E-portfolio: Reflective Skill Self-Assessment

Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Tucker

Isaiah Bagwell-Goines

10 October, 2025

Introduction

Self-reflection plays a critical role in the development and effectiveness of e-portfolios, enhancing metacognitive awareness and promoting deeper learning. As Cheng and Chau (2013) explain, e-portfolios serve as "metacognitive tools that enable students to plan, monitor, and evaluate their learning processes," ultimately cultivating individualism and lifelong learning. Within an interdisciplinary program such as cybersecurity, reflection becomes even more important because it connects multiple domains of knowledge, from technical problem-solving to communication or even analytical reasoning. Therefore, self-reflection within e-portfolios is not merely an assessment exercise but a transformative process or practice that allows learners to take ownership of their educational journey and develop adaptive, self-driven learning strategies/methods.

Throughout my studies in cybersecurity, I have developed core skills that are vital to success in the modern workforce: critical thinking, technical proficiency or programming, and communication/collaboration. These skills were developed through diverse experiences that utilized analytical reasoning, hands-on experimentation, and collaborative problem-solving. The artifacts I have chosen for this reflection represent key milestones in my academic and professional development, demonstrating not only what I have learned but also how I have learned it through persistence, curiosity, and interdisciplinary integration. As such, I will expound upon these skills in the latter sections and outline their significance in my personal and academic development.

Critical Thinking

Critical thinking has been one of the most fundamental skills I have developed throughout my academic coursework in cybersecurity. According to Paul and Elder (2014),

critical thinking involves the “art of analyzing and evaluating thinking with a view to improving it,” ergo, it is a process that supports intellectual discipline and reflective judgment. In cybersecurity, this skill translates into the capacity to identify patterns, question assumptions, and construct effective solutions to complex security problems.

CYSE 200T Analytical Paper

My first artifact, an analytical paper from CYSE 200T, titled *The Impact and Social Meaning of Cybersecurity*, represents my early development of critical thinking within an interdisciplinary framework. In this paper, I explored the social implications of cybersecurity technologies, such as the NIST Cybersecurity Framework, and analyzed how risk management and hacker motivation shape public trust and digital resilience. The assignment pushed me to move beyond technical descriptions of cybersecurity systems and instead examine how these systems influence, and are influenced by, behavior and societal structures. By critically evaluating both organizational policies and the psychology of cyber attackers, I learned to consider not only how security systems function but also why they matter. This exercise strengthened my ability to interpret technical frameworks through ethical and sociological lenses, which is an essential skill for cybersecurity professionals who have to anticipate both technological and human vulnerabilities.

ENGN 150 MATLAB Project

The second artifact, a MATLAB project from ENGN 150, marked a turning point in how I applied critical thinking in a technical context. Before that course, I had only basic exposure to coding, but learning MATLAB and C++ forced me to think logically and sequentially. Debugging errors and optimizing code required the same analytical reasoning that encompasses effective problem-solving in cybersecurity. As I became more comfortable with the syntax and

logical flow of programming, I realized that critical thinking extends beyond abstract reasoning; it also involves persistence, creativity, and the ability to approach technical problems from multiple angles.

CS465 Final Project

The third artifact, the ABC Inc. Ransomware Attack Analysis report from CS465, represented a culmination of these skills in a professional and interdisciplinary context. This assignment simulated a real-world cybersecurity incident, requiring me to analyze the company's infrastructure, assess vulnerabilities, and propose remediation strategies. It demanded not only technical expertise but also the ability to synthesize information across disciplines by combining business continuity planning and other human factors. By evaluating risk, prioritizing mitigation steps, and communicating findings clearly, I demonstrated an ability to apply critical thinking to a complex, pivotal scenario. This particular project shifted my thinking from a technical, cyber perspective through the integration of business and financial factors; essentially, placing my perspective in that of a professional in the cybersecurity career field.

Technical Skills

Continuing, technical proficiency forms the basis of my cybersecurity education and professional development. It is not only about writing efficient code but also about understanding the systems, data, and ethical responsibilities behind it. Through my experiences in courses such as CYSE 270, CYSE 420, and CYSE 450, as well as in my professional work with Red Hat Enterprise Linux (RHEL) systems at BAE Systems, I developed a decent technical foundation that connects theory to practice. These experiences illustrate how my interdisciplinary studies integrate programming, data science, and ethical security operations into a skillset that directly prepares me for a cybersecurity career.

CYSE 450 Encryption/Decryption Ransomware

In CYSE 450: Ethical Hacking and Penetration Testing, I designed a Python encryption and decryption ransomware simulation. This project was one of the most challenging yet rewarding experiences in my academic journey because it required a deep understanding of cryptography and ethical considerations. I created both an encryption program that simulated ransomware behavior and a decryption script capable of reversing the process. Developing both tools emphasized the importance of security ethics, specifically, demonstrating how technical ability must be balanced with responsibility and awareness of potential misuse. The project also built upon my earlier programming foundation in C++ and MATLAB, which helped me approach the problem logically. Understanding data types, syntax, and debugging from those prior experiences made it easier to structure code, manage file I/O, and implement key-handling logic in Python. This progression reflects metacognitive growth by recognizing how prior knowledge shaped my approach to a new challenge. It also demonstrated interdisciplinary learning via the combination of principles like computer science and cybersecurity ethics to produce a functioning tool.

CYSE 420 Machine Learning Model

In CYSE 420, I created a logistic regression model in Python using an 80/20 training-test data split to determine whether network traffic was benign or an attack. This artifact strengthened my understanding of how machine learning intersects with cybersecurity analytics, an interdisciplinary field combining statistics, computer science, and network security. Using Python's scikit-learn library (Pedregosa et al., 2011), I learned to preprocess datasets, extract network features, and evaluate performance with metrics such as precision, recall, and F1 score. More importantly, this project taught me how to interpret data meaningfully by understanding

not just whether the model was accurate, but why it performed that way. The process of parameter tuning and feature selection deepened my analytical reasoning and prepared me for cybersecurity roles that increasingly depend on data-driven decision-making. This experience aligns directly with NIST's NICE Cybersecurity Workforce Framework (2020), which identifies data analysis, automation, and applied AI as key workforce competencies for cybersecurity professionals.

CYSE 270 Bash Scripting

Finally, the Bash scripting projects from CYSE 270 represent another essential piece of my technical foundation. My previous experience with Linux at BAE Systems, where I regularly worked with RHEL, significantly influenced my understanding of system operations and command-line efficiency. That hands-on experience made it easier to adapt to scripting for academic projects, reinforcing the value of experiential learning. Each script I wrote strengthened not only my technical accuracy but also my ability to think procedurally by anticipating potential failures and validating input. These are important facets of professional practice that extend beyond the coursework.

Collaboration & Communication

While technical knowledge forms the backbone of cybersecurity, it is communication and collaboration that help ensure those skills translate into success. In a field defined by teamwork, coordination, and the ability to communicate complex technical findings clearly, these soft skills are paramount. As the ISACA (2023) report on cybersecurity workforce development emphasizes, effective collaboration enhances problem-solving efficiency, reduces operational risk, and ensures that technical solutions align with organizational goals. Throughout my academic and professional journey, I have strengthened these skills through experiences that

required cooperation, adaptability, self-discipline, and leadership, which are reflected in three key artifacts that demonstrate how I have grown as both a communicator and collaborator.

BAE Systems EOTY Award

The first artifact, my Employee of the Year award from BAE Systems, is a tangible representation of professional recognition for teamwork and commitment. This award was given in acknowledgment of my consistent contributions to maintaining and configuring critical government systems, work that required not only technical expertise but also strong interpersonal communication, coordination with senior engineers, and trustworthiness in handling sensitive information/operations. Although the specific nature of these systems cannot be discussed in detail due to their classified/sensitive context, the recognition reflects my ability to apply technical precision collaboratively within a mission-critical environment. I regularly coordinated with multidisciplinary teams to troubleshoot complex network and hardware issues, document procedures, configure systems/equipment, and ensure compliance with security protocols. These interactions taught me that effective communication in cybersecurity is as much about clarity and accountability as it is about technical fluency. The experience also reinforced the importance of emotional intelligence, specifically, responding professionally under pressure and maintaining situational awareness in a professional setting.

PHYS232N Collaborative Experiment/Lab

My second artifact, a collaborative Coulomb's Law experiment from PHYS 232, represents my early experience with teamwork in a scientific and analytical context. This project required close coordination with classmates to design and conduct an experiment measuring the electrostatic forces between charged particles. My role involved collecting data, performing calculations, and helping to add the findings/information to a final lab report. Through this

collaboration, I learned to connect theoretical physics concepts with applied problem-solving, thereby strengthening the interdisciplinary thinking that later shaped my transition into cybersecurity. Above all, this artifact taught me that effective collaboration requires both technical understanding and the ability to construe data into a collective understanding, a skill equally vital in communicating security risks to non-technical colleagues/peers.

ENGN150 Encryption/Decryption Video

The third artifact, a C++ encryption and decryption demonstration video created during ENGN 150, highlights how communication and collaboration extend beyond group work as they also encompass peer mentoring. After completing an encryption/decryption project, I recorded a walkthrough video explaining my approach to syntax logic and debugging to help classmates struggling with similar issues during the assignment. This artifact displays my initiative to facilitate collective learning, reflecting both technical comprehension and the interpersonal motivation to support others' understanding. In the process, I developed greater confidence in articulating technical information clearly and concisely, which is a skill that has since proven paramount when presenting technical information and collaborating across teams in my current role. This act of helping others also illuminated an interdisciplinary insight that communication can be used as an act of problem-solving that links human understanding and technical execution.

Conclusion

Looking back on my academic and professional experiences, I can see how my growth in critical thinking, technical proficiency, and collaboration has shaped me into a better cybersecurity professional. Each skill builds on the other as critical thinking helps me analyze problems, coding allows me to implement practical solutions, and communication and

collaboration ensure those solutions are clearly shared and effectively applied within a team. My interdisciplinary education connected concepts from computer science, engineering, and behavioral studies, teaching me to see cybersecurity as both a technical and human-centered field. These experiences have also strengthened my ability to adapt, communicate, collaborate, and approach challenges ethically and analytically. Whether developing code or coordinating with others on systems, I have learned that success depends on both technical skills and collaboration. Moving forward, I will continue to apply these skills to protect systems and contribute to the field of cybersecurity.

References

Cheng, G., & Chau, J. (2013). Exploring the relationship between students' self-regulated learning ability and their eportfolio achievement. *The Internet and Higher Education*, *17*, 9–15. https://doi.org/10.1016/j.iheduc.2012.09.005

Marinkovic, J. (2023, October 9). *The Shifting Importance of Soft Skills in a Time of AI Systems, Large Language Models and Global AI Regulations*. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/the-shifting-importance-of-soft-skills-in-a-time-of-ai-systems

Paul, R., & Elder, L. (2014). *The Miniature Guide to Critical Thinking Concepts and tools*. The Foundation for Critical Thinking.

Pedregosa, F., Thirion, B., Michel, V., Gramfort, A., Varoquaux, G., Prettenhoffer, P., Blondel, M., & Grisel, O. (2011). Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research* , *12*(2011), 2825–2830. https://jmlr.org/papers/volume12/pedregosa11a/pedregosa11a.pdf

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework)*. https://doi.org/10.6028/nist.sp.800-181r1