

CYSE 368 Final Paper

Kenneth A. Piontek

Old Dominion University

CYSE368 Internship

Dr. Saltuk B. Karahan

November 27, 2002

I decided to join the Department of Homeland Security for both professional and personal reasons. Professionally this was the next progression in my career as a cyber security professional. The insight, visibility, exposure, and responsibility was something that I sought out and an opportunity to challenge myself. Personally I wanted a position where I felt that by doing my job as best as possible that I was then in turn helping to keep people close to me safer. While not taking part in an internship as I'm well within my career in security, my final paper is a reflection of my job as it relates to some of the questions being asked of those engaged in an internship and not already in the workforce.

Within DHS I work for the Office of Biometric Identity Management. According to DHS's official website, the Office of Biometric Identity Management (OBIM) provides biometric match, store, share, and analyze services to DHS and mission partners. The need for biometrics continues to grow among DHS Components; interagency stakeholders (e.g., the Departments of State, Justice, and Defense); state, local, tribal and territorial entities; the Intelligence Community; and international mission partners. Biometrics support critical national security priorities, including counterterrorism and immigration. OBIM is focused on delivering accurate, timely, and high assurance biometric identity information and analysis. OBIM's overall goals and priorities include continuing to improve biometric services and access to expanded biometric data to enable DHS operational missions.

My major work duties include ensuring proper access controls are in place for two major information systems. In addition, ensuring that we have processes in place to adhere to proper account management. Keeping up to date with best practices to ensure that the current policy and implementation of account's access meets our standards. I often work with various stakeholders to make sure that the procurement actions that are necessary for any of my

information systems have the correct language and provisions in place to avoid any security related issues in the future. I'm also responsible for conducting assessments of controls of my systems to ensure the controls have been implemented properly and are still effective on a periodic basis in accordance with the tailored set of controls based on the NIST 800-53 series. I'm also responsible for taking part in presentations for both security awareness and training with all of our various stakeholders. I do quite a bit of log analysis for the purposes of either incident response or compliance and accreditation efforts. I'm also the component registration authority for my division managing PKI activities for the enterprise. This involves creating, deleting, re-keying, and troubleshooting technical issues surrounding certificate issuance and key generation. I'm also responsible for the incident response activities within my enterprise. Working with various stakeholders when either alerted to or discovering incidents on my own to mitigate any damage done and put measures in place so that the same type of incident doesn't happen again.

Specifically in my job I have to make use of a lot of and acquire new skills and knowledge of cybersecurity. The time I spent early on in my career working on a help desk doing break fix and network support I utilize in my career today. The time I spent working in a SOC doing security engineering, security analysis, and customer management I still use to this day. The SIEM tools and linux knowledge acquired through that experience helps me in my job today. The time I spent there at Computer World Services was invaluable as well, in that job I worked as a contractor supporting the same agency and office that I currently work for today. The size of the agency alone makes the onboarding process and learning curve for just the way of doing business and management of your career there something that I can see someone with no exposure to an organization that size could get really overwhelmed with.

The ODU curriculum didn't really prepare me for my job per say, but upon completion of my degree the doors that that achievement will open for me are immeasurable. Not only immediately professionally, but academically as well. I would like to continue my education and open the next chapter of my life and career in the field of data science. I'd like to do some work in security analytics and machine learning. Without my bachelors, I can't start my masters. I was able to make some connections though with what I've learned while here at Old Dominion and in my job. The material is real world relevant and there is correlation between the material and many aspects of my job. The topics studied in networking, forensics, cybersecurity policy, cyberwar, and even interdisciplinary studies can be correlated to my job all throughout the responsibilities mentioned.

The most motivating part of my job is the feeling that I'm doing something worthwhile, important, and impactful. The most discouraging part of my job is that you can't make everything you touch perfect. While that might sound a little silly you often find yourself very emotionally involved in what you're doing and wanting to see a certain positive outcome and when that ideal doesn't happen it can be discouraging. The most challenging part of my job is managing all my responsibilities. If I had any advice to give someone just joining the agency out of college I would suggest day one make sure the way in which you're going to organize all your competing priorities is the first thing you do, the rest your will and skill will take care of.

This is the last semester of my undergraduate career and in conclusion I want to express how the experience will influence my future professional path or planning. In addition to the academic and professional career aspirations personally, the sense of accomplishment that comes with my degree is indescribable. It's the culmination of a long and difficult journey that means anything is possible.