Personal Narrative Essay

Lucas Dyer

Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Carin Andrews

February 6, 2026

Where I started

For the vast majority of my early life, and up until my last few years in high school, I had always envisioned myself finding a job in an engineering field. My biggest hobby as a child was Legos, and I had always loved building and making things. However, as I progressed through high school and my engineering course, I found myself spending more time doing math, and less time actually creating things. Additionally, while certain engineering careers can pay very well, the reason I liked to create things was to express my creativity, and having to make something that I was not interested in simply because it was my job was not appealing to me. As such, I decided to pivot away from engineering and sought an alternate path. As luck would have it, when picking my classes for the next year, a newer class caught my eye, Intro to Cybersecurity. The professor made a very compelling pitch as to why this would be a great career for anyone to pick, which boiled down to two things. There are not enough cybersecurity people at the moment, meaning the job market and security is much better than most other options, and the pay is very good. I happen to think both of these qualities are ideal in a job I would have to do, and thus I switched my focus from engineering to cybersecurity. While not exceptionally passionate about the subject at the time, I did appreciate the interdisciplinary aspect of cybersecurity, as I enjoy a wide range of interests. When I graduated high school, I looked for colleges that offered a major in cybersecurity. In Virginia, there was only one- Old Dominion University (ODU). I applied for an early decision, was accepted in December, and was offered a scholarship due to my high GPA and decent SAT score.

Early Years at ODU

One of the benefits of being an interdisciplinary field is that cybersecurity allows me to study and learn a great variety of subjects and skills. There is, however, a downside to this approach. Despite all the things I was learning, such as how to use virtual machines, Linux systems, criminal justice, digital crimes, ePortfolios, and more, no class I had ever taken had really defined what a cybersecurity job would look like. As I progressed through my classes, I kept asking myself, I have these skills, but what do I do with them? I learned early on that I preferred the more conceptual and person-oriented side of cybersecurity, as the extremely technical and coding side of cybersecurity is not one I enjoy. Coding can be satisfying when it works, but if it is not working, and you don't know why, then there is no feeling more frustrating. It was about halfway through my time at ODU that I had my first internship, and it was in a place that might seem out of place.

The U.S. Embassy in Zagreb, Croatia

Over the summer of 2024, I had an internship with the U.S. Embassy in Zagreb, Croatia. I was initially with the department of technology, but after a month I had finished all the work they had planned for me, so I was moved to the general services department to assist them. I was in Croatia for the summer because I was visiting my parents. My mother, who works as a diplomat at the embassy, informed me that the embassy was offering a summer internship program, which I applied for and was accepted. During my time with the embassy, I handled sensitive but unclassified information in compliance with State Department protocols, digitized a large volume of records, removed hard drives containing sensitive information and prepared them for secure destruction, and promoted cybersecurity awareness by ensuring that every workstation

with a webcam had a proper cover. After my internship I felt more confident with being in a work environment, as well as completing assigned tasks, but most of my work was more general office work than the cybersecurity work I was going to college for. I continued my studies, and in spring of 2025 I was made aware of another internship opportunity, this time explicitly cybersecurity related. The Commonwealth Cyber Initiative for Coastal Virginia (COVA CCI) was offering an ODU specific internship in the fall. I sent in my resume and was accepted into the internship program.

COVA CCI

This internship was a major step in defining what a career in cybersecurity might look like. Not only was I tasked with working in a team for the long term, but we also had a clear goal set before us. After hearing from some cybersecurity speakers and doing some icebreakers, group challenges, and other team building activities, we were assigned our teams and then given our clients, who were small local businesses, sometimes with as few as one owner/employee. Our job was simple. We would meet with our client, hear their cybersecurity concerns, along with any other cyber questions they had, and then we would spend the rest of the semester researching and writing a full report that not only had an analysis of their current cybersecurity capabilities, but also ways to shore up any weakness they might have and how to have good cyber hygiene going forward. We additionally created a presentation of the information we had gathered in our report so it could be delivered verbally in a more digestible format, and so that we could answer any questions our client had regarding our results. My biggest takeaway from this internship was that it provided a clear example of a cybersecurity job, more specifically one in a governance and compliance role. I realized I could easily see myself working in this specific capacity at a

company, where my primary role and responsibility would be to perform research, create papers, policies, and proposals, and then explain them to my higher ups to ensure they understood the need of my policies and would approve them. I would also likely have to explain and justify any increase to the cybersecurity budget. In order to get a cybersecurity budget approved, you have to be very persuasive and have a lot of research and evidence to back up your claims, as the results of a successful cybersecurity defense for a company is that nothing happens. As such it can be difficult to see money seemingly vanish for no reason, when instead approving a higher budget for a different part of the company results in visible capital gains. However, as today cybersecurity is part of the public consciousness more than ever, the vast majority of people understand how important it is, and that having lacking cybersecurity could result in the loss of almost all their assets, especially with how much of the world has become digital.

Conclusion

As I finish my senior year this semester, I hope to graduate with the knowledge and skills required to secure a comfortable position in cybersecurity. I have learned much, both from my education and from my work experiences.