Phishing for Success: My Academic Journey in Cybersecurity

Gabrielle Gaston

IDS 493 EPortfolio Reflection

Throughout my academic journey as a cybersecurity student at Old Dominion University, I have developed a profound appreciation for how technology, policy, and human decision making converge to produce the digital space that sustains the modern world. This ePortfolio explores inquisitive cyber security expertise through a curated selection of coursework that demonstrates my developing technical engagement, analytical thinking, and ability to apply conceptual knowledge to active challenges. Each artifact represents a milestone in my growth, illustrating not only what I have learned but also how these experiences have shaped my professional identity and commitment to continuous learning. Beginning strong with exploring the political evolution of cybersecurity regulations to concluding with understanding operational resilience and disaster recovery, my coursework displayed reflects my intellectual inquisitiveness and readiness to contribute meaningfully to the cybersecurity field, and built a strong foundation for my future in cybersecurity.

Innovation: Instruments of Technology to Improve Systems and Experiences

As a Cyber Security Student, innovation has been one of the most necessary aspects of my academic and professional development. Throughout my studies and internships, I have discovered how creative thinking and technical application can work together to strengthen digital systems and improve user experiences.

One artifact that embodies innovation is my presentation illustrating the benefits of integrating Artificial Intelligence (AI) into healthcare operations. In this project, I explored how AI technologies enhance efficiency in patient care, streamline data management, and improve decision making in clinical settings. Creating this exhibition challenged me to think critically about how innovation can serve as a catalyst for progress but also a source of vulnerability if not properly managed. I learned to evaluate technology not only for capabilities, but for ethical implications and security considerations. This project strengthened my ability to communicate complex ideas clearly, merging technical comprehension with explanations personalized for the target audience. The extensive research of how AI can optimize patient care, streamline administrative workflows, and enhance predictive diagnostics was essential. However, beyond understanding the technical promise of AI, I also examined the cybersecurity implications of its integration, particularly around data privacy, algorithmic transparency, and compliance with regulations such as HIPAA.

As part of my role as a Technology Consultant, I conducted an onsite Cybersecurity Awareness Training that focused on empowering users through innovation in digital safety practices. The session addressed common yet often overlooked risks such as connecting to unsecured public WiFi networks, which can expose users to attacks and data interception.

To mitigate these risks, I introduced participants to the concept and practical use of Virtual Private Networks (VPNs), explaining how VPNs encrypt online traffic to safeguard sensitive information. The training also covered phishing protection strategies, emphasizing key indicators to help identify suspicious emails, verify sender authenticity, and report fraudulent messages effectively. Additionally, I discussed the role of antispam software in filtering malicious content, as well as the dangers of malware and computer viruses that can compromise system integrity. Last but not least, one of the most important points highlighted during the session was the necessity of creating strong, unique passwords for every account, supported by password management tools to reduce the risk of credential theft. This training reflected my innovative approach to cybersecurity education by combining technical instruction with feasible scenarios, transforming complex concepts into practical, user friendly lessons that encouraged safe online behaviors.

Combined, these projects illustrate how I have cultured innovation as a professional skill. Whether deploying new technology, identifying system conflicts, or integrating secure solutions, I learned that innovation in cybersecurity is not limited to adopting new tools, but includes using creativity and knowledge to design solutions that improve systems while maintaining security and user trust.

Regulations: Understanding Governance, Compliance, and Structure

Another pillar of my cybersecurity journey is my understanding of policies and governances. Through coursework and enacted projects, I have come to appreciate how policies establish order, enforce compliance, and foster a environment for secure operations.

The detailed analysis of the political evolution of regulations associated with the Federal Risk and Authorization Management Program (FEDRamp), represents a critical stage in my understanding of how cybersecurity governance functions at the federal level. This research deepened my understanding of how federal agencies maintain secure cloud services through structured governance. While developing this analysis, I studied how cybersecurity policy evolves alongside technology, responding to emerging threats and public concerns. This artifact taught me to interpret and critique policy documents, recognize the influence of political decision making, and appreciate how regulation and technology work together to build public trust while reinforcing the importance of accountability, transparency, and continuous improvement within federal cybersecurity systems.

My comprehensive response on the importance of an organization’s operational policy during unexpected downtime also reflects my ability to apply policy frameworks in practical contexts. This project emphasized the critical role of preparation and structure in maintaining organizational resilience. By studying recorded incidents and analyzing the NIST Cybersecurity Framework, I acquired that having a well documented policy ensures that teams know their

responsibilities beforehand, can respond efficiently, and diminish disruptions. Analyzing regulations enabled me to comprehend the value offered when strong operational policies act as a bridge between technical readiness and human coordination.

Building on this understanding, my paper on the advantage of disaster recovery planning demonstrated the strategic side of policy in action. This artifact emphasized proactive preparation, showing how documented recovery plans ensure business continuity, data protection, and swift restoration after disruptions. Through this research, I developed a holistic approach for organizational security by recognizing that policy is not just about compliance but about foresight. Multiple disaster recovery strategies were evaluated, such as cloud replication and redundancy, and analyzed their effectiveness amongst different organizational settings. This experience allowed me to think critically about aligning cybersecurity policy with business objectives and risk management strategies.

Overall, my work surrounding policy has helped me realize that cybersecurity is not sustained through technology alone but through the frameworks and governance structures that guide its use. Effective operations ensure that innovation comes to life within safe boundaries, protecting organizational integrity and public trust. Understanding and applying these frameworks validated that I have learned to see the bigger picture of cybersecurity as a shared responsibility among government, organizations, and individuals.

Practical Experience: Applying Knowledge in Functional Environments

While innovation and policy have shaped my analytical mindset, hands on experience has been the foundation of my practical growth as a cybersecurity professional. The skills I developed through real world problem solving empower me to translate theoretical concepts into actionable results. This experience has allowed me to strengthen my skills and bridge the gap between academic knowledge and concrete application.

An illustration of practicality is my compiled research on the progression, utilization, and upgrades of the Windows Server. This project amplified my understanding of how operating systems evolve to meet the security and performance requirements of modern enterprises. Through this research, I noted features such as Active Directory, virtualization, and user access control. I also attained experience in identifying vulnerabilities and the necessity of system updates for maintaining compliance and stability. This artifact demonstrated my ability to combine academic research with technical understanding, allowing me to better grasp how servers form the backbone of secure network infrastructures.

Furthermore, my Email Import Resolution project exemplifies practical problem solving in a professional environment. I diagnosed a synchronization issue between the AOL Mail server and the Apple Mail app, which prevented residents from receiving their messages. After thorough investigation, I discovered that the issue was stemming from server authentication.

I was able to adjust account settings and facilitate logins through proper user supervision, effectively restoring email functionality. This hands on experience involved extensive troubleshooting and communication skills, which are vital for IT and cybersecurity roles.

Another example of practicality is my Smart Device Integration project, where I was a part of a launch that provided Amazon Alexa devices for 148 residents at Atlantic Shores. This project required troubleshooting, device configuration, and secure network integration. Applying my prior exposure to wireless networking and IoT security, I ensured that each device operated efficiently while maintaining user privacy. I also learned how to adapt technical solutions to accommodate the needs of a large and diverse user base. This experience enhanced my ability to implement emerging technologies personalized strategically.

Additionally, the Apple Rotating MAC Address investigation further strengthened my practical mindset. When residents with Apple devices began esclating frequent WiFi disconnections, I discovered that Apple's privacy feature, which randomizes MAC addresses, was disrupting network authentication. To address this, I analyzed network logs, studied device behavior, and proposed adjustments to authentication procedures. Solving this issue taught me how innovation and adaptability go hand in hand in cybersecurity. Rather than viewing the privacy feature as a problem, I learned to see it as a security enhancement that required creative reconfiguration on the network side.

I applied critical thinking and analytical reasoning to identify problems, design solutions, and test outcomes. These experiences not only strengthened my technical knowledge but also helped me develop patience, adaptability, and user centered thinking qualities that are just as important as technical skill in the cybersecurity field.

Through all of these experiences, I have learned that practical work is a pivotal transformation that transmutes abstract knowledge into meaningful action. Each challenge I faced equipped me with how to navigate uncertainty, troubleshoot under pressure, and maintain professionalism while supporting users. These lessons are invaluable as I continue to build a career rooted in technical excellence, collaboration, and integrity.

Integrating Innovation, Policy, and Practical Experience

Combined, these artifacts reveal how my understanding of innovation, policy, and practical application has evolved throughout my studies. Each category are interconnected, forming a balanced foundation for professional success in cybersecurity. Innovation encourages creative problem solving and adaptability, while policies provide structure, accountability, and ethical guidance. Practical experience, in turn, grounds these concepts in real world practice, transforming knowledge into capability.

In particular, the innovative problem solving demonstrated in my smart device and AI projects would not have been as successful without an understanding of security policies to guide implementation. Similarly, my experience researching disaster recovery and operational policies became far more meaningful when I applied those principles in real world troubleshooting scenarios. Each experience built upon the last, allowing me to move from theoretical understanding to hands on expertise.

As a whole, these experiences have shown me that cybersecurity is not limited to one area of focus. It is a field that requires continuous learning, collaboration, and integration of diverse skills. My ability to innovate responsibly, interpret and apply policies effectively, and solve problems through practical experience reflects the comprehensive education I have received.

Conclusion: From Learning to Leadership

Reflecting on my academic and professional journey, I see how each experience has contributed to shaping not only my technical capabilities but also my identity as a cybersecurity professional. My education has taught me that success in this field depends on the ability to balance innovation with policy, and theory with practice.

Through innovation, I have learned to approach challenges creatively and to view technology as a tool for progress and empowerment. Through policy, I have developed respect for structure, governance, and the ethical dimensions of cybersecurity. Through practical experience, I have built confidence in my ability to apply these lessons in actual settings, adapting quickly and solving problems with precision and care.

Ultimately, this ePortfolio stands as evidence of my growth, resilience, and readiness to enter the cybersecurity workforce. Each artifact tells a story of learning, adaptation, and achievement. Together, they represent my evolution from a student exploring the foundations of cybersecurity to a professional prepared to safeguard digital systems, support innovation, and uphold the highest standards of ethical responsibility. My journey has recently begun, but the skills I have gained including innovation, policy understanding, and practical expertise will continue to guide me as I build a meaningful and impactful career in cybersecurity.

References:

"2023 National Cybersecurity Strategy." *The White House*, 2 Mar. 2023, bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

"Federal Risk and Authorization Management Program (FedRAMP)." *U.S. General Services Administration*, 2024, www.fedramp.gov/.

HealthIT.gov. "Artificial Intelligence (AI) in Health Care." *Office of the National Coordinator for Health Information Technology*, 2023, www.healthit.gov/topic/scientific-initiatives/precision-medicine/artificial-intelligence-health-care.

Microsoft. *Windows Server Documentation*. Microsoft Learn, 2024, learn.microsoft.com/en-us/windows-server/.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*, Version 2.0. U.S. Department of Commerce, 2024, nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.022024.pdf.

Ready.gov. "Business Continuity Planning Suite." *U.S. Department of Homeland Security*, 2023, www.ready.gov/business-continuity-plan.

Smith, John M., and Priya Patel. "The Role of Disaster Recovery Planning in Ensuring Business Continuity." *Journal of Information Systems Security*, vol. 19, no. 2, 2022, pp. 45–59.

Vaidhyanathan, Siva. *The Googlization of Everything (and Why We Should Worry)*. University of California Press, 2011.