Reflective Essay

Kunal Patel

Old Dominion University

IDS 493

Dr. Phan

December 9, 2025

Abstract

I will use a multi-disciplinary framework of Repko & Szostak (2020) to reflect how, through taking courses in Cybersecurity at Old Dominion University, I developed problem-solving, critical thinking, and technical skills. This reflection essay examines nine artifacts from coursework assignments, which all tested me in very different ways and forced me to create connections between concepts from ethics, law, psychology, computer science, business, and sociology. Problem-solving is evident in my problem-solving artifacts as they illustrate the steps I went through to disassemble complex problems and to approach problems from multiple perspectives before reaching a solution. Critical Thinking is evident in my critical thinking artifacts, illustrating how coursework impacted my ability to critically evaluate and think about cybersecurity laws, academic research, and ethical dilemmas. Technical Skills are evident in my technical artifacts, showing the "hands-on" technical skills that employers anticipate for an entry-level individual into the field of cybersecurity. Through reflecting on the nine assignments, I can clearly see how much I have grown and how interdisciplinary learning has positively affected my confidence and preparedness to enter the field of cybersecurity.

Introduction

At first, when I started to study cybersecurity, I thought it would just be technical – commands, tools, systems, and attacks. In reality, I have found that cybersecurity is so much larger than just technical. Through my classes at Old Dominion University, I was able to learn about the human side of cyber issues, in addition to learning about the ethical, legal, and organizational sides of cyber issues. This made me realize that protecting systems is not just knowing how to use tools but also understanding people's behaviors, motivations, laws, and business decisions. Through all of my courses, I have been able to develop and strengthen three major skills that are important to my development into a future cybersecurity professional: problem-solving, critical thinking, and technical skills. These skills were developed throughout many of the assignments and together reflect the interdisciplinary nature of cybersecurity. All job postings for positions such as SOC Analyst, Cybersecurity Technician, and IT Support Specialist consistently include these skills as requirements. This helps to give me confidence that my coursework will prepare me for the world of cybersecurity.

Problem-Solving Skills

Artifact 1- Entrepreneur Analysis (CYSE 494)

My entrepreneur analysis of Mark Zuckerberg was the first time I recognized how business decision-making can lead to cybersecurity problems. As I evaluated the business decisions Meta has taken throughout the years, I came to see that data misuse, misinformation, and privacy violations were not mistakes but a product of how company leaders make decisions based on both market pressure and also as a result of being ethically "blind." I had to use multiple lenses, including business, ethics, psychology, and technology, to evaluate and analyze this assignment. It taught me that solving cyber problems is not always about the technology used to solve them, but understanding the reasons behind the environment in which they exist, and therefore who created them. According to Repko & Szostak (2020), interdisciplinary problem solving involves breaking down a problem, evaluating it from multiple viewpoints, and then putting the pieces back together in a meaningful way. That is what I did. I have come to realize why so many job postings for cybersecurity positions say you will be required to "evaluate the organizational risk" because cyber problems are rarely a purely technical problem.

Artifact -2 The Rising Threat on the Internet (IDS 300W)

Writing my IDS 300W Final Research Paper was one of the most impactful assignments I have completed in my academic career. The paper allowed me to explore the many facets of cyber threats from law, social structure/ society, psychology, ethics, and technology. To understand why individuals are successful when using phishing attacks, I needed to use an understanding of psychology; to understand why laws related to cybercrime are unable to adequately address cyber threats, I needed to study the limitations placed on legal remedies; to see the effect of cyber threats on various communities I needed to think about them in a sociological context; putting all of the above into a single whole, led me to find a comprehensive solution by increasing educational requirements, updating current cybercrime laws, and utilizing better technology. This is an example of the heart of what it means to be interdisciplinary, according to Newell (2013). It was through this experience that I developed the ability to look at the "bigger picture," which is something that many cybersecurity job postings express as a requirement.

Artifact -3 Business Failure Analysis (CYSE 494)

When I did the My Blockbuster Business Failure Analysis, I found out a lot about how things didn't go as well as they could have, and when I started looking at this, I thought it was completely off topic to Cybersecurity, but the more I looked, the more I realized there were many similarities between technology being stagnant and having security vulnerabilities. Blockbuster went under because it didn’t evolve with the new technologies. Similarly, many companies today do the same thing; They fail to upgrade their systems and/or fail to make investments in security. As a result of doing this assignment, I have come to realize how closely all three areas (business decision making, innovation, and technology) are related. According to Klein (1990), interdisciplinary studies will show us relationships we wouldn't normally see, which is what happened for me. This artifact has also increased my capacity to identify organizational weakness — an area of need that is requested in nearly every Cybersecurity Governance/Risk Management job posting.

Critical Thinking Skills

Artifact -1 Cyber Law Writing Assignment (CYSE 406)

The Cyber Law assignment made me dig deep into the nature of digital rights, moderation in the digital world, and surveillance. I evaluated how the social media sites that we all use to express ourselves, balance our First Amendment right to free speech and our right to be protected from the harm caused by others' speech; additionally, I reflected on my own usage of the internet and how it compares to what scholars such as Schneier (2015), and Zuboff (2019) have written regarding the collection of our personal data and the increasing corporate control over our personal lives. The Cyber Law Assignment, in particular, made me evaluate the underlying ethics and legality that are often hidden in both the way people debate these topics and in the terms that people use when they do so. Many cybersecurity careers require a person to make judgments regarding an individual's right to privacy, as well as determining whether or not an organization is complying with federal laws and regulations. Therefore, this artifact will help prepare me for the mindset required in many of those types of roles.

Artifact -2 Article Review #1 (CYSE 201S)

The Article Review has aided my improvement as a critical reader/thinker. I was forced to critically assess the methodology of an academic study about cybercrime and evaluate the underlying assumptions of that study, as well as the potential social impact of it. I gained a better understanding of where, how data can be collected, who is being represented or not, and whether the conclusions drawn from that data are valid. The authors of "Critical Thinking Concepts & Tools" (Paul & Elder, 2014) place significant emphasis on Clarity, Logic, and Fairness in critical thinking, which were all utilized during my Article Review. I developed the skills to critically evaluate sources through the completion of this review, which is an important skill for a Cybersecurity Analyst to have when they must analyze and interpret threat intelligence and research in order to make informed decisions.

Artifact -3 Reflective Writing on Ethics (PHIL 355E)

The PHIL 355E ethics reflection I completed has allowed me to better understand the role of moral reasoning in the field of Cybersecurity. Through examining several different types of case studies related to issues such as whistleblowing, cyberwarfare, and professional responsibility through the lens of deontology and Just War theory, I was able to consider the potential outcomes from performing actions that are in gray areas. Taddeo (2012) states that ethical consideration is a fundamental aspect of cybersecurity due to the widespread effects digital action can have on others; this project has further enhanced my understanding of the ethical burden associated with Cybersecurity and why many job postings list "Ethical Judgment" as a requirement – it directly relates to our responsibility in protecting others.

Technical Skills

Artifact -1 Ethical Hacking Assignment #4 (CYSE 301)

I gained insight into the basics of penetration testing in this project. I realized how attackers identify vulnerabilities and obtain the required information. At first, it was a little difficult as the tools were foreign; however, getting past the error messages taught me patience and persistence, and I have a better appreciation for the mindset of both the attacker and the defender. Most SOC Analyst and Pen Tester job postings include reference to using vulnerability scanning and reconnaissance tools; this assignment provided me with basic knowledge in how to use these skills.

Artifact -2 Shell Scripting Lab (CYSE 270)

Shell scripting is one of the most rewarding things I have ever done; at first, I had difficulty with shell scripting, but writing and debugging my own scripts has helped me develop a much clearer logical thinking process and attention to detail. From this lab alone, I was able to learn about how using automation could be an extremely efficient way to save time and eliminate errors when performing tasks related to system administration and/or cybersecurity. Volonino & Robinson (2020) highlight that scripting is a major aspect of overall cybersecurity competency, and numerous entry-level job postings include requirements for Bash or Linux experience. As such, this lab has certainly provided me with a clear understanding of what to expect from this requirement.

Artifact -3 Password Cracking Assignment #5 (CYSE 301)

This project helped me gain insight into the vulnerabilities associated with authentication by creating a "hands-on" experience with the weaknesses of using poor-quality passwords. Understanding that it is so simple to crack weak passwords really helped make the need for organizations to enforce strict security policies a reality. This project was also helpful in teaching me how to interpret the data produced by password cracking tools, and therefore greatly improved my analytical abilities. As many cybersecurity job postings list as needed knowledge of various authentication systems and password auditing tools, this project provided me with the ability to gain skills that are directly related to an actual work environment.

Conclusion

Interdisciplinary learning using these nine artifacts shows me how the many disciplines I have used as a Cybersecurity major have impacted my development as a Cybersecurity Student. In order to solve cyber problems, one needs to understand: Human Behavior, Law, Ethics, Business Decisions, and Technical Systems. Solving problems showed me how to consider an issue from multiple perspectives before developing possible solutions. Critical Thinking allowed me to analyze and develop conclusions on very complex dilemmas using the confidence I developed by researching them thoroughly. The technical skills I acquired will allow me to take part in real-world environments where I will be able to apply what I have learned. The combination of these three skill sets (Problem-Solving, Critical Thinking, and Technical Skills) is the same skills listed in most Cybersecurity Job Listings, and it is reassuring to know that my classes have prepared me for this area of study. What was even more important than preparing me for the Cybersecurity industry was the process of building my Professional Identity—now I envision myself as a person who thinks outside of the box, acts with integrity, and approaches challenges with both technical knowledge and a true understanding of humanity. The process of Interdisciplinary Learning has not only prepared me for the Cybersecurity Industry but has also affected the way I approach each challenge I am presented with.

Work Cited

Klein, J. T. (1990). *Interdisciplinarity: History, theory, and practice*. Wayne State University Press.

Newell, W. H. (2013). *The state of the field: Interdisciplinary theory*. Issues in Integrative Studies, 31, 22–43.

Paul, R., & Elder, L. (2014). *The miniature guide to critical thinking concepts and tools*. Foundation for Critical Thinking.

Repko, A. F., & Szostak, R. (2020). *Interdisciplinary research: Process and theory* (4th ed.). SAGE Publications.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W. W. Norton.

Taddeo, M. (2012). Information warfare: A philosophical perspective. *Philosophy & Technology, 25*(1), 105–120.

Volonino, L., & Robinson, S. (2020). *Principles of information security*. Pearson.

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.