Reflection Essay

Johnathan Mack

Old Dominion University

IDS 493

Professor Phan

May 4, 2026

Abstract

The purpose of this reflection is to discuss how my academic, professional and military experience will prepare me for a career in cybersecurity. The ePortfolio has been organized around the three major skill areas that I believe will be essential to success in the field of cybersecurity including; technical problem-solving, professional communications, and leadership/responsibility. Each area includes artifacts from the aforementioned areas (education/certification/coursework/military/service/current employment) which support each of the areas. Examples of some of these artifacts include; CompTIA Security+ certification, Associate Degree from Tidewater Community College, networking assignments, cybersecurity writing assignments, resume, military service photo, experience as a Navy Information Systems Technician, Linux experience and current Department of Defense Work experience. All together they display my development as an individual and as a future cybersecurity professional. In addition, they demonstrate how all aspects of cybersecurity connect with technology, ethics, law, communication, business/risk management and human behavior. As I reflect upon my experiences, I can express how those experiences made me more confident, disciplined, skilled and better prepared to continue to grow in the field of cybersecurity.

Introduction

Beginning with my ePortfolio showing what I've become as a cybersecurity student, it shows the aspects of cybersecurity that I've grown into, which includes the technology (computers, network, etc.), but also the non-technical side of things such as communications, leadership, ethical considerations, accountability and problem solving for real world applications. A cybersecurity professional must be able to ensure protection of information, identify potential risks, communicate risk and concern to stakeholders and make informed decision on behalf of individuals and/or organizations. This connects to the National Institute of Standards and Technology Cybersecurity Framework, which explains cybersecurity through functions such as govern, identify, protect. Detect. Respond, and recover *(National Institute of Standards and Technology [NIST], 2024)*.

My ePortfolio will display various examples of my development through many different artifacts. The CompTIA Security+ certification that I completed during this time, networking projects/assignments that were required of me at TCC, my experience with Linux operating systems, my Associate's Degree from TCC, my cybersecurity writing assignments, resume, military service photo, my experience working as a Navy Information Systems Technician and my current employment as a Department of Defense employee are all examples of the academic, technical, professional, and leadership skills that I have developed. In addition to technical problem-solving skills; I have developed professional communication skills, leadership skills and responsibility.

In summary each one of the artifacts that I've mentioned above tell a portion of my story. Many of them reflect my technical knowledge while some reflect my discipline, professionalism,

communication skills and professional growth. Collectively they illustrate how both my formal education and life experiences have equipped me to pursue a career in the field of cybersecurity.

Technical Problem Solving

The top thing that I have learned from my educational and job history is that I can technically solve problems. The definition of technical problem solving within cybersecurity is using your knowledge, resources, and critical thinking to find out why something did not function correctly (the root cause), and then figuring out what you could do to correct or mitigate the problem. Technical problem solving is crucial in cybersecurity because cybersecurity professionals usually face threats, system failures, network connectivity issues, and end-user problems daily which all require quick and thorough thought and focus on detail.

As stated previously, one way that I demonstrated this was through earning my CompTIA Security+ certification. By obtaining my Security + certification, I furthered my education in the basics of cybersecurity; including types of threats, types of vulnerabilities, risk management, access control, and the operation of the security function. *CompTIA describes Security+ as a certification that validates essential skills for core security functions and a career in information technology security (CompTIA, n.d.)*. My Security+ certification is evidence that I have pursued additional training beyond that received during my formal education. Additionally, the items covered under my Security+ certification will connect directly to my future job goals as many Information Technology (IT) and cybersecurity jobs require a basic level of understanding in the areas of security and to be able to apply those principles in a practical manner.

Another item that supports my claim of having a technical problem-solving skill is the assignments I completed at school regarding Wireshark and networking. Those assignments allowed me to review the flow of data across networks and view how different devices communicate with each other. As part of my studies, I was also required to complete several assignments where I would utilize Wireshark to capture packets of data that were traveling over a network. When reviewing these packets, I was able to visualize how data was segmented and transmitted across a network. This gave me insight into how security professionals utilize similar tools to monitor network activity. Reviewing the flow of data and viewing how security professionals examine network traffic is essential prior to identifying malicious activity. *This connects to the "detect" function in the NIST Cybersecurity Framework because organizations need ways to identify possible cybersecurity events before they can properly respond to them (NIST, 2024).*

Lastly, the fact that I have worked on both Linux and have experienced technical-based work assignments are also examples of technical problem solving. Working with Linux has given me increased confidence in utilizing command line interfaces, troubleshooting, and working in technical environments. During my current and previous work experience, I have been tasked with resolving technical-related issues, supporting end-users, and analyzing various solutions to resolve technical related problems. Through the experience gained while working in such capacities, I feel increasingly more confident when interacting with computer systems and resolving errors.

Professional Communication

The second important skill I developed is the use of professional communication. Professional communication is important for all types of cybersecurity professionals as they have both technical expertise and will be required to communicate their findings. Communication does not necessarily mean being able to write code, develop a new tool, etc. In fact, a person may completely understand a specific security issue however; he/she may not be able to express that understanding to his/her manager, coworker, customer or team members. As such, good communication helps you create incident reports, document events, explain potential risks, and work together with your colleagues to help protect your company's assets. *The NICE Workforce Framework supports this idea because it provides a common language for describing cybersecurity work, knowledge, and skills across education and employment (Petersen et al., 2020).*

My Associate Degree (Associate in Science) from Tidewater Community College serves as one artifact supporting professional communication. By obtaining my associate degree prior to pursuing my bachelor's degree, I was building an educational base which provided me with the opportunity to enhance my writing, research, reading, and critical thinking skills. Since many of my cybersecurity course assignments involve expressing technical concepts to nontechnical audiences, enhancing my academic base through an associate degree has assisted me in developing those written expression skills which are so crucial to success in the field of cybersecurity.

As previously mentioned, the discussion posts and essays I wrote while enrolled in cybersecurity courses are also examples of professional communication. Writing these posts/essays allowed me to review various cybersecurity-related topics by providing analysis and responding to peers and

ultimately providing explanations of my views in an orderly manner. Examples of topics included data breaches, privacy concerns/risk analysis/social engineering, and security policies. The importance of professional communication is evident when reviewing cybersecurity issues, since most of them impact individuals/businesses/organizations rather than simply impacting computer systems.

Lastly, creating my resume and ePortfolio were additional artifacts which demonstrated professional communication. Creating a resume and ePortfolio taught me how to effectively promote my education, experience, and personal/professional development in addition to organizing and communicating my long-term goals. Additionally, completing these two documents served as an excellent reflection of my development as a student and employee.

Leadership and Responsibility

A third skill I developed was leadership and responsibility. Leadership and responsibility is an important part of working as a cybersecurity professional since we are trusted with our organizations' most sensitive systems, private customer or employee information, and critical organization data. As such, we need to be trustworthy, follow procedures, make informed decisions, and fully comprehend the ramifications of all our actions.

The picture of myself in uniform is one artifact representing this skill. This artifact is significant because it represents my time while serving in the Navy, which includes the discipline, teamwork, and accountability that I gained from my time in the Navy. While I was in the Navy, I came to realize how important it was to come prepared to work every day, complete your job accurately and on time, and take full responsibility for your position within a group/team. All

these values can relate to a career in cybersecurity since maintaining system reliability depends heavily on trust and accuracy.

As a Navy Information System Technician (IT), the skills and knowledge I obtained while working in this role also relate to leadership and responsibility. By being involved in technical roles related to information systems, I became aware of how crucial information systems were to our daily operations and ultimately mission accomplishment. Through working as an IT in this environment, I realized that technical work does not only involve computer use. Technical work involves supporting personnel; ensuring information is protected; and ensuring that systems function reliably.

In addition to my military experience, my current DoD work experience is an additional artifact that demonstrates this skill. My continued growth in responsibility, communication, and problem solving has been supported by working in a professional technical work environment. Additionally, my experiences have demonstrated how imperative it is to support users, adhere to the established security requirements, and consistently demonstrate dependability in mission-oriented environments. Overall, these artifacts clearly illustrate that my leadership and responsibility have continually improved throughout my combined military and civilian work experience.

Interdisciplinary Learning and Career Readiness

My educational background in cybersecurity has provided me the understanding that cybersecurity is a multi-disciplinary subject area. This means it combines technology with areas like law, ethics, business, communication, psychology and risk management. CISA

(Cybersecurity and Infrastructure Security Agency) also emphasizes cybersecurity education, training, and career development as important parts of preparing people for modern cyber challenges (Cybersecurity and Infrastructure Security Agency, n.d.). A cybersecurity incident usually doesn't simply exist as a technical problem. For example, while a data breach may include weak technical controls; it could negatively impact customer privacy, company reputation, legal obligations and financial losses. Therefore, cybersecurity professionals must consider the people and organizations impacted by their Security Decisions beyond what they see on their computer screens.

As shown by the artifacts in my ePortfolio, this multidisciplinary approach is reflected in many of them. The networking assignments and Security+ certification shown reflect my growth in the technical areas. The associate degree, writing assignments, resume and ePortfolio represent my growth in academic and professional communications. My military service, experience as a Navy Information Systems Technician and current Department of Defense work experience show my leadership, discipline and professional responsibility. These items collectively represent that I'm building the skills needed to become a well-rounded cybersecurity professional both technically and professionally.

In addition to preparing me for my career as a cybersecurity professional, these experiences have taught me that cybersecurity requires continuous learning due to the ever-changing nature of threats, tools and technologies. *This need for continuous learning is also reflected in the cybersecurity job market, where the Bureau of Labor Statistics projects information security analyst employment to grow 29 percent from 2024 to 2034, much faster than the average for all occupations (U.S. Bureau of Labor Statistics, 2025).* My academic foundation was the base upon

which my technical certifications were built upon. Additionally, my military and professional experiences have given me the discipline and confidence to move forward. In the future I will continue to build my skills in cybersecurity, Linux, network operations and security operations. As such my ePortfolio represents that I've developed through various experiences and I'll continue developing as a cybersecurity professional.

Conclusion

Overall, my ePortfolio demonstrates my growth as a cybersecurity student, as a veteran and as a future professional. The technical skills I have emphasized are technical problem solving, professional communication and leadership/responsibility. Technical problem solving is required for all cybersecurity professionals due to their need to be able to understand systems; communicate risk to stakeholders; protect information and provide solutions when making decision in a live environment. Professional communication is also very important as many organizations require cybersecurity personnel to clearly articulate issues with systems or networks, identify vulnerabilities, and effectively communicate to management why certain changes are necessary. Leadership and responsibility are also very important as cybersecurity personnel are often tasked with managing teams and projects and being accountable for the performance of those teams and project.

Each artifact I selected helps demonstrate my progress in several different areas. My Security+ certification, networking assignment, and Linux experience demonstrate my technical preparation. My Associate Degree from Tidewater Community College, cybersecurity writing assignments, resume, etc., demonstrate my educational progress and my development of professional communication skills. Military service photo, Navy Information Systems

Technician Experience and current Department of Defense Work experience demonstrate my discipline, leadership, and sense of responsibility.

When reviewing my experiences, I can easily see how they have contributed to preparing me for my future profession. My education provided me with knowledge around cybersecurity. My certifications give me confidence that I will be able to pass industry recognized standards. My military and professional experiences teach me accountability and discipline which are required in every day working conditions within the cybersecurity industry. Cybersecurity is an ongoing process where one must continually learn new technologies and techniques, use good judgment and adaptability to remain effective.

References

CompTIA. (n.d.). Security+ certification. *https://www.comptia.org/en-us/certifications/security/*

Cybersecurity and Infrastructure Security Agency. (n.d.). Cybersecurity training & exercises. *https://www.cisa.gov/cybersecurity-training-exercises*

National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). Workforce framework for cybersecurity (NICE Framework) (NIST Special Publication 800-181 Revision 1). National Institute of Standards and Technology. *https://csrc.nist.gov/pubs/sp/800/181/r1/final*

U.S. Bureau of Labor Statistics. (2025). Information security analysts. Occupational Outlook Handbook. *https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm*