Reflection Paper #3

Cora Wilson

CYSE 368 – Cybersecurity Internship

Summer 2026

Professor Teresa Duvall

TA Jade Hines

Envision Holdings Group

As I have continued progressing through my internship, I have noticed a shift in both my responsibilities and my confidence within the organization. During the beginning stages of my internship, much of my work focused on documentation, inventory management, research, and developing Standard Operating Procedures (SOPs). While those responsibilities helped me gain an understanding of organizational processes and cybersecurity policies, my recent experiences have allowed me to become more involved in direct IT support and employee assistance. Through these experiences, I have gained a greater appreciation for the technical side of information technology while continuing to develop professionally.

Over the past several weeks, I have increasingly taken on help desk responsibilities and become one of the primary points of contact for employees experiencing technical issues. One of the most valuable accomplishments during this period was successfully configuring remote support capabilities. By implementing remote support tools, I can connect directly to employee devices and troubleshoot issues regardless of location. Since many employees work remotely or in various locations, this capability has become an important part of providing timely and effective support.

Working directly with employees has provided me with a unique perspective on information technology than what I have experienced through coursework alone. While many cybersecurity courses focus on technical systems, security concepts, and risk management, helping users solve real-world technology problems requires patience, communication, and adaptability. I have learned that technical knowledge alone is not enough to be successful in the field. Being able to communicate clearly with individuals

who may not have technical backgrounds is equally important. Every support request presents a unique challenge and requires me to analyze the situation, identify potential solutions, and guide employees through the resolution process.

One of the topics mentioned in feedback on my previous reflection paper was whether I see myself pursuing a more policy-driven career path or a more technical role. After gaining additional experience during this reporting period, I am naturally drawn toward the technical side of cybersecurity and information technology. While I enjoyed developing SOPs and understanding the importance of organizational policies, I find myself most engaged when actively troubleshooting issues, solving problems, implementing solutions, and working directly with technology. I appreciate the challenge that comes with diagnosing technical issues and finding ways to improve systems and processes. However, this internship has also shown me that effective cybersecurity requires both strong policies and technical implementation, making each aspect equally important to an organization's success.

Another topic asked about was how my desire to continuously learn contributes to my success within the field. I believe that a powerful desire to learn is one of the most important qualities a cybersecurity professional can possess. Technology changes rapidly, and new threats, vulnerabilities, and tools emerge constantly. Because of this, cybersecurity professionals must be willing to continuously expand their knowledge and adapt to new challenges. My curiosity and willingness to learn have helped me approach unfamiliar tasks with confidence and view challenges as opportunities for growth rather than obstacles. Throughout this internship, I have frequently encountered technologies,

processes, and responsibilities that were new to me. Instead of being intimidated by these situations, I have enjoyed researching solutions, asking questions, and developing new skills.

During this reporting period, I also had the opportunity to further develop my communication and presentation skills. Earlier in my internship, I was tasked with researching phishing awareness training and multi-factor authentication solutions. This project required me to evaluate cybersecurity risks facing organizations and identify practical solutions that could improve overall security. I prepared recommendations regarding employee phishing awareness and researched multi-factor authentication options, including Cisco Duo. This experience helped me better understand how cybersecurity recommendations are communicated to decision-makers and reinforced the importance of presenting technical information in a way that non-technical leadership can understand and evaluate.

The work I continue to perform remains intricately connected to the curriculum I have studied throughout my cybersecurity degree program. My coursework has provided knowledge in areas such as cybersecurity fundamentals, systems security, risk management, networking, and information assurance. However, this internship has shown me how those concepts function in a genuine business environment. In many ways, the internship has helped bridge the gap between theoretical knowledge and practical application. Tasks such as troubleshooting employee issues, implementing remote support solutions, and evaluating cybersecurity recommendations have allowed me to apply classroom concepts in meaningful ways.

Overall, I continue to find this internship both rewarding and meaningful. Each new responsibility provides an opportunity to develop additional technical skills while gaining a deeper understanding of cybersecurity and information technology fields. The experiences I have gained through direct employee support, remote troubleshooting, cybersecurity research, and professional collaboration have strengthened my confidence in pursuing a career within the industry. As I move forward through the remainder of my internship, I look forward to continuing to learn, taking on additional technical responsibilities, and further preparing myself for a successful career in cybersecurity and information technology