Personal Narrative Essay

Zufan Abebe

Old Dominion University

IDS 493 – Interdisciplinary Studies

Professor Carin Andrews

July 30, 2025

Abstract

This personal narrative explores my journey from a healthcare background to a career in cybersecurity. The essay highlights key milestones, including my transition from pharmacy technology, participation in the Year Up program, an internship with Becton Dickinson, and consulting work with MedCrypt. Through real-world experience and academic growth, I developed a strong passion for protecting medical technology and ensuring the safety of patients. This essay reflects my personal story, identity, and the professional direction I am proud to follow. It is not only a reflection of my path but also an expression of my long-term commitment to making cybersecurity more human-focused, especially in healthcare.

Before Cybersecurity: My Healthcare Background

Before pursuing a career in cybersecurity, I worked in the healthcare industry, more specifically as a pharmacy technician. My time in pharmacy allowed me to see the impact of healthcare systems on people's lives. I became familiar with regulatory requirements, patient safety protocols, and the importance of accuracy in medication handling. These responsibilities required precision, trust, and accountability, qualities that would later guide me in cybersecurity.

Working closely with patients and healthcare professionals made me realize how essential it is to protect sensitive data and maintain trust in the healthcare system. My role required constant attention to detail and a sense of responsibility that naturally carried over into the world of cybersecurity. Over time, I began to understand that technology was playing an increasingly important role in healthcare, and I wanted to be part of the movement to make it safe and secure. That curiosity set me on a new path.

My Journey into Cybersecurity

In 2021, I joined the Year Up program, an intensive workforce development initiative designed to close the opportunity gap for young professionals. I selected the cybersecurity certification track, which gave me foundational knowledge in risk management, threat analysis, and system security. The hands-on learning and mentorship through Year Up provided me with more than just technical skills. It gave me confidence and a support system to pursue a new career.

After six months of training, I earned an internship with Becton Dickinson (BD), a global leader in medical technology. At BD, I worked as a product security engineering intern and

became extremely interested in cybersecurity for medical devices. This internship opened my eyes to how digital threats could directly affect patient safety and healthcare delivery. This type of hands-on experience helped me translate the academic knowledge I gained from the training into real-world experience.

Being part of that team inspired me. I saw how even a small vulnerability could lead to patient harm. This made my work feel important and personal. I wanted to be someone who made a difference behind the scenes, ensuring that medical devices functioned safely and securely. I also discovered how critical teamwork and clear communication were in this field, as I often collaborated with developers, engineers, and compliance teams to create a shared understanding of security goals.

Experience at BD: Cybersecurity in Action

My role at BD introduced me to the challenges of securing medical devices in both premarket and post-market environments. I worked with industry standards such as the National Institute of Standards and Technology (NIST) Risk Management Framework and contributed to threat modeling, risk assessments, and remediation planning. This experience showed me the real-world impact of cybersecurity and how it can affect people's health and well-being.

It also helped me develop cross-functional communication skills as I collaborated with engineers, compliance teams, and clinical stakeholders. The ability to bridge technical work with regulatory language became one of my strongest assets. I participated in weekly meetings with global teams and presented security findings to internal stakeholders, which helped me grow more comfortably in my professional voice. This role helped me build a strong foundation in product security and understand the full lifecycle of device development.

Professional Growth at MedCrypt

After BD, I joined MedCrypt as a cybersecurity consultant, where I helped lead medical device manufacturers conduct gap assessments and prepare for regulatory submissions. My work involved reviewing product architectures, aligning controls with Food and Drug Administration (FDA) guidance and supporting remediation efforts. I became skilled in applying NIST 800-53, TIR 57, SW 96, (International Organization for Standardization) ISO 14971 and 13485, and FDA pre- and post-market cybersecurity guidance.

This consulting job helped me learn more about cybersecurity regulation around medical devices and how to protect patients from harm by incorporating cybersecurity in the product development phase. I also helped translate technical risks into language that executive and regulatory teams could understand. I took pride in helping organizations close security gaps that could impact real people. These conversations with engineers, product teams, and compliance officers helped me grow into a more thoughtful and effective security professional.

I also had the opportunity to work on projects that prepared manufacturers for FDA audits and submissions, which deepened my knowledge of the regulatory landscape. MedCrypt exposed me to a variety of devices and risk profiles, which made me more adaptable and improved my ability to assess a broad range of security challenges.

Academic Development at Old Dominion University

Alongside my work experience, I pursued academic training at Old Dominion University, majoring in Cybersecurity. Courses such as CYSE 406 (Cyber Law), CYSE 450 (Ethical Hacking and Penetration Testing), CYSE 250 (Basic Cybersecurity Programming and

Networking), CS463 (Cryptography for Cybersecurity), CS 464 (Networked Systems Security) and IDS 300W (Writing in the Disciplines) helped me build both technical and communication skills and understand how cybersecurity problems translate into different societies and geopolitical environments.

I worked on projects involving malware analysis, vulnerability scanning, ethical hacking, and cryptography using tools like Any.Run, Metasploit, and Wireshark. These experiences gave me confidence in my technical abilities and my capacity to contribute to real-world security problems. I also developed the ability to explain complex concepts clearly, a key skill in collaborative environments. My academic work allowed me to connect theories with hands-on practices, which made me a more balanced and effective cybersecurity professional.

Challenges and Resilience

My path has not been easy. Balancing school, work, and family responsibilities has tested my resilience, but it has also built my determination. I faced periods of uncertainty, including job loss and family health challenges, but I never gave up on pursuing a meaningful career. Each time I encountered a setback, I tried to see it as a setup for a comeback.

There were nights when I stayed up late studying after putting my child to bed or moments when I questioned if I would be able to finish my education. But I reminded myself of the future I was building for myself and for my family. Every setback became a lesson, and every success reminded me of why I started this journey. These experiences taught me that perseverance and flexibility are just as important as technical skills in the cybersecurity field.

Conclusion: Looking Ahead

My story is still being written, but my direction is clear. I aim to continue my work in cybersecurity with a focus on healthcare technology, product security, and compliance. I believe in designing systems with security from the start and advocating for safety and trust in medical innovation.

Cybersecurity is not just a job for me. It is something I care about deeply. I bring technical skills, lived experience, and a strong interdisciplinary perspective to every role I take on. I believe that technology should work for people, not against them. As I continue my journey, I hope to be part of teams that prioritize ethical, secure design, especially in spaces where lives are on the line. I want to help shape a future where security is not an afterthought but a foundation.

This reflects what Nguyen describes as using ePortfolios to connect past learning with future identity. According to Smith, we often tell two kinds of personal stories, one of growth and one of consistency, and my journey reflects both. As I move forward, I hope my story will inspire others who come from nontraditional backgrounds to see themselves in this field and to know that their voice matters in shaping the future of technology.

References

Nguyen, C. F. (2013). The ePortfolio as a living portal: A medium for student learning, identity, and assessment. International Journal of ePortfolio, 3(2), 135–148.

Smith, E.E (2017, January 12). The two kinds of stories we tell about ourselves [video]. TED Conferences. https://ideas.ted.com/the-two-kinds-of-stories-we-tell-about-ourselves/