Reflecting on Lessons Learned During the Study of Cybersecurity

Gregory S. Oehm

School of Cybersecurity, Old Dominion University

IDS 493: Electronic Portfolio Project

Prof. Sherron Gordon-Phan

May 5, 2026

Abstract

This paper seeks to describe the knowledge and skills that I have gained during my time studying cybersecurity and how that might positively influence my future work in the field. To do so, each of the nine artifacts included within my ePortfolio are discussed. The information I gleaned from creating each artifact is described, alongside how they have influenced my thinking and outlook about certain topics in cybersecurity. Where applicable, the way in which an interdisciplinary perspective has benefitted me in thinking about the field, and how each artifact and the lessons obtained through it apply to certain kinds of cybersecurity positions, are also included.

Reflecting on Lessons Learned During the Study of Cybersecurity

During my time studying cybersecurity over the last few years, I have gained many important skills and knowledge of countless details related to cybersecurity. Among these are the technical knowledge of, and experience with, the processes and tools used within the field, the understanding of human error's importance to security outcomes and its mitigation through training and awareness programs, and the ability to utilize secure design practices in the creation of networks and facilities. These factors should, in all likelihood, be highly valuable when working in the cybersecurity field in the coming years. The development of my ePortfolio, and this reflection itself, can help to refine and reinforce this past learning, while communicating various facets of the knowledge I have gained during my studies. Several of these artifacts also help to demonstrate the interdisciplinary nature of cybersecurity, as an intersection between both people and technology, and the benefits this interdisciplinary perspective has offered me.

Roshambo Project and Its Relation to Programming Knowledge

The first artifact which I have selected to represent my more technical experience as it relates to cybersecurity is a presentation, which was based on a programming project I completed. In this project, I was able to create a working version of Roshambo or Rock, Paper, Scissors, in the Python language. This assignment served as the culmination of my knowledge of programming up to this point, with a major focus on socket programming, specifically. Socket programming can be used to allow two separate instances of Python to communicate or, in a wider context, used to allow two different devices to exchange information, and is thus a key process to focus on. Serving as a sort of combination of all lessons up to this point, this assignment included a variety of tools within Python. Though I would not say I possess enough knowledge of Python as a result of this class to consider myself an expert, I do believe that I am

familiar enough with it to create simple programs such as this and, perhaps, understand the operation of more complex programs made by others. Notably, this assignment, much like the class as a whole, did not just provide insight into how arguments and parameters are actually used within a given programming language, but in how code must be thought about in order to make a useful program. The skills developed throughout the course culminated in this kind of logical thinking. If code is strung together illogically, it can be highly difficult to work with, and may introduce errors to the program. Utilizing effective planning, ensuring that one's code remains as simple and modular as possible, and using appropriate labeling are all necessary principles to keep in mind to minimize difficulties in creating sound programs.

Malware Analysis and Thinking About Malicious Software

The second artifact chosen to showcase my technical knowledge and experience with the tools used in cybersecurity is a laboratory assignment in which malware analysis was conducted. There were numerous other software tools used throughout this and other classes, including Wireshark, Nmap, Steghide, and many more, but for the sake of brevity I have limited myself to just one, here. This assignment, in particular, made use of ANY.RUN, an online service used to investigate suspected malware. While static analysis, which entails simply looking at the code of a program, might be the most immediately intuitive way to detect whether it is malicious or not, obfuscation in an attacker's code might make this process difficult to complete accurately. Dynamic analysis in a safe environment, then, as allowed by ANY.RUN, helps to see if a piece of software is malicious by observing it in practice. This assignment focused on illuminating how the analysis of malware is performed, evaluating indicators of compromise to find if a piece of software is malicious or not and, if so, what it does. Looking at malware in this way, for me, has helped it to seem like less of a black box. Malware is simply malicious software, and can be

analyzed as such. This was something I had yet to do prior to this laboratory assignment, and thus I found it quite interesting to see how real malicious software acted and could be recognized. This has allowed me the capability to examine and identify potentially malicious software without solely relying on surface-level identifiers or known signatures through antivirus programs. The kind of critical thinking about malicious software encouraged by this assignment, then, is quite valuable, and should help greatly if a new and unknown program must be scrutinized at any point in the future. Such skills are needed for any cybersecurity job involving incident response, of which there are many (*Information Security Analyst II*, 2026).

Blockchain and Using Cryptography in the Real World

The third artifact focusing on my technical learning is a paper written on blockchain technology and its use in cryptocurrency. I had learned quite a bit about hashing and encryption algorithms across multiple of my courses, but these topics were discussed most thoroughly in my Cryptography for Cybersecurity course. Encryption and hashing are foundational processes to ensure the security of data, and are primarily used to provide the confidentiality and integrity of data. The course, as a whole, delved deep into a number of both public key and symmetric encryption algorithms, their strengths and weaknesses, and their use cases. These insights would later assist me in several of my other courses, such as those about ethical hacking and penetration testing, and the techniques and operations used by cybersecurity professionals, among others. This paper in particular, however, was also valuable because of its concentration on the application of cryptographic concepts in real contexts. This allowed me to examine how real businesses and individuals might use these technologies to support their operations beyond simply furthering data security, though that is of course by no means unimportant. To me, this highlighted the importance of these technologies and processes in a number of situations, and

was a valuable opportunity to examine the use cases and security of blockchain technologies. As a result, I feel as though I have a more comprehensive understanding of the situations in which these technologies can be best utilized.

Social Engineering and Understanding the Psychology of Users

The first artifact related to my skills in the more interpersonal side of cybersecurity, and the fourth overall, is a narrated slide presentation based around social engineering. This assignment, and the class it was a part of as a whole, gave me a more complete understanding of the psychology behind user behavior. Users often have an inherent trust in others, which could be exploited by attackers. Using personal information, the branding of a reputable organization, or simply talking to users directly can each increase their perceived credibility. The knowledge of many of the specific ways in which trust might be gained, and how countless kinds of social engineering attacks can be executed, were acquired or strengthened through my research for this presentation. Knowing each of these factors is necessary to help change the outlook of users and prevent these attacks from being successfully executed against both them and the organization as a whole. Notably, an interdisciplinary standpoint, as encouraged through prior coursework, is necessary to fully grasp this issue. Comprehending both the psychological factors that allow for social engineering, such as trust, agreeableness, and a lack of skepticism, alongside the technical results and potential human-centric mitigation strategies, has allowed me to form a more complete picture of this topic and its related solutions.

Mitigating Human Error Through Training and Awareness

The next artifact I have chosen is a paper I had written on some of the solutions available to mitigate human error's impact on security within organizations. This assignment and the class it was a part of focused on the human factor in security, reinforcing my understanding that

humans are the weakest link in the security of an organization. Importantly, it granted me a better awareness of some of the strongest methods available to mitigate the downsides human error can have in cybersecurity. Simply informing users about appropriate or inappropriate actions, while helpful, is not by itself enough to support security objectives in the long term. Apathy can be developed over time as a result of security fatigue and a desire to complete one's work as efficiently as possible, meaning that security can diminish over time, especially as the organization's threat landscape changes. Notably, I had not realized prior to this assignment and its related readings that workplace culture was so important to this goal. This supports secure behaviors by making them seem like the norm, and an objective in and of themself. Through this course, I acquired the knowledge of several psychological and social methods to encourage stronger security among employees and other users that could potentially be used in my future work, such as fostering real engagement with security objectives by connecting it to their everyday activities, utilizing routine training, creating physical media, and making use of other forms of awareness, each of which can help work to inspire a culture of security within an organization. These skills would be necessary to deliver the kind of training, education, and awareness programs as required by many positions in the field, including those in government agencies (*Information Security Specialist*, 2026). Again, understanding the psychology of others and the existing cultural landscape, using an interdisciplinary perspective, is needed to address the need for training and awareness in the best way. Building trust and good communication with employees and other users is a requirement to manifest a culture of security and compliance with organizational policies (Khadka & Ullah, 2025). Simply focusing on technical considerations will never allow human error to be appropriately mitigated.

Cybersecurity Workforce Management

The sixth artifact, overall, is a paper I created which examines the role of cybersecurity workforce management. The goal of this paper was to investigate a specific kind of cybersecurity position, in this case workforce management, and connect it to the social sciences and its related principles. The assignment granted me insight into sociology's place in cybersecurity management, including its use in understanding how cybersecurity workforce managers might use the social sciences to better understand user behavior and promote those behaviors which are most safe and reliable. To me, this also highlights the importance of people to the security of an organization, particularly in regard to its leadership. Naturally, managing the social landscape of an organization is essential for more senior cybersecurity staff within it to be effective leaders, as demonstrated by many job postings, but understanding the role of organizational leaders is crucial for all cybersecurity professionals, as well (*Manager, Security Operations Center*, 2026). Further, it strengthened the connection, for me, between cybersecurity and the social sciences, a connection which may otherwise seem somewhat abstract given that cybersecurity is often viewed as a more technical field. The policies of an organization and its people are just as impactful, if not more so, than the technical controls in place within the organization. Insider threats, for example, must be addressed with social and behavioral acts as opposed to technical controls alone, requiring an interdisciplinary outlook (Khadka & Ullah, 2025). Understanding the principles of the social sciences, then, can allow myself and others to better handle this critical facet of security.

School Ethernet Project and Network Design

The seventh artifact I selected was a design project for one of my networking classes in which we were tasked to identify the items that would be necessary to implement an effective network for a new hypothetical educational facility, specify how this network infrastructure

would be integrated, and determine the cost for each of these items. This gave me practical experience in designing a network for what could be a real facility, which I found to be quite informative, as I had not truly had experience with practical network design prior to this point. As a result, I gained an appreciation for the many factors that need to be taken into account when designing a network, such as the lengths of cables, their type, network devices that must be installed, the size of the building, the requirements of staff and user, and the budget provided for the network as a whole. I will be able to take several insights from this exercise with me in the future, and should be able to design more effective and secure networks as a result. Such skills would be a requirement in any job focused on the implementation of information systems, openings for which are not limited in both the public and private sectors (*Information Systems Security Engineer - Mid to Expert Level*, 2026).

Secure Forensics Facility Project, Physical Security, and Policies

The eighth artifact within my ePortfolio is somewhat similar to the previous network design project, but has some key differences. Much like the network design project, this too was a project related to the creation of a facility. However, it was focused more on physical security requirements and policies that must be in place for a digital forensics laboratory. This granted me an appreciation for the administrative effort that goes into ensuring the area is secure from attackers. This is especially crucial for a digital forensics facility, as outlined in the project, as any lapse in security could allow vital evidence to become inadmissible in court. As a result of this assignment, I am better able to understand the role of inventory, upkeep, and maintenance policies and procedures, the various kinds of physical security controls that can prevent attackers from accessing sensitive systems, information, and resources, and how these measures can be implemented most effectively.

Critical Infrastructure Systems and Promoting Adaptability in Design

The final artifact I have used in my ePortfolio is a paper focused on security in SCADA systems, which are used within many critical infrastructure facilities throughout the United States and the world. The creation of this paper was particularly valuable to me because it allowed for a better understanding of some of society's most important systems, being those in critical infrastructure, alongside the knowledge of how insecure many of them can be. These systems and networks were often not built with long term maintenance or future upgrades in mind, and are often highly vulnerable as a result. Though network segmentation can reduce the ability for attackers to access these systems, any mistakes that allow for an outside connection to the network can still be disastrous. Given this, I have taken with me the importance of future proofing and flexibility in design, rather than simply using what works at the current time. Going forward, I plan to work to allow for adaptability in the design of systems and network infrastructure, given that shifts, whether technological, societal, or simply in the organization itself, are constantly occurring.

Conclusion

As I have studied cybersecurity over the last handful of years, I have grasped many facets of cybersecurity and developed numerous skills related to it. Understanding numerous technical components, processes, and tools used to support security outcomes, the role of people in promoting organizational security and the ways in which human error can be mitigated, and how network infrastructure can be appropriately planned and designed are each highly advantageous results of this study. The insights allowed by interdisciplinarity, made necessary given cybersecurity's connection to both social and technological factors, prepared me by allowing me to see cybersecurity from multiple perspectives, combined into one holistic picture of the field. It

is crucial to think this way as, otherwise, one might miss key facets of security across all aspects of the organization, which might provide opportunities to attackers and lead to significant damage. As I pursue a career in the field over the coming years, I plan to continue to develop my skills, using the knowledge gained through the classes and artifacts shown here as a strong foundation.

References

Information security analyst II. (2026, April 25). GovernmentJobs. Retrieved May 3, 2026, from https://www.governmentjobs.com/careers/fairfaxcounty/jobs/newprint/5313435

Information security specialist. (2026, April 20). USAJOBS. Retrieved May 3, 2026, from https://www.usajobs.gov/job/865859500

Information systems security engineer - Mid to expert level. (2026, April 27). USAJOBS. Retrieved May 3, 2026, from https://www.usajobs.gov/job/866780800

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3). https://doi.org/10.1007/s10207-025-01032-0

Manager, Security Operations Center. (2026, April 14). USAJOBS. Retrieved May 3, 2026, from https://www.usajobs.gov/job/865166600