Reflective Essay

Kendal Eden Taylor

Old Dominion University

IDS 493

Professor Carin Andrews, MBA, MAcc, CPA

December 1st, 2024

Introduction

In my degree program, I have learned several skills on network security, cryptography, cybersecurity best practices, behavioral science and cybersecurity, cyber law, and much more. I have been able to learn research skills in my interdisciplinary classes that have allowed me to conduct research on several topics, including ransomware, malware analysis and incident response analysis. These have come both from the core curriculum, my transfer credits from my community college, the writing requirements curriculum, and the application courses during my time at Old Dominion University. The journey through my academic and professional careers has provided me with many skills essential for a successful career in cybersecurity and information technology. Each supporting artifact from my certifications, my resume, my coursework, and my projects reflect the combination of technical expertise, research skills, and behavioral science in problem-solving. This essay delves into the combination of lessons learned, the problem-solving processes involved, and how they align with my career goals and aspirations.

Information Technology Hard Skills

Through my coursework in IT networking and cybersecurity, both during community college and university, I have honed essential technical competencies in networking, hardware configuration, and system security. I can configure routers, switches, VLANs, manage firewalls, and apply necessary network security protocols. This directly translates to the skills sought in job advertisements for cybersecurity

analysts and network administrators. I have experience with troubleshooting common network issues as well as establishing configuration backups and performing impromptu switch replacements.

Throughout school, I have been working full time in information technology, where I solve various problems daily including hardware issues, network issues, security problems, configuration issues, and more. One of the key lessons I have learned for breaking into IT is the importance of adaptability. IT landscapes are constantly changing and improving with emerging technology, expanding the vastness of cyberspace and the vulnerability of critical infrastructure. One of my long-term career goals is to establish a process to safeguard our nation's critical infrastructure from the ground-up, implementing cybersecurity protocols as early as the electrical engineering phases of new infrastructure we are creating. To begin on this career goal path, I have been working to earn certifications throughout my studies. I currently have A+, Network+, and Security+. This instills a continuous learning mindset and recognizes my ability to adapt to changing industry standards.

While addressing over 1,600 IT-related issues at my work, I relied on both classrooms learned knowledge and practical application of these principles. A specific challenge that comes to mind involves troubleshooting connectivity issues across multiple sites, as our company has several stores across multiple states. This requires isolation of the room problem through troubleshooting, and the ability to work quickly under pressure. In this situation, a VLAN was misconfigured, rendering the entire accounting department offline. Time lost in these departments is critical to our business, so we had to collaborate quickly to determine what was causing the widespread

connectivity issues. Using knowledge gained from my network security and CISCO classes, I was able to remote into the switch that had the misconfigured VLAN and address the problem. This is an example of how my classroom learned skills have been applied to hands-on experience.

Cybersecurity and Incident Response Analysis

One of the biggest undertakings of my academic career was my interdisciplinary research paper; the topic I chose was “What Can the U.S (United States) Learn from the Work of the European Union Agency for Cybersecurity (ENISA) Based on Major Ransomware Attacks in European Hospitals During the Covid-19 Pandemic?”. This paper highlighted the values of integration and international cooperation. It provides insights from cybercrime, policy studies, and medical cybersecurity techniques utilized in the aftermath of the attacks. This experience demonstrates the necessity of applying technical knowledge within breaded organizational, governmental, and societal frameworks. I learned that the most effective cybersecurity strategies extend far beyond technical solutions; they can include proactive policy development, user training, behavioral analysis, and more. This research paper highlighted the critical importance of incident response planning, disaster recovery, vulnerability management, and interdisciplinary collaboration in mitigating cyber threats.

In addition to the European policies studies, I have analyzed the Uber 2022 data breaches, and the vulnerabilities exploited to allow that breach to happen. This process reinforced the importance of understanding how attack vectors exploit vulnerabilities, and the importance of managing those security gaps. By breaking down the phases of the breach, such as initial access, lateral movement, and data exfiltration, I developed a

methodical approach to analyzing cybersecurity incidents. This provides a foundational framework essential for responding to real-world attacks in professional environments, and applying the lessons learned from prior breaches to future applications.

My research on incident response combined technical insights with a great understand of human factors, as social engineers typically exploit behavioral aspects of individuals long before breaching technical systems. For example, the uber breach was initially facilitated by a social engineering attack of a phishing email being opened. These experiences relate to the job requirements of a cybersecurity professional, as they are often responsible for creating or partaking in incident response exercises and procedures. They must synthesize technical and behavioral insights to design a program that encompasses all risks across all departments, not just in the information technology sector.

Skill 3 Behavioral Science and Cybersecurity.

Through my review of behavioral aspects in cybersecurity, I have recognized the critical role of human factors and behavioral considerations when creating cybersecurity strategies. Human factors serve a critical role in shaping organizational security postures. Vulnerabilities such as insider threats and lack of cybersecurity knowledge highlight the need for integrating psychology, criminology, and social science disciplines in cybersecurity practices. I also learned about the impact of prior victimization on user behavior, and how it can be used to gauge the likelihood of whether a person will be re-victimized in a cyber-attack. Understanding these patterns is essential for developing user-focused secure solutions that anticipate and mitigate human error and faults.

Applying the principles of behavioral science, I was able to explore solutions for insider threats by seeing the success of automation detection tools for unauthorized activities. An example of this can be detecting when admin credentials are exported, or for when privilege escalation occurs. This process requires Dinter to grate psychological insights, such as signs of disgruntled employee, into technical solutions such as privilege escalation detection. Concepts such as the theory of planned behavior and social learning theory also broadened my understanding of how users are impacted by technology. These frameworks provide critical knowledge for developing and designing training programs and security policies the tardies both technical and behavioral concerns.

Conclusion

In conclusion, each of these artifacts, from my resume to my research, have contributed to a comprehensive skill set essential for a career in cybersecurity. Together, they emphasize technical pruriency, interdisciplinary problem-solving, research skills, and continuous learning. This bridges technical knowledge with interdisciplinary perspective, allowing me to bring a unique approach to cybersecurity solutions. The lessons learned from the experiences in malware analysis and incident response include adaptability, analytical thinking, and a commitment to collaboration. This underscores my readiness to meet the demands of an ever evolving and challenging field, allowing me to create a rewarding career full of learning and opportunities.