Internship: Reflective Paper #3

by

Galen Cole

A Reflective Paper

Submitted to CYSE 368

Old Dominion University

Reflection Paper 3

November, 2024

Contrary to my previous entry, a lot has changed. Throughout this time, I've worked in a customer-facing role, assisting users with any problem with university services. This time has been invaluable in showing me the workings of enterprise IT operations, the human factor in security, and much more. The list of systems, procedures, and users has grown continuously. At the same time, so has my non-official guide helping me help others.

Not only do we have the Easter Virginia Medical School (EVMS) merger, but we also have many upgrades to existing systems. This began to create many problems that previously didn't exist regarding normal operations at the university. Specifically, the Banner upgrade, which was supposed to be completed on October 17th, continues to face migration issues as of my writing on November 3rd. I've found the story's moral is that more work is not always good work. Personally, Banner should have remained hosted internally at ODU, or a rollback plan should've been put in place if particular objectives were not met. This process has made me realize how deadlines outside of my department can affect my department. For example, this weekend was the deadline for the Student Opinion Survey reports for teaching staff; however, Banner Insight (Cognos) required a VPN to access it after the migration. This does not reflect our documentation, creating confusion and upsetting staff members. The worst part is that my department has nothing to do with this update, and it is all just a waiting game with me repeating less-than-perfect news to users.

Over time, and more recently, ODU/EVMS has been targeted with increasingly sophisticated phishing emails. This has led to a lot of time at the help desk being allocated to password resets, a workforce that could be used for more complicated tasks. ODU has finally started to address the issue as these attacks rage on. Specifically, the ITS Help Desk plans to implement a process with IT Security to identify and contain these issues and assist users with

the fallout of these encounters. IT Security has also begun to create ‘fake’ phishing email campaigns to enroll users in mandatory cybersecurity training courses. Any user who clicks the ‘phishing’ link in the email is enrolled in the training. These are being implemented to mitigate these attacks, whether successful or not. Most notable in these attacks is how malicious users circumvent existing protective measures, like denying external emails with Outlook’s filters. In recent attacks, users were able to get a foreign government email as well as a @***.edu email to send emails through our filters.

I would not trade this time for anything. This has provided me with priceless experience, insight, and skills that I can apply in future enterprise environments. It has introduced me to imposter syndrome, but weirdly enough, it has helped me deal with it. Specifically, what helped was becoming a Head Help Desk Technician and the separation of duties at ODU ITS. After almost two years, I’ve finally been notified, to my knowledge, of my first ‘good job’ email someone sent specifically to my hiring manager; they were even an EVMS user. I’ve been introduced to a plethora of services, departments, and roles within this environment I would be completely unaware of otherwise. Moreover, this has been a tedious yet rewarding process that has given me my first glimpse into the somewhat ‘real world’ of enterprise cybersecurity, which I’ll be dealing with for the rest of my life.