Reflection Essay

Jessica Frimpong

Old Dominion University

IDS 493

Professor Prihoda

Date: May 8th, 2026

Introduction

My educational path allowed me to see myself and my working position in cybersecurity more clearly. The interdisciplinary studies program provided a chance for knowledge to be gathered from different areas while technical skills were improved. When the projects and research assignments in this collection of work are viewed, the growth of the individual becomes visible. Education showed that communication and ethical thinking have a connection to cybersecurity. Experts claim that the combination of these fields creates a better professional.

This reflection essay discusses the lessons gained during the creation of the items in this collection. The experiences in the program helped because leadership and problem-solving were practiced through many assignments. It has been observed that combining different fields of study helps a person understand cybersecurity challenges better. Cybersecurity is significant because the field requires a person to be adaptable when thinking about problems.

The Value of Interdisciplinary Learning

A major lesson learned in the educational institution is that cybersecurity does not belong to just one subject. In the past, cybersecurity was viewed as a field only for computers and coding. After more classes were taken, the realization came that the field includes law and business too. Many people believe that interdisciplinary studies help connect these different parts of life. The program assisted in seeing how these subjects function together in the real world.

The scholar Julie Thompson Klein explains that interdisciplinary learning helps students use knowledge from many fields (Klein, 1990). Complex problems are solved more effectively when different perspectives are used together. This idea is relevant because cybersecurity needs people who understand technology and human behavior at the same time. Experts claim that organizations look for individuals with these diverse skills.

Thinking about the collection of work helped me see how much progress was made in the educational institution. Every item in the collection shows a different skill that was learned by the student. It has been observed that some assignments made communication better while others improved technical problem-solving. These experiences shaped the student into a stronger cybersecurity professional.

Communication Skills and Personal Growth

The ability to talk to others became a strong skill during this time. At the start of the educational institution, confidence was not present when speaking in front of a group. Through written assignments and reflections, the way to share ideas was improved. Many people believe that expressing ideas clearly is a necessary way to show growth.

One specific item that shows this change is the Toxic Love and Familial Love presentation. Important lessons about teamwork were learned even though the topic was not cybersecurity. Information was organized by the group so that the audience could understand the

research. It has been observed that dividing responsibilities helps a team finish a project successfully.

During the development of this presentation, knowledge regarding the significance of audience awareness was obtained. Visuals and examples from films were included because these tools make the subject more relatable. Many people believe that making information accessible to various groups is the main purpose of communication. In cybersecurity, technical risks are often explained by professionals to individuals who lack technical backgrounds. This assignment helped with preparation for those types of professional interactions.

The Executive Team Reflection from CYSE 368 was an artifact that strengthened leadership and communication skills. Within a cybersecurity internship course, a reflection on teamwork and leadership was required. Experts claim that communication impacts the way teams stay accountable and productive. While writing this reflection, knowledge was gained regarding how communication influences collaboration.

A significant lesson from this artifact was seeing how teamwork becomes a struggle when communication is not consistent. Leadership and organization are considered vital when individuals work on technical projects. This reflection also allowed for a deeper awareness of personal strengths within group settings. Because security professionals work with teams during investigations and risk assessments, successful cybersecurity work depends on strong collaboration. It has been observed that teamwork becomes a difficult task when words are not clear.

Communication skills were also improved through the professional email artifact. Writing professional emails taught the method of maintaining professionalism while staying organized and clear. Many people believe that tone and structure influence professional relationships and the way people share information. Before entering the educational institution, the importance of professional communication in a working position was underestimated. Professionalism was taught through the practice of writing these messages.

According to the National Initiative for Cybersecurity Education, communication and teamwork are necessary skills in cybersecurity careers because professionals work with leadership teams, employees, and clients (NICE Framework, 2020). While reflecting on these communication artifacts, improvement was recognized in the way ideas are expressed. Experts claim that expressing ideas confidently is a requirement for professional growth.

Technical Skills and Problem-Solving

Growth in technical problem-solving and cybersecurity skills was another major area of development. Before the start of cybersecurity courses, limited experience with programming or networking tools was possessed. Experts claim that confidence in solving problems grows through hands-on projects and technical assignments. Technical problem-solving requires critical thinking when challenges arise.

One of the most difficult experiences in this portfolio was the Socket Programming project from CYSE 250. This project required the creation of a client-server application while the way systems communicate through networks was being studied. It has been observed that patience is a necessary trait when people solve technical issues. Programming concepts were applied to ensure the application functioned correctly.

During this assignment, a lesson was learned that problem-solving involves many moments of trial and error. Because the program did not always work correctly, the code was reviewed carefully to find the source of errors. Many individuals believe that a systematic approach is the best way to handle technical difficulties. This experience strengthened analytical thinking, and a stronger understanding of data transmission processes was gained.

The Cybersecurity and Infrastructure Security Agency explains that the comprehension of network systems carries great weight in cybersecurity because attackers often hunt for weaknesses in communication (CISA, 2023). When I looked back at this specific task, the observation was made that my technical self-assurance grew through active educational practice. Experts claim that the growth of a student occurs when hands-on tasks are completed.

The Traffic Tracing and Sniffing assignment served as another item that helped my technical growth. Network analysis was introduced to me by this task, and the movement of data through network systems was shown clearly. I discovered the methods that attackers use when they watch network traffic. Many people believe that security experts utilize those same instruments to find doubtful actions.

Ethical responsibility provided a significant lesson during this educational task. Even though tools for traffic analysis help cybersecurity, personal information worries are raised if the tools are used in a bad way. It has been observed that a balance between technical ability and moral choices must be held by security experts. Protection of people and information is included in the duties of cybersecurity when the work is done with care.

A big role in my educational process was played by the Linux Password Cracking project. The ways that attackers find weak passwords with dictionaries and brute-force attacks were explained to me during this challenge. My experience was gained while I used Linux command-line tools and looked for vulnerabilities. Many researchers argue that the examination of system vulnerabilities allows for better protection.

The necessity of preventative safety steps was taught to me by this specific artifact. Small weaknesses like weak passwords create large dangers for organizations and individuals. IBM's Cost of a Data Breach Report identifies compromised credentials as one of the leading causes of security breaches worldwide (IBM, 2024). It is often said that cybersecurity awareness prevents many problems. My appreciation for strong authentication was increased because I reflected on this work.

Cybersecurity Policy, Ethics, and Social Responsibility

My coursework assisted me to gain a better understanding of cybersecurity policy, ethics, and social responsibility. Cybersecurity was seen by me as a technical field only before I took these classes. I learned through detailed investigations that the choices made in cybersecurity touch governments and the whole of society. Experts claim that policy decisions change how the world operates.

My detailed investigation into cybersecurity frameworks demonstrates this growth well. The way organizations use structured frameworks to find risks was learned by me during this task. Planning and consistent standards are required by cybersecurity to improve safety. It has been observed that structured systems make security better for everyone.

The National Institute of Standards and Technology explains that cybersecurity frameworks help organizations strengthen risk management and improve resilience against cyber threats (NIST, 2024). A deeper understanding of how policy and technical safety function together was reached when I thought about this assignment. Many scholars believe that resilience is built through these frameworks.

The legal frameworks surrounding cybersecurity were the focus of another important assignment. Laws and regulations that govern personal information worries and data protection were studied in this work. My realization was reached that technical ability is not enough for a person in this working position. It is often claimed that security experts must know the law to do their work well.

Understanding was gained from this artifact that cybersecurity choices require a balance between protection and personal freedoms. Diverse political and social viewpoints influence the way nations create cybersecurity regulations and digital privacy. Because multiple perspectives required evaluation to see the wide effects of cybersecurity rules, critical thinking skills were made more robust during this assignment. Many people believe that cybersecurity choices require careful thought about social consequences.

Comprehension of the effect of cybersecurity on the community was increased by the artifact regarding social implications of legal frameworks. Technology influences the connection of trust between establishments and community members when topics like digital privacy and data protection are researched. It has been observed that digital privacy impacts the way individuals interact with technology.

Bruce Schneier explains that cybersecurity involves individuals, trust, and human behavior as well as technology (Schneier, 2015). Cybersecurity specialists have moral duties to the community, which was realized after reflecting on these policy-related assignments. These lessons expanded personal views because the importance of human impact was observed alongside technical protection. Experts claim that the human element remains a significant factor in any security strategy.

Career Readiness and Future Goals

Growth as a learner and an individual is recognized when looking back at the educational background. Professional preparedness was assisted by the interdisciplinary studies program which helped with the growth of communication, group cooperation, technical problem-solving, and critical thinking skills. Each artifact in the portfolio represents a learning experience which contributed to personal and professional progress. It has been observed that interdisciplinary studies provide a wide foundation for learners.

The importance of being adaptable is one of the largest lessons that were acquired. Because technology and threats continue to change, cybersecurity is a field that is constantly shifting. Researching information, analyzing problems, and adjusting to difficulties were learned through coursework and projects. These skills will assist the professional journey while the career progresses. Many people believe that adaptability is a vital trait in the modern workforce.

Confidence in personal abilities was also developed during this time. Doubt about the future and a lack of direction existed at the start of the educational institution experience. A passion for cybersecurity was discovered when projects were completed and challenges were overcome. Experts claim that self-reflection leads to greater professional certainty.

Technical knowledge alone does not provide full professional preparedness. Individuals who communicate well, cooperate with teams, solve problems, and think with logic are sought by those in a working position. Each of these areas was made more robust by interdisciplinary education. Meaningful contributions to cybersecurity environments are possible because

communication-based assignments, technical projects, and policy research were completed. It has been observed that employers value well-rounded professionals.

Conclusion

The academic journey has been a path of growth, learning, and finding personal purpose. Reflecting on the portfolio allowed for the recognition of how development and professional preparedness in cybersecurity were assisted by each artifact. Skills in communication, technical problem-solving, leadership, ethics, and critical thinking were gained through interdisciplinary learning. Many people believe that self-reflection is a key to academic success.

Lessons learned during the creation of these artifacts helped with the realization that cybersecurity is more than technical tasks. This field is a space that needs cooperation, adaptability, moral duty, and clear communication. Different areas of study were connected and applied to real-world cybersecurity challenges because the interdisciplinary studies program provided the opportunity. It has been observed that cybersecurity requires a holistic approach.

As preparation for graduation is coming, and the next stage of the professional journey feels ready to begin. Approaching challenges from many viewpoints and continuing to learn in a changing field was taught by these experiences. Uncertainty was changed into confidence and purpose by this journey. Progress that has been made brings pride while the future as a cybersecurity professional is anticipated. Many people believe that a strong educational foundation leads to a successful career.

References

(n.d.). CISA: Home Page. Retrieved May 8, 2026, from https://www.cisa.gov/?

Cost of a data breach 2025. (n.d.). IBM. Retrieved May 8, 2026, from https://www.ibm.com/reports/data-breach?

Cybersecurity Framework | NIST. (n.d.). National Institute of Standards and Technology. Retrieved May 8, 2026, from https://www.nist.gov/cyberframework?

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

NICE Framework Resource Center | NIST. (n.d.). National Institute of Standards and Technology. Retrieved May 8, 2026, from https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center?

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton.