Introduction

Cybersecurity is far more than a purely technical field. Cybersecurity is a complex, interdisciplinary field that requires multiple skillsets to include ethical reasoning, strong communication, and creative problem-solving. My experience in Old Dominion University's Cybersecurity program, combined with my service in the U.S. Navy, has made me well-prepared and armed with the diverse skillset needed to be successful in the modern workforce. Not only have I gained technical knowledge to manage networks or prevent breaches, but also the soft skills to make well thought out decisions, explain threats to non-technical audiences, and adapt quickly in high-pressure scenarios. This reflective essay highlights my top three skills. These skills are ethical judgment, communication, and creative problem-solving. Furthermore, it explains how specific artifacts I created during the program demonstrate my growth and readiness to enter the professional field.

Ethical Judgement

Ethical judgment has been an important skill that I've possessed throughout both my military service as well as my cybersecurity education at ODU. As an Operations Specialist in the Navy, I worked with classified information where ethical decision-making was required for everyday operations. This mindset carried into my academic studies, particularly through assignments that focused on real-world cybersecurity examples.

In my Case Analysis on Corporate Social Responsibility (CSR), I applied ethical frameworks such as utilitarianism and deontology to evaluate the responsibilities of corporations handling consumer data. Similarly, in the Data Privacy case study, I analyzed companies' data retention

practices, emphasizing the importance of user consent and transparency. Lastly, in my Whistleblowing analysis, I explored the risks and moral justifications behind disclosing sensitive information in public interest.

These assignments helped me understand the ethical stakes involved in cybersecurity, from insider threats to corporate accountability. They taught me to think critically about legal and ethical boundaries while considering how emerging technologies impact society. Ethical reasoning is listed as a core requirement in many job descriptions for cybersecurity analysts, risk officers, and compliance managers that demand careful judgment when navigating laws, policies, and user rights. Through these artifacts, I've shown that I can apply ethical theory to practical scenarios, preparing me to meet the demands of this high-responsibility field.

Communication Skills

Effective communication is essential in cybersecurity, especially when translating technical problems into terms that executives, users, or other stakeholders can understand. My time in the Navy reinforced this skill as I had to communicate clearly under pressure, whether delivering a radar report or coordinating team responses. I've honed these skills further during my academic work, especially through writing assignments and presentations.

One artifact that demonstrates this is my IoT Data Breach Write-Up, where I explained what the Internet of Things (IoT) is and examined its vulnerabilities using the Mars Hydro data breach as a case study. I had to break down complex networking concepts for a general audience while highlighting security concerns in everyday consumer technology.

My Incident Report on the 2017 Equifax Breach required me to examine and explain a high-profile public cybersecurity failure into a clear, structured report that non-technical users would be able to understand. This involved not only technical analysis but also an explanation of its broader implications, regulatory, financial, and reputation. Lastly, my CIA Triad Explanation showcased my ability to articulate the foundational principles of cybersecurity, confidentiality, integrity, and availability while also distinguishing between authentication and authorization, a key area of confusion even among entry-level professionals such as myself.

These experiences have made me confident in my ability to "bridge the gap", so to speak, between technical and non-technical audiences. Job roles such as a Security Consultant or an IT Policy Analyst consistently demand this ability. Thanks to my academic training and Navy background, I can speak the languages of both cybersecurity operations as well as successfully incorporate leadership skills I picked up while in the Navy.

Creative Problem Solving

Problem-solving is the heart of any cybersecurity role, wehether you're defending a network, analyzing malware, or developing user education tools such as my team's "Cyber Sensei" program. I've always approached challenges analytically. I developed this mindset \through managing radar systems in the Navy and strengthened it through hands-on assignments at ODU such as VM labs.

In my UX Design Thinking project, my team and I created a gamified tool to teach users cyber hygiene leveraging psychology, user experience design, and education theory to make security practices more engaging and effective. This project was a turning point in how I view

cybersecurity, not just as a defense mechanism, but as a user-centered discipline. I had to think outside the box, using empathy and creativity to solve a real-world problem and explain it effectively to a normal audience.

Furthermore, my Game Design artifact involved developing a functioning cybersecurity-themed game using third-party assets. It was a crash course in project management, digital storytelling, and the development involving user experience. I gained insights into user interaction and learned how to troubleshoot design challenges using logic and persistence, as week as teamwork from fellow industry professionals.

Lastly, my Python Socket Programming project involved writing client-server code to support a plant care assistant application. While not strictly cybersecurity in nature, this project taught me the basics of secure communication, sockets, and user-interface design. It's a great example of how technical creativity and interdisciplinary skills can be used to solve problems.

Employers consistently seek cybersecurity professionals who are not just technically skilled but also inventive and adaptive in the face of complex challenges. These artifacts show that I can apply cybersecurity principles across different domains and build tools that are both functional and user-friendly.

Conclusion

Looking back on my time at Old Dominion University, I see how the interdisciplinary design of the Cybersecurity program gave me an edge. Courses like IDS 300W helped me articulate my ideas clearly, while philosophy classes trained me in structured ethical reasoning. Meanwhile,

computer science and design thinking projects taught me to apply security principles in practical and innovative ways. My academic path has not been a technical experience, but it has also been one collaboration between disciplines, reflection, and real-world application, whether as an individual, or in a team environment.

The combination of ethical judgment, strong communication, and creative problem-solving is more than just a checklist of skills, it's also an important mindset to have. This mindset enables me to respond to evolving cybersecurity threats with well-flushed out strategies, as well as to convey my ideas in an effective manner across organizational boundaries. It also allows us to remain ethically grounded in a world where digital power is easily abused.

Being an interdisciplinary thinker in cybersecurity is not just helpful, it's also necessary. The problems we face are global, multifaceted, and constantly changing. To protect systems, data, and people effectively, I must continue to increase my knowledge from various disciplines. That is the foundation I've built through my studies at ODU, and it's what will carry me forward as a cybersecurity professional in the future.