A Reflective Journey: Navigating Your Cumulative Experience at Iowa State University

Anish Nag

My journey at Iowa State University has been nothing short of exciting and fulfilling. Embarking on this path to becoming a cybersecurity engineer has fundamentally transformed not only my technical abilities but also my perspective on what it means to be a lifelong learner and ethical engineer. From writing my first lines of code as a freshman to designing a complex computer processor and analyzing sophisticated cybersecurity threats, the past three years have challenged me to grow in ways I never anticipated.

. This transformation did not happen just within lecture halls; it came through experiences that included diving deep into various clubs and organizations, engaging with professional cybersecurity and development communities, adapting my learning strategies, and constantly pushing beyond my comfort zone. As I reflect on my undergraduate journey, I want to explore how these interconnected experiences have shaped my approach to problem-solving, prepared me to tackle complex engineering challenges, and instilled in me the mindset necessary for continuous professional growth in an ever-evolving field like cybersecurity.

The foundation of my engineering mindset was set through Iowa State's systematic approach to building both technical depth and critical thinking skills. My journey truly began with the fundamentals of coding in C. Learning to code in this language as someone who had never written a line of code before college was genuinely one of the hardest things I have ever done. It seemed like an insurmountable challenge trying to learn the syntax and develop the logical mindset to code, but the feeling I got as I progressed through the course and started picking up pace was rewarding. I gradually improved, moving onto Object Oriented

Programming in Java, culminating in the rigorous problem-solving demands of Data Structures, which remains one of the most challenging yet transformative courses I've taken. This progression taught me that mastering complex engineering concepts requires patience, persistence, and a willingness to embrace initial confusion as part of the learning process.

However, the true test of my holistic engineering development came through my first major cybersecurity lab in my CybE/CprE 230 Network Fundamentals class. I was tasked with analyzing a live enterprise-level network for my final using industry-standard SOC tools like Splunk SIEM and Suricata IDS. This experience demanded far more technical proficiency because it required me to think critically, remain skeptical of apparent normalcy among logs and findings, pay meticulous attention to detail to make sure I did not miss anything at all, and communicate security findings through precise technical reports. While sifting through alerts, identifying vulnerabilities, and implementing mitigation strategies, I realized I wasn't learning just cybersecurity tools; I was developing the analytical mindset and communication skills essential for protecting organizations and their stakeholders from real-world threats.

The power of this foundation was clear when I began applying classroom knowledge to practical knowledge. The network defense and attack fundamentals I learned did not remain confined to just academic assignments and exercises; they became the backbone of my performance in cyber defense competitions, internships, and various types of hacking competitions. What started as a theoretical understanding of attack vectors and defensive strategies transformed into hands-on expertise as I delved deeper into penetration testing, red teaming exercises, and platforms like TryHackMe and HackTheBox. Through CTF competitions, I discovered that the critical thinking and systematic problem-solving approaches developed in

my coding classes were directly applicable to cybersecurity challenges, demonstrating how Iowa State's multifaceted curriculum prepared me to synthesize knowledge across disciplines.

My education at Iowa State extends far beyond the confines of traditional coursework through active engagement with the external resources and professional communities that allowed me to grow. I recognized early that cybersecurity evolves very quickly and very often, so I made it a priority to stay current with industry developments through HackerNews, cybersecurity blogs, and specialized forums where practitioners share real-world insights and emerging threats. This habit of seeking external knowledge became invaluable when I joined Iowa State's Hacking and Security Club, where weekly meetings exposed me to advanced hacking challenges, CTFs, and cyber defense competitions that pushed my skills beyond classroom boundaries. The competitive environment proved to be transformative, earning first, second, and third-place finishes in various cyber defense competitions over the past couple of years. This taught me not just technical skills, but how to perform under pressure and think strategically about complex security scenarios.

Iowa State's career services and industry connections also opened doors I never could have accessed alone. Through the university's career fair, I secured my first internship at John Deere as a freshman, an opportunity that would define my professional trajectory over three consecutive summers. Each internship I had at John Deere since then demanded that I adapt and refine my knowledge in different ways. My first role as a security software engineer intern allowed me to apply programming methodologies and thinking from my coursework, but my second internship in GRC Third Party Risk Management introduced me to a completely new territory that wasn't covered in any class. I had to quickly understand and master governance, risk management, and compliance frameworks while learning to communicate complex technical

risk to business stakeholders. This experience taught me that successful engineers must be comfortable operating outside their formal training and continuously acquiring new competencies.

The culmination of this adaptive learning and being under pressure came during my third internship as an Embedded Security Engineer on the Red Team, essentially a paid ethical hacker. This is where I faced some of the most technically challenging work of my career. Embedded hacking required me to synthesize knowledge from my computer engineering courses, attack fundamentals training, and coding classes while developing entirely new skills in hardware-level security analysis. The rigorous and demanding course schedule I had navigated at Iowa State proved to be really good preparation for this specialized role because the ability to persist through difficult material work under pressure and rapidly absorb difficult technical concepts became my greatest assets. Beyond the technical learning, my involvement with professional organizations like SecDSM and attendance at BSides conferences expanded my professional network and exposed me to cutting-edge research and industry best practices, reinforcing that lifelong learning in cybersecurity requires both formal education and continuous engagement with the broader security community.

Looking back to how I approached my education as a freshman, I recognize that the most valuable lessons often come from understanding what I would approach differently with the wisdom I've gained. If I could restart my undergraduate experience, the first change I would make would be to immerse myself in cybersecurity conversations and competitions from day one. Rather than waiting until my sophomore year to engage with cybersecurity outside of the classroom, I would have seized every opportunity as a freshman, joining competitions, failing early, and learning from those failures when the stakes were lower. This earlier engagement

would have not only accelerated my technical development by a full year but also fostered the collaborative learning environment that comes out when peers and professors discuss complex cyber challenges together. The critical thinking skills, innovative ideas, and community bond that develop through these interactions are invaluable.

My learning strategies have changed dramatically since my freshman year, transforming from passive absorption to active application and synthesis. Where I once approached difficult material with hesitation, I now jump directly into challenging tasks, having learned that consistent daily effort yields far better results than last minute cramming. My current approach emphasizes asking extensive questions, taking comprehensive notes, and immediately applying classroom concepts to real-world scenarios. Most importantly, I've discovered that teaching others what I've learned significantly enhances my own retention and understanding. This evolution in methodology has completely changed my relationship with difficulty. I do not fear challenging situations but actively seek them out, having grown comfortable with operating in uncomfortable environments where the most significant learning happens.

Looking toward my future as a cybersecurity professional, I envision myself in several key areas for continued growth and contribution. My immediate focus centers on deepening my expertise in red teaming and penetration testing while expanding into vulnerability research and security analysis, where I can contribute to the broader security community. I plan to continue developing my coding skills and technical capabilities with the goal of becoming a subject matter expert in cybersecurity. Beyond technical growth, I'm committed to giving back to the community that has shaped me through continued participation in conferences and meetups, delivering presentations on cybersecurity topics, and eventually returning to Iowa State, possibly as a part-time instructor and red teamer during the cyber defense competitions. My long-term

vision includes transitioning into leadership roles such as CISO or CTO, where I can apply everything I've learned to protect large-scale businesses and organizations. This trajectory reflects my understanding that cybersecurity expertise must be coupled with leadership skills and a commitment to continuous learning in a field that evolves as rapidly as the threats we work to defend against.

Now that I am in my final year at Iowa State, I realize that my journey represents more than personal growth; it reflects a fundamental shift in how the next generation of cybersecurity professionals must be prepared to tackle an increasingly interconnected and vulnerable digital world. The freshman who struggled with basic C syntax has now grown into someone who does not just want to defend against cyber threats, but someone who envisions fundamentally changing how we approach cybersecurity education and industry practice.

The traditional model of cybersecurity training often treats technical skills, communication, and ethical reasoning as separate competencies. However, my experiences have shown me that the most pressing cybersecurity challenges, from nation-state attacks to AI-powered threats, require professionals who can think holistically across all disciplines, adapt rapidly to emerging technologies, and bridge the gap between technical complexity and human understanding. This realization gave me a certain purpose: To help contribute to and create a new paradigm where cybersecurity professionals are not just defenders, but educators, innovators, and community builders who can democratize security knowledge and make robust security accessible to all organizations.

My goal extends beyond becoming another cybersecurity expert. I want to be part of the generation that transforms how we prepare for and respond to cyber threats.