Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2022 TREOs | TREO Papers

12-12-2022

Building a Cross Disciplinary Cybersecurity Program in the IS Department

Arun Aryal
California State University Los Angeles, aaryal@calstatela.edu

Follow this and additional works at: https://aisel.aisnet.org/treos_icis2022

Recommended Citation
Aryal, Arun, "Building a Cross Disciplinary Cybersecurity Program in the IS Department" (2022). *ICIS 2022 TREOs*. 39.
https://aisel.aisnet.org/treos_icis2022/39

This material is brought to you by the TREO Papers at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2022 TREOs by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

TREO
Technology, Research, Education, Opinion

Building a Cross Disciplinary Cybersecurity Program in the IS Department

Piecemeal Approach to Building a Cybersecurity Program

Arun Aryal, aaryal@calstatela.edu

Global demand for cybersecurity professionals is growing, and organizations are struggling to find qualified applicants (Crumpler et al., 2019). Responding to these shortages, the National Security Alliance (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program by promoting higher education and research in security to increase cross-disciplinary cybersecurity experts. In creating this cybersecurity program to align with NCAE programs, universities must focus on the standards, such as establishing a standard cybersecurity curriculum, competency development, and community outreach. The NSA and DHS provide guidelines on "what" to focus on but lack suggestions on "how" to accomplish these goals.

Implementing these guidelines is challenging. Some criticisms include the certification-oriented focus vs. academic degree focus and the lack of resources. Certification programs are not substitutions for academic learning objectives (Wang et al., 2019). The main problem with using NCAE guidelines for college-level curriculum development is that the goals of NCAE focus more on specific job areas. In contrast, academic education emphasizes a fundamental understanding of principles and concepts and their applicability in practice. Funding also remains a challenge, specifically for public teaching universities forcing the faculty to become program administrators in addition to their regular duties such as teaching, course development, student mentoring, and research.

In this report, I will outline our incremental and iterative approach to building a cybersecurity program. The initial focus was on merging the degree's professional certification and accreditation requirements by redesigning our courses, where students would earn two entry-level professional certifications as part of their coursework. Addressing the resource constraints, we partnered with an organization to provide certification materials, including cloud-based cybersecurity labs, to our students. In addition, we created a partnership with ISACA (a global association of IT professionals) to engage students with professional development and networking opportunities. Despite the challenges, IS departments should build a cybersecurity program that can engage students, faculty, and the industry.

References

Crumpler, W., & Lewis, J. A. (2019). The cybersecurity workforce gap (p. 10). Washington, DC, USA: Center for Strategic and International Studies (CSIS).

Wang, P., Dawson, M., & Williams, K. L. (2019). Improving cyber defense education through national standard alignment: case studies. In National security: Breakthroughs in research and practice (pp. 78-91). IGI Global.