4/27/2026

Interdisciplinary Approach to Cybersecurity

Reflecting on my education

Kyle Sershon
IDS 493

My academic coursework and experience at Old Dominion University have given me the opportunity to build on my previous education from my associate's degree in information systems and my career in information technology. Hands-on experience in lab environments, cybersecurity technology analysis, social sciences, and criminal justice has provided a well-balanced interdisciplinary experience.

As part of an interdisciplinary program, I have learned to analyze cybersecurity through multiple lenses. The ability to analyze current social issues in cybersecurity, including ethical concerns, enables me to view cybersecurity through a sociological lens. Understanding how and why people engage in deviant behavior, the laws governing cybersecurity, and the technical skills of digital forensics help integrate the criminal justice discipline into cybersecurity. Cybersecurity technical labs across various systems, combined with basic programming skills and policy analysis, have provided me with a third pillar of skills for succeeding in a cybersecurity role throughout my career.

The holistic approach in this interdisciplinary program has been insightful regarding cybersecurity and the different avenues I can pursue in my career. My e-portfolio showcases my skills across disciplines and their application to cybersecurity. As I continue my career in information technology, I will apply these skills to help solve critical problems, support secure infrastructure, and analyze the challenges society faces in a constantly changing technological environment.

One of the most valuable skills I developed during my coursework is analyzing cybersecurity through a sociological and economic lens. Understanding how technology impacts society is important because it touches every aspect of modern life. As technology rapidly evolves, it has changed society through social media, artificial intelligence, and how we work and live. There are now generations that have grown up with constant internet connectivity. The integration of technology in grade schools has reshaped the way our children learn.

Cyberbullying, privacy concerns, and ethical responsibilities regarding organizational data collection and protection are problems to consider when approaching current challenges we face as a society. Having a foundational understanding of how technology works in our society provides a perspective that is beneficial when communicating with people throughout my career. Being able to clearly communicate the risks we all face helps create proper cyber hygiene and a strong security posture with my employer and throughout my community.

Since the largest vulnerability in any environment is “The human factor,” it requires close and careful analysis. Communication through technology provides people with constant access to massive amounts of information. Engagement is sold to advertisers as a commodity, driving the social media economy. Companies study human behavior closely to keep people engaged, and criminals exploit it to gain an advantage in attacks. Understanding that helps me think beyond the technical side of cybersecurity. It helps me focus on better policies, clearer communication, and practical security awareness for coworkers and the community.

Another skill I developed was understanding cybersecurity from a criminal justice and legal perspective. During my coursework, I explored how laws, regulations, and investigations relate to cybercrime. This included topics such as, digital evidence, legal responsibilities, jurisdiction, and evidence custody, as well as the proper processing of evidence at a crime scene to maintain integrity and authenticity. Cybersecurity is not only about protecting systems, but also about making sure I operate within legal boundaries.

The artifacts in my portfolio demonstrate the skills I apply to my digital forensics and cyber law assignments. In digital forensics, I focused on how evidence is preserved, collected, and processed to maintain authenticity and integrity. This required strict attention to detail and following proper procedures to avoid mishandling or contaminating evidence in a case. It also helped me understand what would be required to provide testimony as an expert witness. In cyber law, my assignments included topics such as whistleblowing, cyber warfare, and ethical considerations in cybersecurity. In addition, it helped me understand legal frameworks and ethical decision-making. I was required to analyze complex situations and the legal consequences and ethical responsibilities related to international privacy laws and cyber warfare, as well as criminal law in relation to computer crimes.

Sharpening these skills has strengthened my ability to approach cybersecurity incidents from a wide perspective. It helps me understand why an attack might occur and the legal ramifications of a breach for an enterprise or national security. It will benefit me as I move forward in my professional career and make decisions that help my organization. Having this experience helps me proficiently handle incident response, conduct threat analysis and

investigations, and help design and recommend policies that align with my employer's responsibilities to the public regarding data and bolster our overall cyber defenses.

During my degree, I developed technical skills essential to a career in cybersecurity. Through courses such as “Linux Systems for Cybersecurity”, “Windows System Management and Security”, and “Cyber Security Techniques and Operations”, I gained hands-on experience with various systems and network configurations, as well as security controls. This provided foundational knowledge on how systems communicate, network topology, and how systems can become exploited. I explored various protocols and how they are used for communication between systems around the globe.

I demonstrated my skills in technical labs, including network hardening, penetration testing, and simulations. I worked with firewalls to understand how network traffic is filtered and how rules protect systems. Understanding both offensive and defensive perspectives is important to identify how an attacker can exploit a system and to create rules and policies that reduce the network's attack surface. I spent time learning about various attack types and payloads, including malware, botnets that conduct DDoS attacks, and physical security.

It was beneficial to work across multiple systems to understand how each operates and its unique vulnerabilities. Network labs reinforced the importance of proper configuration and monitoring while providing hands-on practical experience. It also helped strengthen my troubleshooting skills with simulated environments. A combination of all the knowledge gained helped me achieve exceptional performance during my internship, where I was able to apply all the skills I had learned over my degree and career.

My experience in the interdisciplinary cybersecurity program enabled me to develop a holistic, unique skill set that draws on technical knowledge, legal understanding, and human behavior as they relate to technology. Taking courses across multiple disciplines gave me the opportunity to view challenges through different lenses and adopt approaches from different perspectives. Engagement in my coursework required proper discipline and an open mind to analyze topics effectively. Courses like "Interdisciplinary Theory" were critical in strengthening my critical thinking skills as I approached challenges that required consideration of multiple disciplines.

A career in cybersecurity requires strong technical skills and a foundational knowledge of networked systems. Just as important, though, is the understanding of how technology impacts all of society. Generations are now growing up connected to the internet in some form earlier than ever, and social media has provided an avenue for cyberbullying and other mental health challenges for children. Fortunes are being made from the collection and sale of individual data, and privacy concerns are more highlighted now than ever. Cybercrime is a multibillion-dollar industry that faces many challenges that traditional crime does not, which targets everyone. Even now, as new technologies become mainstream, such as generative artificial intelligence, more sophisticated cyber attacks are emerging. Quantum computing's emergence will rewrite fundamentally how we approach security policies and protocols. These topics highlighted the kinds of challenges I will need to consider for my career and future education. To properly approach and solve these problems, we must understand and explore all avenues of human behavior and technological advancements. Interdisciplinary approaches to

cybersecurity are essential in this sense and have provided me with a solid foundation to continue my journey in cybersecurity.