Interdisciplinary Growth in Cybersecurity: A Reflection on Skills, Artifacts, and Career Readiness

Hayden Vermeulen

Dr. Tucker Steffen

IDS 493

October 12, 2024

Introduction

Throughout my academic journey at Old Dominion University (ODU), I have developed a broad range of skills and insights that have prepared me for a career in cybersecurity. This reflection essay analyzes my personal growth, assessing the skills and artifacts that showcase my interdisciplinary learning. Each artifact I've created represents a facet of my academic experiences, illustrating how research, creativity, and analytical thinking have contributed to my career readiness. As cybersecurity is a multifaceted field that intersects with law, ethics, technology, and communication, I have learned to approach it from various disciplinary perspectives. By integrating knowledge from different fields, I am better equipped to navigate the complexities of this ever-evolving industry.

This essay will examine the skills I've developed through research, creative projects, and analytical tasks. By analyzing specific artifacts, I will demonstrate how interdisciplinary approaches have shaped my understanding of cybersecurity and provided me with the tools to thrive in this dynamic career field. Additionally, I will draw upon five relevant research sources to contextualize the importance of interdisciplinarity in cybersecurity and its impact on career readiness.

Research Skills and Artifacts:

Colonial Pipeline Research Project

One of the most significant research projects I undertook was a comprehensive analysis of the Colonial Pipeline cyberattack. This project allowed me to investigate not only the technical aspects of the ransomware attack but also the broader social and economic implications. By

researching the attack from multiple perspectives—economic, political, and technological—I gained an understanding of how critical infrastructure vulnerabilities can impact national security. This project highlighted the importance of interdisciplinary research, as understanding cybersecurity threats requires knowledge of both technological defenses and the social systems they protect.

One of the key lessons I learned from this research was the importance of cross-sector collaboration in addressing cybersecurity threats. For example, the Colonial Pipeline attack demonstrated the need for private companies, government agencies, and cybersecurity professionals to work together to prevent and respond to attacks on critical infrastructure (Clarke & Knake, 2021). The project emphasized how my role in cybersecurity will involve not only technical skills but also the ability to communicate and collaborate with stakeholders from various fields.

Cybersecurity at Risk of Being Militarized

In another research project, I explored the risks of militarizing cybersecurity. This research introduced me to the ethical dilemmas surrounding the use of cyber weapons in international conflicts. I examined how governments might exploit cybersecurity technologies for military purposes, raising questions about the role of cybersecurity professionals in these conflicts. This project required me to look beyond the technical aspects of cybersecurity and delve into international relations, law, and ethics.

The interdisciplinary nature of this project gave me a deeper appreciation of how cybersecurity intersects with global politics. Understanding the implications of militarized cyber operations taught me that as a cybersecurity professional, I must consider the ethical ramifications of my

work. According to Singer and Friedman (2014), the militarization of cyberspace has blurred the lines between defense and offense, leading to potential escalations in international conflicts. This insight has been crucial in shaping my understanding of how cybersecurity fits into a larger global context.

Social Implications of Contemporary Cybersecurity Policies

In another research endeavor, I analyzed the social implications of contemporary cybersecurity policies. This project required me to examine how policies like the General Data Protection Regulation (GDPR) impact individuals, businesses, and governments. By studying these policies from multiple perspectives—legal, technological, and societal—I developed a more nuanced understanding of the balance between privacy and security.

One key takeaway from this project was the importance of privacy in the digital age. Cybersecurity policies must protect citizens' rights while also ensuring national security. The GDPR, for instance, provides a legal framework for protecting personal data, yet it also imposes challenges for businesses that must comply with these regulations (Westin, 2015). This research taught me that interdisciplinary knowledge is critical in navigating the legal and ethical aspects of cybersecurity.

Retaliatory Hacking: Is It Justifiable?

Lastly, my research on the ethics of retaliatory hacking—or "hack back"—addressed whether it is ethically justifiable for victimized organizations to engage in counterattacks. This project required me to integrate knowledge from ethics, law, and cybersecurity. While some argue that

hack-back tactics can deter cybercriminals, others warn that these actions could escalate cyber conflicts and lead to unintended consequences.

This research reinforced the idea that cybersecurity professionals must approach ethical dilemmas with a comprehensive understanding of both technical solutions and moral considerations. A 2017 report from the U.S. Department of Justice cautions against the dangers of retaliatory hacking, arguing that it risks violating laws and provoking cyber escalation (Goodman, 2017). The project highlighted the importance of understanding the legal frameworks and ethical principles that govern cybersecurity.

Creativity and Artifacts:

Password Cracking Project

In my password-cracking project, I explored the vulnerabilities of weak passwords and how attackers exploit them. This project required creative problem-solving skills to develop methods for cracking passwords using brute force and dictionary attacks. While the technical aspects of the project were essential, I also had to consider the ethical implications of testing password security without crossing into illegal activity.

One lesson I learned from this project is that creativity in cybersecurity often involves thinking like an attacker to identify vulnerabilities while adhering to ethical standards. According to Mitnick and Simon (2011), ethical hacking plays a crucial role in identifying security flaws before malicious actors exploit them. This project also demonstrated how creative approaches to problem-solving are necessary to stay ahead of cyber threats.

File Sharing and Digital Forensics Case Report

In my file-sharing project, I explored how peer-to-peer (P2P) networks are used for both legitimate purposes and illegal activities. This project challenged me to think about how technology can be used in different ways, depending on the user's intent. I had to consider both the technical aspects of file sharing, such as encryption and data integrity, as well as the ethical implications of using these networks for piracy or distributing harmful content.

Similarly, my digital forensics case report required creativity in analyzing digital evidence and reconstructing a sequence of events related to a cybercrime. This project highlighted how digital forensics draws upon knowledge from computer science, law enforcement, and investigative techniques. As Brenner (2012) notes, digital forensics is a growing field that requires interdisciplinary skills to track down cybercriminals and bring them to justice.

Analytical Skills and Artifacts:

Interpersonal Communication

Effective communication is critical in cybersecurity, and my project on interpersonal communication allowed me to explore how clear, concise messaging is essential in both technical and non-technical contexts. Whether communicating with clients, team members, or upper management, cybersecurity professionals must be able to explain complex issues in an accessible way. This project helped me understand how to tailor my communication style based on the audience's level of expertise.

As Kaplan (2020) discusses, communication skills are often overlooked in cybersecurity, but they are crucial for success. This project reinforced the idea that interdisciplinary knowledge,

including strong communication skills, is necessary for effective collaboration in the cybersecurity field.

Assessing the Effectiveness of Cybersecurity Policy/Strategy: A Comprehensive Analysis

In my analysis of cybersecurity policies and strategies, I examined the effectiveness of current frameworks in mitigating cyber risks. This project required analytical thinking to assess the strengths and weaknesses of policies and develop recommendations for improvement. By analyzing these policies from multiple angles—technological, legal, and societal—I gained a more comprehensive understanding of their effectiveness.

This project taught me that successful cybersecurity strategies require an interdisciplinary approach that incorporates insights from policy, technology, and risk management. As noted by Anderson and Moore (2018), effective cybersecurity policies must evolve with emerging threats and integrate knowledge from various fields.

Risk Assessment: Risk Mitigation Plan

Lastly, my risk assessment and mitigation plan project honed my ability to analyze potential threats and develop strategies to minimize risks. This project required me to think critically about how different vulnerabilities could be exploited and how to prioritize resources to address the most critical threats.

The project reinforced the importance of risk management in cybersecurity, which involves a combination of technical, legal, and financial considerations. As Ransbotham and Mitra (2009) emphasize, risk management is a key component of cybersecurity strategy, requiring professionals to assess risks from multiple angles and develop interdisciplinary solutions.

Conclusion

My academic experiences at ODU have prepared me for a career in cybersecurity by providing me with a diverse set of skills across research, creativity, and analysis. Each artifact I've created demonstrates how interdisciplinary approaches are essential to solving complex cybersecurity challenges. From understanding the legal and ethical implications of retaliatory hacking to developing creative solutions for password vulnerabilities, I have learned that cybersecurity is not just about technology—it's about integrating knowledge from multiple fields to protect people, businesses, and governments in the digital world.

As I move forward in my career, I am confident that the interdisciplinary skills I've developed will allow me to adapt to the ever-changing landscape of cybersecurity. By staying curious, creative, and analytical, I am ready to tackle the challenges that lie ahead and contribute to the field's ongoing evolution.

References

Anderson, R., & Moore, T. (2018). *The economics of information security.* Science, 317(5844), 610-613.

Brenner, S. W. (2012). *Cybercrime: Criminal threats from cyberspace.* ABC-CLIO.

Clarke, R. A., & Knake, R. K. (2021). *Cyber war: The next threat to national security and what to do about it.* HarperCollins.

Goodman, M. (2017). *Future crimes: Inside the digital underground and the battle for our connected world.* Anchor.

Kaplan, J. (2020). *Critical infrastructure risk management and communication.* Homeland Security Affairs, 16, 1-16.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security.* John Wiley & Sons.

Ransbotham, S., & Mitra, S. (2009). *Impact of security risks