

Reflection Essay

Samuel Woodruff

Department of Cybersecurity, Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Sherron Gordon-Phan

August 17, 2026

Introduction

Throughout my time at Old Dominion University, my understanding of cybersecurity has developed beyond how computers work, how networks communicate, and how security tools operate. My coursework has introduced me to several different disciplines including the legal, social, technical, analytical, and ethical aspects of cybersecurity. By exposing me to these different disciplines, I was able to build a stronger overall understanding of cybersecurity and understand how each discipline contributes to solving cybersecurity problems. Through these different experiences, I've developed three primary skills that I believe will be particularly important for my career: technical research and communication, cybersecurity analysis and investigation, and risk analysis. The artifacts that I included in my ePortfolio help demonstrate how I developed these skills through different kinds of courses and assignments. Some of the assignments challenged me to learn unfamiliar technical concepts while others challenged me to research complex issues, analyze outcomes, and communicate technical information effectively. Reflecting back on these experiences, I can see now that while I felt I was completing individual courses at the time, each course across the disciplines fits together to establish the groundwork of my education. Together, these experiences have prepared me for a career in cybersecurity by not only teaching me how to understand technical concepts, but also how to research and communicate their significance, investigate potential vulnerabilities, and develop strategies to mitigate the risks they create.

Technical Research and Communication

The first skill that I believe I've developed strongly at Old Dominion University is the ability to properly perform technical research and communication. According to Ashley Furr of Boise State Online, "The ability to explain complex topics in a way others can understand is

another crucial facet of the soft skills needed to excel in cybersecurity” (Furr, 2025).

Cybersecurity professionals are often tasked with giving presentations and updates to individuals without the same technical knowledge, so it’s crucially important to be able to communicate ideas effectively. I will present over the next three artifacts how I was able to develop these skills throughout my time at Old Dominion University including what I learned, what challenges I faced, and how I overcame them.

Technical Research and Communication Artifact #1

For my first artifact representing my technical research and communication skills, I presented a slideshow centered around cybersecurity education and awareness. Researching for this assignment, I learned how crucial cybersecurity education is for not just organizations, but also individuals. According to Claire Reilly, RN MSc, Director of Clinical Operations at Imprivata, a survey performed around 2022 found that “Only 16% of health workers reported a clear understanding of phishing – demonstrating the least awareness relative to other industries surveyed” (Reilly, 2022). Statistics like this one made me consider how cybersecurity education may vary across the general population, particularly among those who have not received any formal cybersecurity awareness training. For that reason, I felt it was important to provide a slideshow on how cybersecurity awareness training is a continuous challenge that must be remedied to have a more secure society.

Technical Research and Communication Artifact #2

For my second artifact representing my technical research and communication skills, I provided an artifact of an essay I wrote concerning how artificial intelligence may be used for cybersecurity. By researching for this essay, I found that artificial intelligence will have many different uses for cybersecurity professionals to use in the future. Artificial intelligence could

accelerate monitoring of systems and provide a more thorough screening. At the same time, I discovered that cybercriminals may also use artificial intelligence to carry out malicious automated cyberattacks against organizations big and small. The most challenging part of this particular essay was finding concrete examples of these ideas in action since artificial intelligence is such a new realm of cybersecurity. I overcame this by using websites like Google Scholar to find good examples and sources to cite from with trusted information.

Technical Research and Communication Artifact #3

For my third and final artifact representing the skills of technical research and communication, I provided an essay I wrote investigating the potential cybersecurity vulnerabilities of the Neuralink implant. Neuralink is a brain chip interface (BCI) that is implanted into an individual, giving them the ability to remotely control devices like computers, mouse cursors, video games, and much more. I think that this essay helped me develop the ability to perform technical research greatly since the Neuralink implant is still very young in its development. I made sure to understand how the device works, what its components are, and how similar devices work in order to communicate the potential vulnerabilities that come with smart implants. Overall, I think this essay was one of my strongest in my time at college and I think represents my research and communication skills strongly.

Cybersecurity Analysis and Investigation

The second skill I believe I developed strongly in my time at Old Dominion University is the ability to carry out cybersecurity analysis and investigation. A majority of my assignments were centered around this skill, with me having completed numerous lab assignments over the past few years. The labs would vary in topic and complexity which challenged me to learn how

to operate different software, operating systems, and security tools. Overall, I think that this skill is one of my strongest and one of the most important for landing a job in cybersecurity.

Cybersecurity Analysis and Investigation Artifact #1

For my first artifact demonstrating my ability to perform cybersecurity analysis and investigation, I shared a lab assignment in which I cracked passwords using a Linux machine and Windows machine. I created user accounts with passwords of varying complexity, beginning with very simple passwords to moderately-strong passwords for each device. Using the Linux password cracking tool called Jack the Ripper, I was able to crack two out of three user account passwords in roughly ten minutes. I was also able to simulate a remote desktop protocol (RDP) exploit on a Windows machine, allowing me to remotely control the desktop and steal user account hashes. I then used the Windows password cracking tool called Cain and Able to perform dictionary and brute force attacks against the user accounts, which revealed the user account's passwords over the span of roughly ten minutes. The most challenging part of this lab was being able to set up the RDP exploit from a separate machine. After some time and a few more attempts, I was able to set up the RDP exploit correctly and successfully complete the lab. Overall, I feel like this lab helps demonstrate my abilities to carry out cybersecurity analysis and investigation greatly.

Cybersecurity Analysis and Investigation Artifact #2

For my second artifact demonstrating my skill to perform cybersecurity analysis and investigation, I provided a lab assignment in which I cracked various WiFi passwords in order to steal network traffic. Check Point explains that one of the primary targets for these kinds of attacks are public networks which then "...enable cybercriminals to intercept or manipulate data for various purposes, including credential theft, session hijacking, and malware injection"

(Check Point Software, n.d.). In this particular lab, I was provided snippets of network traffic presumably from a home network. I was then asked to crack the WiFi password in order to decrypt network traffic and perform a detailed traffic analysis. Overall, I was able to successfully crack each network's password and decrypt their individual network traffic. This lab assignment helped give me a better understanding of how network traffic is transmitted and how it is protected.

Cybersecurity Analysis and Investigation Artifact #3

For my third and final artifact representing my skill of cybersecurity analysis and investigation, I provided another lab in which I was tasked with performing steganography. This lab in particular was insightful because it asked me to differentiate between cryptography and steganography, helping me to understand the two topics' independent meanings. I thought that it was very interesting how steganography enabled me to hide bits of information inside of an image file. It reminded me of real life examples like false-walls and fake paintings which helped me connect to the topic more. Steganography was important for me to understand because cybercriminals might hide malicious information or incriminating evidence inside of image files like I did here.

Risk Analysis

The third and final skill I believe I developed strongly during my time at Old Dominion University was the ability to perform risk analysis. I was able to develop this skill through several assignments asking me to research various infamous cyberattacks throughout history and how they occurred. Not only would these assignments help me understand the causation of these cyberattacks, but they would also require me to think of ways to mitigate the vulnerabilities they

suffered from. The next three artifacts I share will help demonstrate my proficiency with this skill.

Risk Analysis Artifact #1

For my first artifact representing my skill of risk analysis, I provided an essay in which I researched the vulnerabilities and risks associated with the 2017 Equifax data breach. The Equifax data breach was one of the largest in all of history, resulting in millions of customers' personal data being exposed. In addition to the personal data being compromised, according to the Federal Trade Commission, Equifax was ordered to pay a settlement of "...up to \$425 million to help people affected by the data breach" (Federal Trade Commission, 2024). This breach ended up being one of the most costly and one of the most consequential in history. In the end, it was discovered that a known vulnerability located in one of Equifax's systems was the root cause of the attack. A patch had been released for the vulnerability for months before the attack occurred, making the event entirely preventable. The key takeaway from this artifact and the research from it is that risk assessments and analysis are extremely important. A thorough risk assessment and analysis could lead to small vulnerabilities being discovered which could prevent the next big cyberattack.

Risk Analysis Artifact #2

For my second risk analysis artifact, I included another essay in which I researched the cause of the MGM ransomware attack and resulting consequences. This particular cyberattack was interesting to me because it was one of the biggest examples of a successful social engineering attack. Specifically, this attack was carried out using a very specific kind of attack called "vishing". As defined by Cisco, vishing is "...short for voice phishing, uses fraudulent phone calls to trick victims into providing sensitive information, like login credentials, credit

card numbers, or bank details” (Cisco, n.d.). This attack shows that one employee has the ability to unintentionally “hand the keys” of a company over to cybercriminals. For that reason, it’s important to conduct risk assessments alongside having adequate cybersecurity awareness training.

Risk Analysis Artifact #3

For my final risk analysis artifact, I created a unique artifact based upon a real job posting I found online. The job posting is for a Cyber Security Information Assurance Specialist role that requires risk assessment/analysis as a mandatory qualification. Based on that requirement, I created a basic risk assessment for a fictional company so that I may demonstrate my risk analysis skills. The fictional company, called Shenandoah Technology Consulting Co., suffers from a relaxed security posture and has an overall weak cybersecurity culture. As a result, the company suffers from several different kinds of vulnerabilities with increased risks. I examined each vulnerability one by one and detailed recommendations I would make so that the company would be more secure. Overall, this new artifact I created made me critically think and present my knowledge in a unique way.

Conclusion

Looking back at my coursework and the artifacts included in my ePortfolio, I believe that I have developed a much deeper understanding of what it means to work in cybersecurity. Cybersecurity itself is a complex discipline that is built upon several other fields, and my time at Old Dominion University has shown me how they all come together. In addition to this, I have learned several valuable skills including but not limited to technical research and communication, cybersecurity analysis and investigation, and risk analysis. Developing my ePortfolio helped me catalog my experiences and pick out which ones I felt best represented my

work over the past few years. I feel as if the artifacts I selected help tell the story of my growth within my degree program and display my understanding of my major. As I look toward beginning a career in cybersecurity, I will carry the skills I've demonstrated in my ePortfolio forward and continue to build upon the foundations I formed at Old Dominion University.

References

Cisco. (n.d.). What is vishing? Cisco.

<https://www.cisco.com/site/us/en/learn/topics/security/what-is-vishing.html>

Check Point Software. (n.d.). Wi-Fi hacking: How it works, and how to stay secure. Check Point Software.

<https://www.checkpoint.com/cyber-hub/cyber-security/what-is-hacking/wi-fi-hacking-how-it-works-and-how-to-stay-secure/>

Federal Trade Commission. (2024, November). Equifax data breach settlement.

<https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>

Furr, A. (2025, May 23). The importance of soft skills in cybersecurity. Boise State Online.

<https://www.boisestate.edu/online/2025/05/23/the-importance-of-soft-skills-in-cybersecurity/>

Reilly, C. (2022, January 31). If 95% of cyber-attacks are due to human error, why have so few clinicians been trained to avoid them? Imprivata.

<https://www.imprivata.com/blog/if-95-cyber-attacks-are-due-human-error-why-have-so-few-clinicians-been-trained-avoid-them>

