The Reality of Studying Cybersecurity vs. Real-World Expectations

Erik Sorto

Old Dominion University

IDS 300W: Interdisciplinary Theory and Concepts

Professor Kathryn Lafever

April 25, 2025

Reality vs. Real-World Expectations: Studying Cybersecurity

The cybersecurity industry is booming at a phenomenal rate. Global digital transformation and cyber threats create more need for professionals. However, rising demand for IT professionals does not mean easy employment paths for students. Many cybersecurity graduates face harsh reality in the workforce. They get degrees but are often underprepared for real-world jobs that require certifications, hands-on experience, technical experience, and soft skills. Employers expect instant job-readiness whereas academic institutions tend to be more concerned with foundational theory. This research paper examines how students learn about cybersecurity in programs versus what the industry expects. This research will examine why this is so, identify how education, workforce development and cybersecurity/IT contribute to it and offer interdisciplinary strategies for improving career outcomes.

Justifying an Interdisciplinary Approach

The complexity of this issue cannot be addressed in one disciplinary way or perspective. The issue, however, intersects across education, workforce development and cybersecurity/IT with each bringing insight. Education provides knowledge regarding curriculum development and pedagogical models and strategies. Workforce development contributes labor trends, hiring practices & sociological implications of employment barriers. Cybersecurity / IT provides technical perspective on job demands / job prospects. Only by combining these perspectives can we understand why students have trouble transitioning from classroom to career and design solutions that reflect this

complexity.

Literature Review Across Disciplines

Education

Some academic institutions try to offer cybersecurity programs that meet industry needs, but few succeed. Yusuf (2024) claims slow curriculum reform and inadequate faculty training prevent program effectiveness. Most universities put accreditation standards and theory before practice. Chen, Becker & Davis (2021) concluded that experiential learning in the form of labs, project-based courses and simulations improves student preparedness. Yet some schools make certifications and lab experience optional instead of required. Another problem is that students often receive general IT instruction without much specialization - leading to career confusion in cybersecurity.

Workforce Development

For workforce development purposes the job market reflects an imbalance between academic output and employer demand. Cybersecurity ranks among the fastest growing fields yet there is a talent shortfall, according to the National Center for Science and Engineering Statistics (2023). However, the hiring process often has unrealistic expectations like three to five years of experience for entry-level jobs. These demands are particularly trivial for underrepresented students who may not have access to internships, portfolios with documented self-driven projects or professional networks, Burrell (2018) notes. Certifications, networking and real-life projects are used by employers instead of

degrees as indicators of job readiness. This creates a paradox: Students study cybersecurity for good jobs, then are unqualified upon graduation.

Cybersecurity/IT

Cybersecurity as a field is dynamic and requires the intitiative to never stop learning and keeping up to date with new policies, laws and threats. Tools and techniques used today might be outdated in a few years. This requires ongoing learning. Goupil, Smail, and Desmet (2022) stress that employers want practical skills more than academic credentials. Capture The Flag (CTF) competitions, CompTIA Security+ certifications and building a home lab are seen as indicators of motivation and competence. Industry forums and job listings often say certifications are the minimum and self-learning is expected. Students whose only focus is their coursework are often behind those who actively seek out extracurricular learning opportunities.

Additional Perspectives from Practice

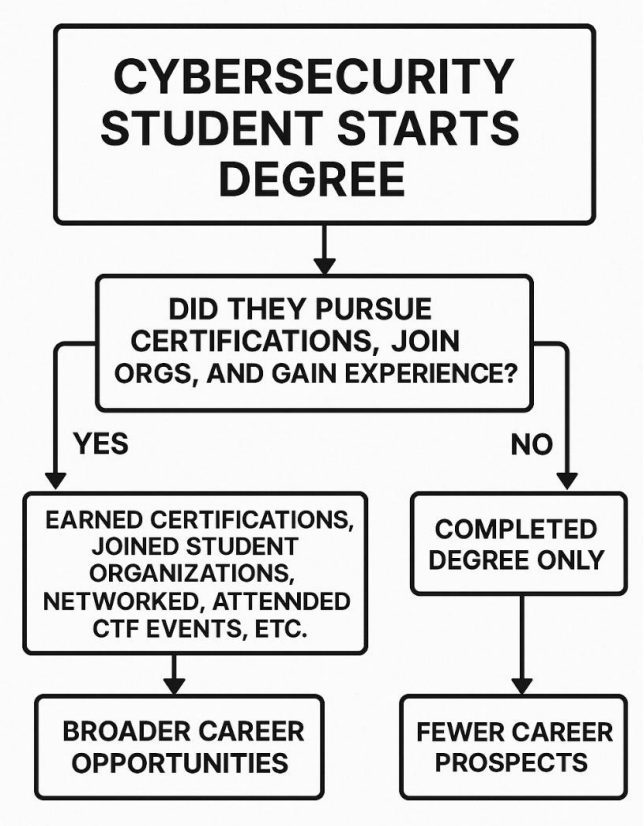
Student attendees at conferences and cybersecurity clubs, internships and local meetups often gain significant career advantages compared to students who do not partake in such extracurricular activities. Such practices are seldom embedded in curricula but are essential for success in the field. Defending the preparation gap has been a priority for the Department of Homeland Security and National Institute of Standards and Technology (NIST) through public-private partnerships and structured internship pipelines. Such programs are underused by schools and under-marketed to students.

Synthesis and Common Ground

A horizontal causal integration strategy explains how overlapping problems appear from each discipline. From education we understand the institutional limitations of curriculum development. From workforce development we see rigid hiring systems that are often skewed toward the privileged and the accessible. From cybersecurity/IT we learn that employers want hands-on, real-world technical expertise.

Despite their differences in industry, these disciplines agree on some key points. First, everyone agrees that hands-on learning is important. Second, they understand the value of ongoing, self-directed learning. Third, it seems that academia and industry collaboration can benefit students and greatly give them a deeper insight on the reality of what is required to succeed. Institutions could require certifications as part of graduation criteria and employers could offer more paid internships or junior-level apprenticeships to build job readiness. It will ultimately take major collaboration and joint efforts to address the issue and solve this problem.

Visual Argument



In this flowchart, it illustrates how student outcomes differ across extracurricular engagement. One path shows a student who gets the degree but has trouble finding work. A different route leads a student to certifications, cybersecurity associations, networking with professionals and cybersecurity events. That student is prepared, confident and likely to get a job. This image contextualizes the issue in real-world terms and supports the interdisciplinary findings by visual mapping consequences of action versus inaction. This approach aligns with Nissani's (1995) concept of a 'fruit smoothie' interdisciplinarity, where distinct disciplines are blended into a cohesive analysis.

Conclusion

The cybersecurity workforce gap is more than a shortage of labor - it's a reflection of

misaligned systems. Education, employers and students all play their part. Universities must remake curricula to emphasize real-world readiness by including certifications, labs and internships. Employers must lower unrealistic experience expectations for entry level roles and provide opportunities for those willing to learn. Those skills, credentials and networks that employers require must come from outside the classroom. We identify the causes of this problem and propose solutions that will enable future cybersecurity professionals to graduate and thrive through interdisciplinary work.

References

Burrell, D. N. (2018). Women and minorities in cybersecurity: Addressing the gaps. *Journal of Strategic Innovation and Sustainability*, 13(1), 29–33.

Chen, J., Becker, B., & Davis, M. (2021). Pathways to cybersecurity: Designing engaging curriculum from K-12 to college. *International Journal of Computer Science Education in Schools*, 5(1), 105–110.

Goupil, G., Smail, L., & Desmet, P. (2022). An exploratory study of job readiness in cybersecurity education. *Journal of Cybersecurity Education, Research and Practice*, 2022(1), 475–485.

National Center for Science and Engineering Statistics. (2023). *Cybersecurity Workforce Statistics and Labor Trends*.

Repko, A. F., & Szostak, R. (2020). *Interdisciplinary research: Process and theory* (3rd ed.). SAGE Publications.

Sorto, E. (2025). *Visual argument: Cybersecurity career pathways flowchart* [Infographic]. Canva.

Yusuf, I. (2024). Cybersecurity education reform: Bridging the industry-academic gap. *Journal of Technology and Education*, 10(2), 5–12.