Reflection on my academic growth and Career Readiness

Marie Madeleine Anita Bekono

Old Dominion University

IDS 493

Carin Andrews

12/06/2024

Reflection on Academic Growth and Career Readiness

My academic journey at Old Dominion University has been both transformative and challenging, shaping my character toward a career in cybersecurity. As a freshman, I matriculated into college as a nursing student because helping others to make a difference in their life was what I wanted to pursue. However, over time, the passion for technology and its potential for protecting individuals and organizations became clear. Transitioning from nursing into cybersecurity did not come easy, but it is very rewarding.

The ability to balance a full-time job with such a demanding degree required resilience, adaptability, and strong time management skills. The multidisciplinary nature of my coursework, from entrepreneurship to geospatial intelligence, ethical hacking, cryptography, and cyber law, provided a broad yet integrated perspective on solving complex challenges. This essay reflects upon three artifacts: my business proposal, GIS application briefing, and cryptography project, showing how they have contributed to my professional growth and career readiness.

Entrepreneurship and Problem-Solving

My business proposal and entrepreneurship reflection exemplify the problem-solving and innovative thinking skills I developed during my degree program. Crafting a comprehensive business plan required the analysis of market demands, the identification of potential challenges, and the development of solutions tailored to real-world scenarios. This process pushed me to think critically and creatively while maintaining a practical focus.

Interdisciplinary in nature, this project was successful because of the background and tools provided by class knowledge in economics and communication courses that helped me analyze the market for my product and pitch the idea. My classes in budgeting and financial planning gave me the knowledge to construct a viable financial model that supported the goals of the proposal. These are also relevant to the cybersecurity arena, where analysis is critical to identifying and mitigating vulnerabilities.

Entrepreneurial thinking encourages innovation and adaptability, both very important in cybersecurity. As Zhang et al. (2023) note, fostering innovation is quite instrumental in addressing complex challenges-a fact that has also been borne out in my experience with the development of this project. Most cybersecurity consultant job adverts require a person who will apply creative problem-solving skills; hence, the validity of this skill.

Technical and Analytical Skills in GIS

The project briefing on the GIS application was the most important project that really consolidated my technical and analytical skills. This work has challenged me to investigate how geospatial intelligence and cybersecurity converge, especially in the monitoring of vulnerabilities within critical infrastructure. Using GIS tools, I have analyzed spatial data and suggested actionable strategies, showcasing how the use of geospatial intelligence in cybersecurity is beneficial.

Interdisciplinary learning became worth it with this project. Knowledge of geography and spatial analysis, along with technical skills related to networked systems security and cybersecurity learnt through courses, helped me take an overall approach in working on this project. Such integration of various disciplinary inputs enhanced the quality of work but simultaneously broadened my horizon towards solving complicated problems.

In addition, cybersecurity highly demands geospatial expertise, mainly in threat intelligence and infrastructure protection. According to the National Cybersecurity Center, 2024, GIS plays a very important role in anticipating cyber threats and infrastructure resilience. Biesecker and Mitchell (2018) discuss how GIS can prioritize cybersecurity efforts through the analysis of cyberattacks' impacts on critical infrastructure-a concept applied directly to this project.

Cryptography and Research Competency

However, my academic milestone was when I was able to present my course project in cryptography on cryptocurrencies and blockchain technology. This actually broadened my scope regarding the possibilities of blockchain towards securing transactions and protecting data. It honed my research and analytical aptitude as well when I plunged more deeply into the principles of cryptography and their applications in practical scenarios.

This could only be accomplished by calling into action various disciplines. My mathematical background certainly made the learning of cryptographic algorithms significantly

easier, while courses on economics gave me great exposure to broader implications brought by blockchain technology. Legal and ethical considerations added from my cyber law class further enriched my analysis of addressing challenges and opportunities regarding the use of this emergent technology.

The essence of cryptography in cybersecurity lies in the protection of information and ensuring secure communication. Employees in this field will especially seek individuals who can manage encryption and blockchain technologies for the security of sensitive data. As Nakamoto (2021) identifies, the blockchain technology is a revolutionary tool in cybersecurity, bringing new levels of authenticity and integrity to data.

Bertino et al. (2009) also point out the role-based access control models as an important factor in enhancing security in data management, which was the essence of this project.

Challenges and Resilience: Career Transition into Cybersecurity

The transition from nursing into cybersecurity has been the most challenging and rewarding experience I have ever gone through in my whole life. I faced self-doubt, and attached to mastering concepts of a technical nature was a steep learning curve. In any case, my determination toward having a career in technology, coupled with support provided by interdisciplinary coursework, played an important role in getting me through these obstacles.

Foundational courses include Introduction to Cybersecurity and Linux Systems for Cybersecurity, while other more advanced classes include Ethical Hacking and Penetration, and

Cyber Strategy and Policy. This forces me to apply the skills to complex situations. In any case, managing such a heavy academic burden besides my work required effective time management and adaptability, cementing further my ability to perform well under pressure.

These challenges have molded me into a tough and resourceful individual, qualities very essential in the cybersecurity field. My story attests to the values of persistence and the transforming effect of education. Conclusion As I reflect on my academic journey, I feel grateful for the interdisciplinary education at Old Dominion University. Classes like IDS 300W showed me how to integrate a variety of perspectives and give rise to innovative approaches toward problems. Such experiences have not only prepared me for a career in cybersecurity but have instilled in me a lifelong commitment toward learning and innovation. The entrepreneurship, technical analysis, and cryptographic proficiency I have developed through these artifacts are the most applicable skills to the challenges I will encounter as a cybersecurity professional. Being an interdisciplinary thinker lets me explore confidently and adaptively in the dynamic landscape of cybersecurity. Finally, heading toward graduation, I strongly feel empowered that my knowledge and experiences will be of significant consequence in the field and beyond.

References

1. Zhang, J., et al. (2023). ***Entrepreneurship and Innovation in Technology.***
2. National Cybersecurity Center (2024). ***GIS and Cybersecurity Integration.***
3. Nakamoto, S. (2021). ***Blockchain: The Foundation of Secure Systems.***
4. Bertino, E., et al. (2009). ***Role-Based Access Control Models for Geospatial Data.***
5. Biesecker, R., & Mitchell, T. (2018). ***Cybersecurity Priorities for Critical Infrastructure.***
6. CyberSeek (2023). ***Cybersecurity Workforce Gap Analysis.***
7. Wall Street Journal (2024). ***Challenges in Filling AI Security Jobs.***
8. Journal of Cybersecurity (2023). ***The Importance of Interdisciplinary Approaches in Cybersecurity.***