

Kerina Drummond
June 6, 2025
Professor Duvall
CYSE 368

Reflection Paper #1

BLUF: This reflection paper follows events that have taken place during my current summer internship, which has had an impact on my learning and has strengthened my knowledge in the fields of cybersecurity and IT alike.

Introduction

Over the past 50 days, I have been interning with Old Dominion University's Information Technology Department under the DSG ACAD group. This team primarily handles hardware and software tasks, including device re-enrollment, property control of out-of-warranty equipment, configuring new devices, troubleshooting remotely or in person, and securely wiping hard drives. During this time, I've learned how to conduct detailed inventory checks, configure devices for end users, and efficiently navigate our internal ticketing system. These experiences have enhanced both my technical skills and my understanding of institutional IT infrastructure.

Inventory Check

For the past two weeks, our student worker team has conducted inventory checks across various ODU buildings, including Batten Arts and Letters, Education, and the Student Recreation Center. These checks are essential for accurate asset tracking, compliance, and security. Maintaining up-to-date records ensures we know who owns each device, where it's located, and whether it's under warranty. This process directly supports cybersecurity efforts by identifying outdated hardware and ensuring software updates are applied regularly. In a network

as large as ODU's, minimizing vulnerabilities through effective asset management is critical. During these checks, we matched devices to records using location, assigned user, ETF tag, and serial number. If the information was accurate, we marked the entry green; if the device was missing, red; if the device was present but not found in the system, yellow. We also added any unlisted devices we encountered. This process gave me a practical understanding of how cybersecurity and asset management intersect in real-world environments.

Device Configuration

Device configuration becomes necessary when a staff member's computer is out of warranty or has persistent issues that cannot be resolved. The process involves naming the device, recording its location, and installing all required software to ensure smooth and secure operation. This week, I configured a device for a staff member in the Goode Theater. I began by backing up files from the old device to our shared drive. I then selected a new, in-warranty device and followed all required steps to prepare it, ensuring the hardware and software were functioning properly. Finally, I transferred the files from the drive to the new device to ease the staff member's transition. While the configuration process may seem routine, I have come to appreciate its significance in maintaining operational efficiency and cybersecurity standards across the university.

Ticketing System

In our department, the ticketing system is essential for managing IT support requests. It centralizes communication, ensures secure information exchange, prioritizes issues, and helps allocate resources efficiently. Over the past week, I have used the system frequently, particularly

while configuring a new device. It allowed me to communicate clearly with both colleagues and the end user, making updates and coordination easy. One feature I particularly enjoy is the “In State” button, which indicates whether a device is actively being worked on, on hold, or delayed. This allowed me to keep everyone informed throughout the process. This tool not only improved my workflow but also gave me insight into how structured communication enhances productivity and accountability in IT operations. This system also helps with troubleshooting by allowing us to keep detailed records of a device's movements.

Takeaways

Over the past 50 days, I have gained a range of valuable technical and soft skills. I've worked with systems and tools that I am likely to encounter in future IT and cybersecurity roles, while also strengthening my communication and collaboration abilities. I've come to understand that technical support is just as much about customer service as it is about problem-solving. Some users are cooperative, while others require more patience and adaptability. I've learned how to explain technical concepts in simple, accessible ways to users with limited technical knowledge. Tasks such as inventory checks, device configuration, and use of the ticketing system have taught me critical lessons about asset management. Ensuring that devices are in warranty, secure, and regularly updated is essential, not just for individual users but for the security of the entire network. Prevention is key in cybersecurity. Seeing the concepts I studied in class applied in a real-world setting has deepened my understanding and strengthened my confidence as an aspiring cybersecurity professional.