Interdisciplinary Reflective Essay

Ayoob Ibrahim

IDS 493

Professor Andrews

June 23, 2025

Reflective Essay: Integrating Interdisciplinary Skills for a Cybersecurity Career

Introduction

As I complete my undergraduate degree in Cybersecurity with a minor in Information Technology, I have come to appreciate the extensive array of interdisciplinary skills that I have developed. The skills have shaped my academic path and prepared me to excel in a constantly changing career in cybersecurity where communication, cybersecurity knowledge, and systems thinking are necessities. By completing coursework in writing, IT, and cybersecurity, I built more than a technical skill set. In this essay, I analyze the way my number one, two, and three skills in communication, cybersecurity knowledge, and information technology and systems were constructed through interdisciplinary education, as indicated by selected artifacts. These abilities closely correspond with what employers seek in IT and cybersecurity professionals and have provided me with confidence to pursue challenging careers within a constantly evolving digital landscape.

Ability 1: Communication

Artifacts: Annotated Research Project, Death Penalty Research Paper, Skills & Job Ad Worksheet

Disciplines: English Composition, Research Writing, Career Development

Effective communication is an essential skill in any field, especially in cyber security where threat description, incident reporting, and collaboration are on a daily basis. Throughout my university experience, I developed communication skills through research writing as well as professional self-reflection. Through the Annotated Research Project and Death Penalty Research Paper, I became accustomed to critically reading sources, constructing arguments, and expressing thoughts of high sophistication with clarity and intent. These assignments, grounded in disciplines like criminal justice and rhetoric, taught me how to support ideas with thorough evidence without prejudice skills necessary for creating significant reports, writing security assessments, or contributing to white papers when employed in cybersecurity. I also discovered the value of toning down and varying my language based on my audience, reflecting the way that a cybersecurity analyst would report technical results differently to executives than to IT staff. The Skills & Job Ad Worksheet reinforced my sense of how to match personal strengths with career opportunities. It also required clear written communication to explain why I would be a good fit for a real job posting—similar to cover letter writing or performance reviews in the business world. This task also had me determine the most valuable soft skills employers look for, such as being flexible and being able to work under time pressure, and forced me to explain how I obtained them in the classroom and in the workplace. Across all three artifacts, I had to think critically, organize information in a logical manner, and write clearly skills which started with writing-intensive coursework and now carry over directly into the professional environment. This skill at communicating will be essential when creating cybersecurity documentation, writing up incidents, or delivering risk assessments to non-technical stakeholders. Employers always specify strong verbal and written communication as important requirements in job advertisements, and my educational history has directly prepared me to meet that demand.

Skill 2: Cybersecurity Knowledge

Artifacts: Two-Factor Authentication Setup Guide, Random Password Generator Project, How to Spot a Phishing Email Guide

Disciplines: Cybersecurity Fundamentals, Ethical Hacking, Public Education

My second major skill, cybersecurity knowledge was built through a combination of technical learning and applied assignments that mirror real-world responsibilities. Each of the artifacts I've selected reflects not just theoretical understanding, but the ability to apply cybersecurity concepts in practical, user-focused ways. The Two-Factor Authentication Setup Guide made me distill a key security principle into step-by-step instructions, making it accessible to a non-technical crowd. This meant using both technical knowledge and communication techniques illustrating the necessarily interdisciplinary nature of cybersecurity education. With human mistakes frequently holding the key to security breaches in modern times, having the ability to educate others is a highly desirable skill. For the Random Password Generator Project, I applied programming competencies to create a secure password generating utility. This artifact illustrates the intersection of cybersecurity and computer science as well as software engineering. Even writing out the code reinforced lessons about input validation and randomness, two basic tenets of secure system design. The project also gave me the opportunity to practice debugging and error handling skills, central to cybersecurity engineering careers. Finally, the Phishing Email Guide taught me how I could take cybersecurity threats and simplify them into concrete, actionable suggestions. It compelled me to read real phishing emails and summarize patterns demonstrating analytical, pattern-matching, and public knowledge skills. I also connected this guide with recent high-profile phishing cases reported by the news, so that I could talk about cybersecurity in a current and relevant sense.

These three projects prove that my cybersecurity knowledge transcends book theory to real-world, user-based learning. Because hiring notices for cybersecurity roles consistently mention phishing prevention, password safeguarding, and training end-users as key duties, these projects adequately prepare me to meet those needs. Even more importantly, these exercises illustrated how security is in everyone's hands and how much education and thoughtful design can determine security success.

Skill 3: Information Technology and Systems

Artifacts: IT Case Analysis, AI Chatbot Assignment, Office Network Plan

Disciplines: Systems Design, IT Management, Programming

My third key skill is information technology and systems, the skill of knowing how to understand, create, and debug interdependent digital ecosystems. This is an essential skill for anyone working in an IT or cybersecurity role and is a product of cross-disciplinary learning in the fields of information systems, logic, and infrastructure planning. In IT Case Analysis, I applied problem-solving frameworks to examine a real-world business IT scenario. The project forced me to examine like a systems analyst, specifying problems and proposing structured alternatives. The case format emphasized communication, analysis, and technical planning skills for any help desk support, IT consulting, or risk management position demands. It was the first project where I came to fully understand how abstract IT concepts become real business impacts. The AI Chatbot Assignment asked me to think about system interaction, user activity, and process mapping. I designed use case diagrams, activity flows, and specified nonfunctional requirements (e.g., speed and security), drawing on principles of programming, user experience, and systems design. This artifact shows my understanding of both the internal workings of systems and how to represent their function using industry-standard diagrams. I was also able to include ethics and data privacy concerns, showing how IT professionals have to consider legal settings like GDPR when creating new technology. The Office Network Plan helped me advance my technical abilities in a practical way. I designed a full internal office network for a fictional office using diagram tools. It incorporated information from IT infrastructure, logical planning, and visual communication. This project shows how I can design working systems when it comes to layout, user needs, and expandability in the future. This project enabled me to know the relationships between physical hardware, logical architecture, and organizational needs. Collectively, these artifacts show I am prepared to work, safe, and describe complex IT systems. These are the kinds of abilities employers seek in junior analysts, technicians, and support engineers. As security and IT systems grow more complex and integrated, those individuals able to communicate across layers from hardware to software to business impact will become more valuable.

Conclusion: The Power of Interdisciplinary Learning

The interdisciplinary nature of my academic experience has been essential to my growth not just as a student, but as a future cybersecurity professional. Each skill I've developed communication, cybersecurity knowledge, and systems thinking was strengthened through exposure to multiple disciplines, from writing and logic to programming and network design. Courses like IDS 300W also taught me to write plainly to diverse audiences, a skill I employed in technical writing and instructional guides. I learned technical expertise through my IT and cybersecurity courses, but also learned to think about user needs, system architecture, and legality implications. Even unrelated disciplines, even research writing or researching social problems, gave me ways of reasoning critically, arguing persuasively, and collaborating effectively. Understanding how domains overlap has allowed me to work on cross-functional teams, to communicate across departments, and to resolve complex issues with ease. Whether building a secure application, explaining a phishing attack to a non-tech end-user, or mapping a company's network, I now have the expertise to bridge the knowledge chasms and get the job done. Cybersecurity threats are interdisciplinary so must our skills. I learned in this program to learn, adapt, and apply between boundaries, and I believe that mindset is one of the most valuable things that I can contribute to the field. Seeking to move my career forward in cybersecurity, maybe in AI security or threat intelligence, I can surely say that I am prepared to make an impact due to the interdisciplinary knowledge that I have gained.