ePortfolio Reflection Essay

Introduction

In my cybersecurity degree at Old Dominion University, I learned many things that have taught me to look at cybersecurity in more ways than one. After beginning classes at Old Dominion University that taught me the basics of cybersecurity, I started to think that cybersecurity was just about keeping your computers, networks, and information safe. Throughout my coursework, I learned that cybersecurity is about much more than that.

During my coursework and internship at Place4Us, I learned skills that I believe will be beneficial to my future career. The three key skills I selected to demonstrate in my ePortfolio are Technical/Cybersecurity Skills, Research & Critical Thinking, and Communication & Professional Skills. I chose these skills because they are all in different areas of my education and show my growth as a student. The nine artifacts in my portfolio show how I have applied these skills in my coursework and my internship. Developing my portfolio also helped me see links I had not noticed between assignments that I previously saw as discrete pieces of work.

Technical/Cybersecurity Skills

The first artifact I chose as a demonstration of my technical cybersecurity skills is Reflection #2 from CYSE 368. In this reflection, I discuss the work I did in my internship at Place4Us, where I looked at security and privacy issues on the platform. I looked mainly at the authorities and roles of the users. I looked at how permissions were assigned to users, the reasons for having different roles, and why access should be restricted. I gained more of an understanding of role-based access control, authentication, authorization, and least privilege. Sandhu et al. (1996) talk about how role-based access control assigns permissions to roles within an organization. This applies to my internship because I was researching the way that different users should be provided access to the platform. Many of these ideas I was familiar with beforehand from class. My internship showed me how they could be put into practice on a platform.

My second technical artifact is *Exploring Attacks on Availability* from CYSE 200T. In this assignment, I researched distributed denial-of-service attacks and how they interfere with legitimate users. I learned that in such attacks, other devices can be used to inundate a system or network with traffic, thereby rendering it unusable to the business or organization that is impacted. Through research, I found out that traffic filtering and redirection, system redundancy, monitoring, and use of the cloud were a few forms of protection against such attacks. The National Institute of Standards and Technology (2024) explains how to manage cybersecurity risk through the functions of identify, protect, detect, respond, and recover. This is relevant to

availability, as organizations must plan for the inevitable attacks rather than depend solely on one protection plan.

The third artifact I want to share is my work on SCADA systems for CYSE 200T. Before working on it, I didn't really understand how cybersecurity applied to vital services like electricity, water, transportation, and manufacturing. I researched potential security issues like aging equipment, login procedures, network linking, and monitoring. I also researched safeguards like segmenting networks and tighter login procedures. This assignment opened my eyes to the fact that cybersecurity attacks can have impacts that go beyond computers and data; an attack on infrastructure could impact services that everyone relies on. Together, these three artifacts show how I learned technical information during my coursework and then used similar principles in my internship.

Research & Critical Thinking

One of my strongest artifacts for a research assignment is Policy Analysis Paper 5 from CYSE 425W. In this project, I looked at the 2023 U.S. National Cybersecurity Strategy and focused on whether the strategy's aims and objectives were being met. From this project, I learned that reviewing a cybersecurity policy is more than reporting on what a policy says. I also had to look at evidence that might be used to measure progress and whether the strategy was providing enough direction to meet its aims. I think I did a good job of finding, using, citing, and comparing sources to reach a conclusion. NIST (2024) talks about the importance of governance in cybersecurity risk, and I did see a similar concept in my policy analysis.

My second artifact is Article Review #2 from CYSE 201S, which looked at social skills, cyberbullying, and empathy. Unlike most of the technical artifacts in my portfolio, this one was focused on human factors and social science. In addition to writing up the research question, variables, methods, and results of the study, I learned about how researchers analyze data to look for relationships among different factors and how differences in research methods can lead to different conclusions. For example, the research by Zych et al. (2019) showed a connection between different cyberbullying roles and empathy. This has helped me realize that cybersecurity issues are not always technical but can be social and psychological as well.

My analytical paper in my CYSE 200T class enhanced my research and critical thinking skills. I investigated cybersecurity challenges of telecommuting and authentication technologies, trying to determine how technology can be advantageous while also raising privacy and security issues. I learned that telecommuting and authentication can lead to threats involving people's personal computers, networks, authentication processes, and user behavior. Herley (2009) describes how users may choose to ignore some security advice if they do not believe the time and effort required is worth the benefit. I learned that a security measure can be technically effective but awkward to use, making it problematic. From this learning artifact, I gained insight into how

research entails examining evidence and considering different points of view before coming to a conclusion.

Communication & Professional Skills

The internship with Place4Us also gave me the chance to build on my communication and professional skills beyond what would be required in the classroom. One artifact I have chosen to include is my Place4Us Research Draft. During the internship, I explored a variety of topics, including user roles, authorization, privacy, MyFiles, generative AI detection, use of passwords, security logging, and error handling. My task was not only to identify potential concerns but also to organize my research and present recommendations to the team. Pollini et al. (2022) explore human factors in cybersecurity and the interaction between people and technical systems. This applies to my internship, as the security recommendations that were made around access and privacy will also need to take the people who are using and managing the platform into account.

Reflection #3 from CYSE 368 also exemplifies my growth during the internship. By the final stage of the internship, I felt comfortable researching cybersecurity issues and making recommendations based on my research. I worked on many areas, including access control, password security, privacy, error handling, logging, and backup and recovery. One important thing I learned was that discovering a security vulnerability does not necessarily mean that other people will understand why it is a risk. I had to communicate it to other people and make recommended solutions understandable to them. Bada et al. (2015) deal with the use of cybersecurity communication to change behavioral patterns and express the concern that cybersecurity knowledge may not necessarily change anyone's behavior.

My last artifact is the Cybersecurity Professional Career Paper from CYSE 201S. I learned about the career of a cybersecurity analyst and how it relates to social science and human behavior. I learned that cybersecurity analysts do more than just monitor networks and investigate attacks; they also need to understand human interactions with technology and how humans make decisions. I discussed topics such as social engineering, perception of risk, trust, and insider threats. I learned that I do not only need to be technically sound for the future career I want, but I also need to be able to communicate with others, discuss risks, and direct organizations toward security decisions. My internship and my career paper have helped me understand the role of a cybersecurity professional as well as how all of these skills I am developing come together.

Interdisciplinary Learning and Portfolio Growth

The most valuable thing I've learned throughout my degree is that cybersecurity can link to so many other fields. My technical courses gave me insight into systems, networks, threats, and security controls. My policy and research courses provided an understanding of government, organizations, policymaking, and decision-making. My social science courses provided

knowledge of how people's behavior can impact cybersecurity. I realized this during my internship. In my research on access control, I needed technical knowledge about permissions, passwords, and authentication, but I also needed an understanding of organizational responsibilities and what the end user actually does when using the platform. In my privacy research, I needed technical knowledge of the protections in place, but I also needed to consider what those protections meant to the people whose information was being collected.

Putting the ePortfolio together made me see these experiences differently. When I first completed many of these assignments, I saw them as course assignments and course requirements. Assembling this ePortfolio helped me see them as artifacts that reflect my growth and learning. The artifacts are part of my narrative identity because individually they don't show everything I learned, but collectively my technical coursework, research, interdisciplinary assignments, and internship all serve to show how my skills as a student and professional have grown.

This cross-disciplinary mode of thinking will be useful in my future career because cybersecurity issues tend to involve technology, people, groups, institutions, privacy, and ethical aspects simultaneously. A technical solution might not work if it does not take into account how people act, and a policy might not work if organizations cannot practically implement it. My education has helped me approach these issues from multiple angles instead of viewing every cybersecurity issue as simply technical.

Conclusion

Making my ePortfolio was my chance to reflect on the knowledge and skills I have acquired in the pursuit of my cybersecurity degree from Old Dominion University. These nine artifacts exemplify how I have advanced my skills in technical cybersecurity, research and critical thinking, and communication and professionalism. I was able to gain greater insight into security threats, access control, availability, and critical infrastructure in my technical coursework. I am able to evaluate information, investigate policies, and understand the interaction of cybersecurity and society in my research coursework. My internship with Place4Us enabled me to relate my classroom learning to applied cybersecurity research and professional communication.

Viewing these experiences together made me see that I hadn't completed my classes in isolation. Technical skills allowed me to understand the technical issues, research enabled me to evaluate those issues, and communication gave me the tools to communicate what I found. I also realized that cybersecurity isn't just about technology. It's about people, businesses, privacy, policies, and the ramifications of our decisions. I think the knowledge and skills I've gained in my degree have prepared me to move into the next stage of my career while providing a solid foundation to build on as I gain more experience.

References

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*.

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 New Security Paradigms Workshop*, 133–144. https://doi.org/10.1145/1719030.1719050

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work, 24*, 371–390. https://doi.org/10.1007/s10111-021-00683-y

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29*(2), 38–47. https://doi.org/10.1109/2.485845

Zych, I., Baldry, A. C., Farrington, D. P., & Llorent, V. J. (2019). Are children involved in cyberbullying low on empathy? A systematic review and meta-analysis of research on empathy versus different cyberbullying roles. *Aggression and Violent Behavior, 45*, 83–97. https://doi.org/10.1016/j.avb.2018.03.004