IDS493 PERSONAL NARRATIVE ESSAY

Alan Schneider

Department of Cybersecurity, Old Dominion University – Norfolk

IDS493: Electronic Portfolio Project

Dr. Gordon-Phan

29 July 2023

My First Career

I never imagined myself where I am now, after having spent 21 years in the military and now graduating this fall with my bachelor's degree. My intention was always to retire, like my parents did in their mid-forties. Putting the stressful day-to-day of a career behind me and focusing on those things I always wanted to try but did not seem to have the time for. My journey began some 30 years ago, the youngest of my children had just turned five and I was working two jobs to make a payment on a house I could not afford. Living paycheck to paycheck just was not cutting it, not if I wanted my family to enjoy a better life. So, with my wife's support I chose to join the military.

I remember being more focused during those long months at boot camp and follow-on training than I ever had before I joined. Motivated by a need not only to provide for my family but also to prove to myself I could do it and excel at it. After completing training, my first command was at Little Creek Amphibious Base, right here in Hampton Roads. I showed up fairly confident I was prepared for whatever they threw at me. The military's emphasis on teamwork, discipline and attention to detail were fairly well ingrained after nine months between boot-camp and training and so I believed at the time the ins and outs of my job as a radio communications technician. Let us just say that it did not take long for me to realize that I had a long way to go before I could truly consider myself professional at my job. That is when I understood that a set period of instruction does not make you a professional in your field, it is committing to a lifelong continuum of education that does.

Over the course of five years at that command, I learned more about radio frequency propagation, line of sight tactical communications equipment and techniques, satellite communications voice and data capability and encryption handling, dissemination, and

accountability. At the same time, I was developing hard skills, I was mentored in the soft skills required to lead and manage people. They taught me to identify and nurture talent, encourage critical thinking in myself and others, how to motivate people as individuals and a team by learning what drives them and investing my time to help them achieve their goals. Learning the importance of recognition, that praise from peers is an important component that ensures people understand that they're valued and their contribution matters. I also had to learn the other side of leadership, having to make hard choices on who to recommend with a limited pool of promotions and awards, how to deal with disciplinary problems without ego and protect my people by treating each command position like it's my last instead of chasing promotion by trading on my integrity. Those lessons are not only part of being good at your job, but they are bricks in the foundation of your professional career.

But part of being professional is staying relevant, and information technology matured during that time, networks went from being exceptions built for research, industry, or limited government use to the ubiquitous Internet of things that is part and parcel of our lives. Ships no longer primarily relied on voice circuits and limited satellite bandwidth to connect. So, my exposure to modern networking and the follow compliance and auditing aspects of cybersecurity did not come until my second command located at a schoolhouse on damneck base. I had no formal training in networking. So, I had to complete a network analyst course that taught windows server 2003 environment. Active directory users and groups. Configuration, and maintenance of exchange, forest and domain structure and routing using CISCO IOS and protocols. After that, I settled into my new job as a network administrator: creating accounts, modifying file and folder permissions, monitoring switches and routers while dealing with daily trouble tickets. Some as simple as rebooting a computer to having to rewire an entire classroom

after someone's spilled coffee coated the fiber optic cable runs under the false floor, prompting the buildings rodent population to go on a chewing spree. I also had the opportunity to plan and execute updated network segmentation architecture utilizing Virtual Lan's. Improving the schools network performance reducing the amount of broadcast traffic that devices needed to process by segmenting the domain into smaller broadcast domains. Over the three years I was there, I learned quite a bit about network administration and disaster planning and recovery. But what really captured my attention was the auditing and compliance process that was crucial in obtaining a network's Authority To Operate (ATO) on the DOD's Global Information Grid.

I learned as much as I could about the certification and accreditation process ensuring security of government information systems. Evaluating, testing, and examining security controls and comparing the current systems' security posture with specific standards. Ensuring that security weaknesses were identified with mitigation strategies in place. And then accepting the residual risks associated with the continued operation of that system. I had a new aspect of information technology to explore and as soon as I transferred, I trained as an Information Systems Security Manager (ISSM) and never looked back. From there my professional focus was on vulnerability scanning, reporting and remediation. I was tasked with developing and maintaining information assurance programs encompassing system security accreditation documentation, validate system configurations to include new installations and/or modifications as well as DOD information technician certification program compliance across multiple commands. Finally, after 21 years in the military, I retired and decided to use the college benefits promised under my contract.

Never too late to learn

I have to admit, I was a little hesitant. Here I was one year shy of fifty, retired from my first career and now contemplating being a student again. It seemed a little backwards, but I went with it and registered at Tidewater Community College. I remember my first semester, when I logged into zoom for my freshman ITP100 Software design class and was promptly mistaken for the instructor, it was a little awkward. What was interesting about that class is that although I understood the basis for popular machine languages like Java and SQL I had actually never programmed in any. It took me a while to get a handle on essential programming logic in structured and object-oriented design. But, by the end of the class I did not have any issues. The rest of my classes at TCC afforded me the opportunity to revisit skills I had not used in the latter half of my career. Reintroducing me to network administrative tools, CISO configuration and routing fundamentals and exposing me to cloud computing infrastructure design and services that the military was just starting to truly embrace.

It was not until I transferred to Old Dominion that I feel I have broken some new ground in my education. Cybersecurity Techniques gave me the opportunity to learn tools and techniques involved in ethical hacking. Traffic tracing and analysis, using port scanning tools and penetration testing were new in my military experience and training. Using Metasploit to enumerate target machine vulnerabilities and deploy Server Message Block exploits in a custom payload, executed through a reverse shell granting access to the target machine. As well as using brute force and dictionary attack methods to crack passwords and tools to crack and decrypt Wi-Fi traffic were also proficiencies never acquired. Cyber law opened my eyes to key regulations governing fourth amendment search and seizure of digital property and the legal precedents that frame just how much an effect that improper collection and chain of custody of such can have on

individual due process and informational privacy. It also expanded my awareness of a gap between traditional ideas of just cause and just war governing international conflict and the gray area of cyberwarfare inhabits contributing to “soft conflicts” that are neither proportional nor limited in the suffering they can cause.

However, Interdisciplinary Theory and Concepts delivered the most radical shift in my definition of stakeholders as it relates to complex problem solving. I was always mentored to bring in a broad offering of expertise to bear on complex problems. Sometimes solving an insurmountable problem just requires a little face to face time or someone with a little distance from the problem. The difference between what I learned and what IDS 300W had to teach is that I never truly looked outside my discipline for insights. Preferring to reach a solution using corporate knowledge within my field. However, IDS taught me that that even seemingly disparate disciplines have contributions to offer. This allowed me to integrate deep knowledge of disciplines outside my wheelhouse like economics, federal regulation, and psychology. Aiding me in creating a comprehensive understanding of the forces incentivizing cyber attacks like ransomware on critical infrastructure. And that a singular focus on IT as both source and answer, robs cybersecurity professionals of wider viewpoints outside their chosen discipline. Constituting missed opportunities to apply more effective and robust approaches leading to real world solutions to complex cybersecurity problems.

Conclusion

As I said in the beginning, being a professional in your field is a commitment to lifelong education. Technical, leadership and management skills are part of being good at your job. Requiring constant maintenance and practice to ensure continued relevance in the field as it

matures. But equally important is being able to see the contribution other disciplines have to offer and take a chance that embracing other worldviews will benefit you and those around you.