perspectives and methods are integrated to arrive at a well-rounded, conclusive understanding.

Through this assignment, I learned how to synthesize information from multiple disciplines, including law, ethics, and cybersecurity. By integrating these perspectives, I was able to analyze cybersecurity from a broader, more comprehensive viewpoint rather than a purely technical one. This project required me to critically evaluate existing literature, identify potential cybersecurity risks, and propose strategies for mitigating those risks. The challenges I faced in this project, such as distinguishing between ethical and legal cybersecurity responsibilities, improved my ability to think critically and systematically. These analytical skills are essential in cybersecurity careers, where professionals must assess complex security incidents, evaluate risk factors, and develop strategic security measures.

Problem-Solving

Artifact: DOJ Cybersecurity Internship

Problem-solving is a fundamental skill in cybersecurity, as professionals must continuously address and mitigate security threats. My cybersecurity internship with the DOJ

provided firsthand experience in solving technical and security-related issues. Early in my internship, I encountered challenges related to IT configuration and access control, such as resolving PIV badge access issues and setting up security protocols on my work laptop. During the initial phase of my internship, I completed the onboarding process, which included obtaining my DOJ badge, configuring IT security software, and troubleshooting access control problems. This process reinforced the importance of IT support and secure system configurations in a federal agency. As I progressed in my internship, I became more involved in cybersecurity-related tasks, such as analyzing insider threats and reviewing security policies.

One of the most valuable aspects of my internship was participating in weekly meetings with my team leader, Mr. Dondrea Minus, and supervisor, Mr. Christopher Barker. These discussions provided insights into real-world cybersecurity issues and strategies for addressing them. I also completed courses on cyber threats and social engineering, which enhanced my ability to recognize and mitigate security risks. The experience of identifying security vulnerabilities and proposing solutions helped me refine my problem-solving abilities, making me more prepared for cybersecurity roles that require quick and effective decision-making.

Technical Proficiency

Artifact: DOJ Cybersecurity Internship

Technical proficiency is essential in the cybersecurity field, as professionals must be adept at using security tools, analyzing threat intelligence, and implementing security measures. My internship at the DOJ significantly enhanced my technical skills by exposing me to government cybersecurity strategies and security frameworks. As part of my responsibilities, I reviewed key security documents, such as the CIO CS Weekly Status Report and the JCAM tool device report. These reports provided valuable insights into network security, system

vulnerabilities, and proactive threat management. Additionally, I participated in discussions about the EOIR Security Posture, which deepened my understanding of how federal agencies implement security controls and respond to cyber threats.

The internship also involved completing DOJ-required training, such as the DOJ Records and Information Management (RIM) course and the Continuity of Operations Overview (COOP). These training sessions provided a foundational understanding of agency procedures, data security policies, and emergency response strategies. Moreover, I gained hands-on experience with cybersecurity tools and methodologies through courses on cyber threats, social engineering, and insider threat detection. This practical exposure reinforced the importance of staying updated on evolving cybersecurity threats and security measures. The ability to apply technical knowledge in a real-world setting strengthened my readiness for cybersecurity careers, where expertise in security tools and threat analysis is crucial.

Furthermore, my exposure to real-world cybersecurity issues at the DOJ highlighted the importance of continuous learning and adaptability in this fast-evolving field. Engaging with cybersecurity professionals allowed me to understand how technical skills are applied in practice, including the use of security software, vulnerability assessments, and risk mitigation strategies. These experiences have prepared me to tackle challenges in my future cybersecurity career by equipping me with both theoretical knowledge and practical problem-solving abilities. As I continue developing my expertise, I recognize that technical proficiency is not just about mastering tools but also about critically assessing security risks, implementing strategic defenses, and ensuring compliance with industry standards.

Conclusion

My academic coursework and cybersecurity internship have played a significant role in

developing my analytical thinking, problem-solving, and technical proficiency, three skills essential for success in the cybersecurity field. The interdisciplinary approach of my education, particularly through IDS 300W, allowed me to analyze cybersecurity issues from legal, ethical, and technical perspectives. Meanwhile, my DOJ internship provided practical experience in addressing cybersecurity challenges, improving security protocols, and analyzing cyber threats.

The integration of interdisciplinary learning and hands-on experience has prepared me for the dynamic and evolving nature of cybersecurity. Through problem-solving and analytical reasoning, I have learned to approach security threats systematically and develop effective solutions. Additionally, my technical proficiency has been strengthened through exposure to security tools, cybersecurity frameworks, and real-world security practices.

Being an interdisciplinary thinker is vital in cybersecurity, as professionals must navigate the intersection of technology, law, policy, and ethics. My coursework and internship have taught me how to engage with complex cybersecurity issues, adapt to new challenges, and collaborate with industry professionals. Courses like IDS 300W have been instrumental in developing my ability to analyze cybersecurity issues from multiple viewpoints, while my DOJ internship has provided me with the hands-on experience necessary to apply these skills in real-world scenarios.

As I move forward in my cybersecurity career, I will continue to build upon these skills to contribute effectively to the field. The combination of academic learning and practical application has strengthened my career readiness, equipping me with the knowledge and expertise needed to succeed in government cybersecurity roles. Through continuous learning and professional development, I am confident in my ability to navigate the challenges and advancements in cybersecurity, making meaningful contributions to the field.