Reflection

Elliot Mason

Old Dominion University

Dr. Mary Ann Kozlowski

IDS 493

May 6, 2026

Throughout my academic journey at Old Dominion University, I have developed interdisciplinary skills that combine cybercrime studies, criminal justice, cybersecurity, research analysis, networking, and communication. As a Cybercrime major with a previous degree in Criminal Justice, I have learned that modern cyber investigations require far more than technical knowledge alone. Professionals in this field must understand criminal behavior, investigative methods, cybersecurity strategy, communication, and organizational planning. My coursework and experiences helped me build skills that support my long-term goal of working in investigative and forensic-focused cybercrime roles, particularly involving online crimes against children and digital investigations.

This portfolio demonstrates three primary skillsets developed throughout my degree program: Cybercrime Investigation and Threat Analysis, Risk Management and Security Strategy, and Technical Communication and Operational Planning. These skills were selected after analyzing cybersecurity and investigative job postings during coursework assignments and identifying the competencies employers consistently seek within the field. Employers in cybersecurity increasingly value analytical thinking, communication, adaptability, and leadership alongside technical abilities (Finley, 2021). The artifacts included throughout this portfolio demonstrate how my coursework, research, and interdisciplinary learning experiences prepared

One of the most significant projects included in my portfolio is my white paper on child cyberpornography and online sexual exploitation. This artifact reflects both my research abilities and my long-term career interests. The project required extensive research into online exploitation statistics, investigative practices, offender behavior, and the role organizations such as the National Center for Missing & Exploited Children play in combating online exploitation. Completing this project strengthened my ability to analyze large amounts of data while also

developing a deeper understanding of the human impact cybercrime can have on victims and society.

This project also demonstrated interdisciplinary thinking because it combined criminal justice concepts, cybersecurity concerns, psychology, and investigative research methods. Cybercrime investigations involving children require both technical investigative skills and an understanding of victimization and offender behavior. Through this assignment, I learned how cybersecurity and criminal justice intersect in real-world investigations. The project also reinforced my long-term interest in investigative work involving online crimes against children.

One of the most important lessons I learned during this assignment was the importance of communication and organization when discussing sensitive topics. Presenting difficult material professionally while maintaining factual accuracy challenged me to improve both my writing and research abilities. According to Meade (2023), reflection allows students to connect experiences and develop deeper understanding through meaning-making and systematic thinking. This project represented that process because it connected my academic interests directly to my career goals and future aspirations.

Another artifact that demonstrates my investigative and analytical abilities is my interdisciplinary analysis discussing why traditional criminal justice deterrence often fails against ransomware attacks. This assignment explored how modern cybercriminals operate in ways that traditional criminal justice systems struggle to address. Because ransomware attacks often involve anonymity, international actors, and decentralized operations, traditional deterrence methods are less effective within cybercrime environments.

This artifact demonstrates interdisciplinary learning because it combined criminal justice theory with cybersecurity analysis and global policy concerns. Through this project, I learned that cybercrime problems cannot be solved through one discipline alone. Understanding ransomware requires knowledge of cybersecurity infrastructure, criminal justice systems, international law, economics, and human behavior. Reynolds and Davis (2014) explain that integrative learning encourages students to connect knowledge across disciplines to solve complex problems. This assignment reflected that concept by combining multiple academic perspectives into one analysis.

The project also strengthened my ability to critically analyze modern cybersecurity challenges. I learned how important adaptability and interdisciplinary thinking are within cybersecurity careers. Since cybercrime evolves constantly, investigators and cybersecurity professionals must continue learning and adjusting strategies to address emerging threats.

My analysis of the 2019 Capital One cybersecurity incident further developed my threat analysis and investigative skills. This assignment focused on how vulnerabilities within cloud infrastructure and organizational security practices contributed to one of the largest financial data breaches in recent years. Analyzing this breach helped me better understand incident response, organizational accountability, and cybersecurity risk management.

This artifact demonstrates my ability to evaluate real-world cybersecurity events while connecting technical issues to broader organizational and societal impacts. Through this project, I learned that cybersecurity incidents often involve both technical vulnerabilities and human decision-making failures. IBM (2024) reports that human error remains a major contributing factor in cybersecurity breaches. This assignment reinforced the importance of proactive security planning and continuous monitoring within organizations.

Additionally, the project strengthened my research and communication skills because I had to explain technical cybersecurity concepts clearly while analyzing the causes and impacts of the breach. This ability to communicate complex information effectively is critical within investigative and cybersecurity careers.

One of the strongest examples of my strategic thinking and organizational planning abilities is my risk management policy project. This assignment required me to create a structured cybersecurity policy designed to identify, assess, and reduce organizational security risks. Through this project, I developed a stronger understanding of how organizations balance operational efficiency with cybersecurity protection.

The assignment also demonstrated the importance of leadership and planning within cybersecurity environments. Security professionals must not only understand technical systems but also create policies that employees and organizations can realistically follow. This project improved my ability to think strategically while also strengthening my professional writing and organizational skills.

One challenge I faced during this assignment was learning how to create policies that addressed both technical risks and human behavior. Cybersecurity policies are only effective if organizations can implement them successfully. This project helped me understand how leadership, communication, and organizational structure all influence cybersecurity effectiveness.

Another artifact connected to this skillset is my analytical paper discussing whether cybersecurity should rely more heavily on humans or technology. This assignment explored one of the most debated topics within cybersecurity. While advanced technology can significantly

improve security defenses, human behavior remains one of the largest vulnerabilities organizations face.

Through this assignment, I learned that cybersecurity is not solely a technical field. Human decision-making, communication, awareness, and organizational culture all play major roles in security effectiveness. The project strengthened my critical thinking skills by requiring me to evaluate multiple perspectives while supporting my arguments with research and analysis.

This artifact also reflects interdisciplinary learning because it combines psychology, technology, organizational behavior, and cybersecurity practices. Finley (2021) explains that employers increasingly seek professionals who can combine technical expertise with communication and interpersonal skills. This project reinforced the importance of balancing both technical and human-focused approaches within cybersecurity environments.

My mock Chief Information Security Officer (CISO) analysis further strengthened my understanding of cybersecurity leadership and organizational security strategy. This assignment focused on how security leaders balance technical security controls with employee behavior and organizational culture. Through this project, I learned that effective cybersecurity leadership requires communication, adaptability, and strategic thinking in addition to technical knowledge.

This assignment also helped me better understand the responsibilities associated with leadership roles within cybersecurity organizations. Security leaders must coordinate teams, communicate risks effectively, and create environments where employees understand the importance of cybersecurity practices. My previous leadership experiences working in hospital security helped me connect real-world leadership concepts to this assignment.

The project demonstrated how interdisciplinary thinking contributes to effective cybersecurity management. Technical solutions alone cannot solve cybersecurity problems if organizations fail to address human behavior and communication challenges.

The insurance business plan project demonstrates my teamwork, communication, and organizational planning abilities. Although this project was not directly cybersecurity-focused, it strengthened skills that are highly valuable within cybersecurity and investigative careers. The assignment required collaboration, professional communication, and strategic planning while working with other students to develop a realistic business structure.

One important lesson I learned through this project was how essential teamwork and communication are within professional environments. Cybersecurity professionals frequently work with teams across departments, requiring strong collaboration and planning skills. This assignment also improved my ability to communicate ideas clearly and contribute effectively within group settings.

My wired network design project for Maury High School demonstrates my technical communication and operational planning abilities. This assignment involved calculating cabling requirements, planning VLAN structures, selecting networking hardware, and estimating implementation costs. Through this project, I gained practical experience with network infrastructure design and organizational planning.

The assignment strengthened my understanding of cybersecurity fundamentals related to network segmentation and infrastructure security. Creating separate VLANs for students, staff, and infrastructure demonstrated how organizations improve network security through segmentation and access control.

This project also improved my ability to organize technical information clearly and professionally. I learned how technical planning involves balancing security, efficiency, scalability, and budget limitations simultaneously.

The home network diagram project further strengthened my understanding of networking structure and cybersecurity planning. Through this assignment, I learned how devices, routers, switches, and security measures connect within a network environment. This project improved my ability to visualize technical systems and communicate networking concepts clearly.

Although smaller in scale than the Maury network project, this artifact helped reinforce foundational networking knowledge that supports future cybersecurity and investigative work. Strong technical communication skills are important within cybersecurity careers because professionals must explain technical concepts to both technical and non-technical audiences.

One of the most important lessons I learned throughout my degree program is the value of interdisciplinary thinking. Cybercrime and cybersecurity require professionals to combine knowledge from multiple fields, including criminal justice, technology, psychology, leadership, communication, and organizational planning. My coursework consistently reinforced the idea that complex cybersecurity problems cannot be solved through technical knowledge alone.

Courses such as IDS 300W helped prepare me for advanced coursework by strengthening my research, writing, and analytical thinking skills. These interdisciplinary experiences improved my ability to analyze problems from multiple perspectives while communicating ideas effectively. According to Reynolds and Davis (2014), ePortfolios help students connect learning experiences and demonstrate integrative thinking across disciplines. Developing this portfolio

helped me better recognize how my coursework collectively contributed to my professional growth and career readiness.

My self-assessment also reinforced the importance of perseverance, adaptability, and leadership throughout my academic journey. Maintaining a 3.9 GPA while balancing personal challenges demonstrated resilience and commitment to my goals. Additionally, my leadership experiences through the National Society of Leadership and Success and my supervisory role within hospital security strengthened my confidence, communication abilities, and decision-making skills.

Overall, this portfolio reflects the interdisciplinary skills, experiences, and personal growth I developed throughout my Cybercrime degree program at Old Dominion University. Through coursework involving cybercrime investigations, risk management, networking, research analysis, and leadership development, I strengthened both technical and analytical skills that support my future career goals.

The artifacts included throughout this portfolio demonstrate my abilities in investigation, cybersecurity strategy, communication, and operational planning while also highlighting the importance of interdisciplinary thinking within cybercrime careers. As I prepare to graduate and transition into professional opportunities, I plan to continue developing my technical and investigative skills while pursuing careers focused on cyber investigations and digital forensics. This portfolio represents both my academic accomplishments and my continued commitment to personal and professional growth.

References

Finley, A. (2021). How college contributes to workforce success: Employer views on what matters most. Association of American Colleges and Universities.

IBM. (2024). Cost of a data breach report 2024.

Meade, L. (2023). Documenting your learning and personal growth: Critical reflection.

Reynolds, C., & Davis, N. (2014). Leveraging the ePortfolio for integrative learning. Stylus Publishing.

Rodgers, C. (2002). Defining reflection: Another look at John Dewey and reflective thinking. Teachers College Record, 104(4), 842–866.