Reflective Essay IDS493.

Alan Schneider

Department of Cybersecurity, Old Dominion University – Norfolk

IDS493: Electronic Portfolio Project

Dr. Gordon-Phan

29 July 2023

Abstract

As ransomware attacks, data breaches, denial of service attacks and other cybersecurity incidents continue to increase in number and complexity. Industry leaders, Cybersecurity professionals and Legislators are continuously looking for ways to mitigate the extraordinary economic and national security consequences of these threats. This underscores the necessity in acquiring a diverse range of skills required for success within the field of cybersecurity. E-portfolio reflections serve as a summary of the technical, writing, and critical thinking skills acquired over the course of training within the field of cybersecurity. The artifacts presented within an e-portfolio are then critical components in creating a comprehensive permanent record of those skills. Ultimately, not only providing the creator valuable insights into the body of knowledge gained over the course of their education, but also a top-level view of gaps in both the hard skills acquired from education, training and work experience or soft skills of adaptability, teamwork and communication that are so essential to job success.

Introduction

My e-portfolio serves as a professional roadmap. Giving me an idea of the areas of cybersecurity competency I'm practiced in and where I'm missing critical certifications. Not only serving to expand my knowledge base but to encourage continued education and growth that supports continued relevance in the field. It also serves as a basis to create a better resume. Increasing the likelihood of future employment and better salary negotiation position when interviewed. Over the course of my cybersecurity education beginning at Tidewater Community College and graduating from Old Dominion University, I have acquired technical, writing, and critical thinking skills essential for success within my chosen field. Technical skills like ethical hacking or cloud computing infrastructure and deployment. Critical thinking skills, through study of cyber law and philosophy enabling me to assess the impact of various U.S. laws and legal considerations on informational privacy and the scope of legal as well as moral responsibility owed in protecting it. As well as writing skills garnered in English writing classes aiding me to effectively communicate the essence of policy recommendations and frame the critical nature of investment in not only technical but human solutions to complex cybersecurity problems.

Technical Skills

My time at Tidewater and Old Dominion has reinforced and updated the foundational skills I acquired through the military and need for a successful career in Cybersecurity. As a discipline cybersecurity exists to prevent, detect, and respond to cyber-attacks, ensuring critical information systems operate with a measure of integrity and maintain availability. This means acquiring knowledge in networking and network architecture, operating systems, virtual machines, cloud security, blockchain security, IoT, and ethical hacking topics. Not only to develop the computer forensics skills required to investigate security breaches and recover data, but to be able to develop and implement security, access, administrative controls, and policies that are the core of network defense. All while staying abreast of new technologies, techniques, security standards and practices designed to defeat evolving threats. In the next few paragraphs are artifacts that demonstrate some of the technical skills I have gained during the course of my studies.

CYSE301 Cybersecurity Techniques and Operations

Artifact 1: Cybersecurity Techniques and Operations-Sword and Shield

This course focused on tools and techniques involved in ethical hacking and cyber forensics. I've always been interested in learning ethical hacking, so when presented with the opportunity to take this class, I jumped at the chance. This artifact demonstrates practiced skill as an attacker conducting initial reconnaissance to identify network vulnerabilities and subsequently apply countermeasures to those identified vulnerabilities as a defense. Using NMAP from an external kali host, I was tasked with collecting basic information about the target Virtual Machines subnet topology. Identifying open ports, service and backend software information associated with those ports. Concurrently, I utilized Wireshark on the target VM to conduct a packet capture of external kali attempting to scan for open ports. I observed external

kali scanning for open ports by attempting 3-way handshake connections between source and destination port. From that capture I was able to build firewall rules designed to block TCP, UDP and ICMP packets received over selected ports and from specific Ip's. Successfully blocking further NMAP scanning originating from the external host.

Artifact 2: Cybersecurity Techniques and Operations-Ethical Hacking

My second artifact is an ethical hacking assignment that demonstrates my ability to conduct penetration testing of target hosts. I was tasked with penetrating several hosts with different operating systems. Utilizing NMAP I identified open ports and backend operating system information. I then used Metasploit to enumerate target machine vulnerabilities and Msfvenom command-line utility to create custom payloads compatible with a number of different architectures and operating systems. I then deployed several Server Message Block exploits executing both bind and reverse shell connections to grant access to the target machines. The reverse shell required uploading the payload to a compromised web server running Apache. Once the target machine clicked on the malicious link and downloaded the payload, I was able to gain access to the host and exfiltrate user id's, system information and screenshots of the target desktop.

Artifact 3: Cybersecurity Techniques and Operations-Password Cracking

This assignment taught a variety of password cracking techniques. I was tasked with creating a set of login credentials, using the Linux command: shadow to encrypt the passwords. The first cracking technique used was a dictionary attack using a set wordlist with john the ripper against the saved hashes. I then used the brute force method against the same set of password hashes. This assignment also gave me the opportunity to practice decrypting Wi-Fi WEP, WPA and WPA2 encryption schemes using the airdecap program for WEP and WPA and aircrack.ng for WPA2. This assignment really underscored the importance of strong encryption schemes to protect not only data at rest, but wired and wireless communications.

Critical Thinking

Critical thinking skills applied to Cybersecurity are just as important as the technical skills you need to be successful in the field. Asking the right questions, evaluating, and assessing data, identifying assumptions, alternatives, understanding context. helps you to make high-stakes decisions about your organization's security. Being effective in cybersecurity means cultivating self-awareness that bias can cloud your judgement and that an open mindset breeds flexibility in thinking allowing you to look outside your chosen discipline for insights into complex problems. My exposure to cybersecurity management, philosophy and interdisciplinary research at Old Dominion have broadened my worldview and allowed me to redefine what it means to be a stakeholder in an organization's cybersecurity. The artifacts below are just a few of the examples that demonstrate my critical thinking skills:

CS462 Cybersecurity Fundamentals

Artifact 1: Kaseya VSA Ransomware term project

This course gave me valuable insights while practicing and improving my analytical skills. During this course I learned applying deep analysis to cyber-attacks not only reveals the vulnerabilities, techniques and methods utilized, it can also illuminate the incentives that drive these attacks, and the individual and societal costs associate with them.

For my final project, I was tasked with describing a recent cybersecurity attack in detail. Analyzing the breach to include the devices, protocols, or applications used to perpetrate the attack. But, also to frame the cost of these attacks to society. My papers focus was on the July 2, 2021, Kaseya cyber-attack in which a Ransomware as a Service (RaaS) group were able to disrupt up to two thousand organizations spread around the world. Not just private corporate networks, but government systems as well. What captured my attention went beyond the technical details and the cost of this particular attack. They were the unintended third order effects caused by other

attacks that finally tipped the scales, pushing people to act. Unintended deaths both abroad (Koplowitz Howard) and at home (Ralston) as well as attacks directed against our universities, water (CISA) and fuel distribution motivated a sitting president to threaten unilateral action against Russian and Belarusian groups responsible for the attacks if those countries leaders didn't act. Spurring our government to designate Ransomware attacks as a threat to national security. This project taught me to look outside the narrow scope of any attack affecting an organization I work for and consider the wider implications to others I might consider unaffected.

IDS300W Interdisciplinary Theory

Artifact 2: Effects of economics, cyber fatigue, and poor regulation on cyber defense.

Interdisciplinary theory introduced me to an examination of the history, concepts, and application of interdisciplinary study. Teaching me tools to analyze similarities and differences in academic disciplines and then apply an interdisciplinary approach to a specific topic of study. My final project was to dissect this attack, not in terms of the technical details of the breach. But rather what the attack can teach us about the effects of ransomware economics, cyber fatigue and regulatory challenges on coordinated network defense and recovery. What excited me about the project was the chance to step outside the "comfort zone" of my discipline and look to others for answers. Research into collective bargaining strategies (Hernandez-Castro et al., 2017) and price discrimination (Hernandez-Castro et al., 2017) provided me a lens through which risk vs reward factors, influencing decisions to conduct ransomware attacks could be identified. I developed a better understanding of the psychological effects that overexposure to cybersecurity-related work demands, or training has on cognitive disengagement in positive cyber-related workplace behaviors or advice (Nobles, C. 2022, p.3). And I was able to codify the challenges posed to regulatory and prosecutorial efforts by the transnational nature of these attacks (Lubin, A, 2022). My research allowed me to combine the insights gleaned from each discipline's narrow field of view into a comprehensive approach and taught me the considerable value other disciplines bring to the table, when tasked with solving complex problems.

PHIL355E Cybersecurity Ethics

Artifact 3: Case Analysis on Cyberconflict

While the other courses emphasized technical and disciplinary aspects affecting the field of cybersecurity my philosophy class examined ethical issues relevant to computing and information technology: privacy, freedom of speech, individual and social responsibility, and ethical obligations of professionals within the field. My experiences in the military through a culture of mentorship ingrained ideas of integrity and responsibility as equal important to any technical capability acquired. This paper gave me the opportunity to explore what happens when powerful nations; in this case Israel and Iran, reject traditional ethical rules aimed to govern armed conflict, in favor of a form of "soft conflict" ostensibly causing damage in a non-physical or violent way. But that invariably lead to an escalatory tit- for-tat cycle of cyberconflict, just as likely to cause suffering and death as traditional warfare. This is where Mariarosaria Taddeo concept of transversality (Taddeo, M) in cyberwarfare was fundamental to my understanding of the issue. That transversality cuts across any traditional warfare distinction such as 'violent-non-violent', 'civil-military', 'human agents-artificial agents. Resulting in a blurring of lines between levels of violence and escalation from non-violent to more violent forms, without regard to principles of proportionality and last resort. Ultimately, this course and in particular this paper, reminded me that employing technical capability without examining ethical responsibility is a mistake that too many within the cybersecurity field are prone to make.

Writing Skills

Over the course of my military career, I've been given the opportunity to write extensively: fitness reports, awards, white papers, and policy recommendations. Each of these exercises were important in building my communication skills. Skills I need to clearly articulate complex strategies and solutions to co-workers, effectively convey levels of risk, urgency of taking action on critical issues to my seniors, convincing them to spend the human and financial capital required to address them. Over the course of my college education, I've had the opportunity to continue to refine those writing skills, through English writing courses at TCC as well as Cyber Law at Old Dominion. These next few artifacts will demonstrate my ability to clearly convey ideas, explain problems and recommend solutions.

CYSE406 Cyber Law

Artifact 1: Privacy Policy Guidance

I've written, reviewed, and commented on military policies ranging from programs to personnel and security as directed by senior military leaders. However, my cyber law class was my first introduction to writing policy recommendations concerning federal law as it relates to constitutional privacy and for dissemination to publicly elected officials. In this assignment I was tasked with crafting a privacy policy recommendation for a fictional state, regarding collection, use, retention, and dissemination of information of its citizens by federal and commercial entities. I included legal definitions and examples of what constitutes Personally Identifiable Information (PII), Biometric data and Protected/Personal Health Information (PHI). From there I was able to reference applicable federal statutes like the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPPA) that govern PII and protected health information. I was also able to reference Illinois Biometric Information Privacy Act. (BIPA). One of only three states that have enacted privacy legislation as it relates to biometric collection. Informed by the current state of privacy legislation, I was able to recommend specific changes

that would allow an elected official to craft a robust privacy regulation and allow them to address organizations using Terms of service as a way to make consent for data collection a requirement for use of their goods or services. As well as ensuring that biometric information as detailed in Illinois Biometric Information Privacy Act is specifically enumerated in the policy guidelines above or adopted as a separate and distinct regulation.

Artifact 2: Senate Bill 686 background research memo

This assignment hit a little closer to home, as I had to produce a research memo covering a proposed bill currently making its rounds through the senate. Dubbed colloquially the "Tik Tok ban" this bill would give the Department of Commerce Secretary the authority to review, block, and mitigate transactions involving foreign information and communications technology (ICT). Essentially, the Act would enable the U.S. government to ban the sale of certain countries specific software or equipment or force a change in ownership of those companies if deemed to pose a spying risk. I found the language of the bill to be overbroad, giving the government too much leeway to control and censor information. Banning apps and services that allow people to communicate, such as TikTok, potentially limits freedom of speech. I also raised additional concerns in the memo that VPN use could be interpreted as illegal based on the Act. This was based on sections describing services "designed or intended to evade or circumvent the application of this Act" (S.686) as being covered under the Act. My final concern was the inclusion of a FOIA exemption (U.S.C. § 552) that raises questions of transparency in an age of government misconduct.

English 112: College Composition

Artifact 3: Zero Tolerance in schools

This assignment allowed me to communicate to a wider audience the evolution of zero tolerance policies applied by today's public schools. This was a topic I researched when my children were still in school. What I found in part were patterns of unacceptable and unconstitutional behavior by organizations ostensibly established to educate and protect our children. In theory Zero tolerance policies were designed to reduce alcohol and drug use by minors at school and to protect children from gun violence. In practice however, zero-tolerance policies were aimed at all sorts of petty annoyances that get under the skin of individual administrators. Routinely violating minors constitutional right to due process and eroding trust between school administrators and parents. In completing this paper, it reminded me that in the past, as an individual and parent I've sometimes taken for granted that others have my children and other children's best interest at heart. The reality is that abrogating parental responsibility in keeping an eye on those ostensibly tasked with your children's safety is a recipe for disaster.

Conclusion

This next semester, I'll graduate from college and start my second career. This doesn't mean my education is over, it just means I'll continue to work toward excellence in my field by learning in a different environment. As I've said previously, each skill acquired over my military and college career are my disciplines building blocks. As I think back over the course of my college career, I'm grateful for the opportunities to expand my knowledge base, for exposure to real world scenarios that allow me to practice critical thinking and clearly communicate common-sense solutions. And finally, for teaching me interdisciplinary theory, giving me the tools, I need to combine the expertise of disparate disciplines and bring them to bear in solving my employer's future cybersecurity problems.

References

Ralston, William. "The Untold Story of a Cyberattack, a Hospital and a Dying Woman." WIRED UK, 11 Nov. 2020, www.wired.co.uk/article/ransomware-hospital-death-germany

Koplowitz, Howard |. "Alabama Mom Claims Baby Died Because of Undisclosed Cyberattack, Fights for Hospital Records." Al, 1 Oct. 2021, Alabama mom claims baby died because of undisclosed cyberattack, fights for hospital records - al.com

"Ongoing Cyber Threats to U.S. Water and Wastewater Systems: CISA." Cybersecurity and Infrastructure Security Agency CISA, 20 July 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic Analysis of Ransomware. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2937641

Nobles, C. (2022). Stress, Burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA – Journal of Business and Public Administration, 13(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

Lubin, A. (2022, August 6). The law and politics of Ransomware. SSRN. Retrieved April 7, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4181964

Taddeo, M (2012). An analysis for a just cyber warfare. (n.d.). https://www.researchgate.net/publication/261488493_An_analysis_for_a_just_cyber_warfare

S.686 - 118th Congress (2023-2024): Restrict Act. https://www.congress.gov/bill/118thcongress/senate-bill/686.

"The Freedom of Information Act, 5 U.S.C. § 552." *The United States Department of Justice*, 21 Jan. 2022, www.justice.gov/oip/freedom-information-act-5-usc-552.