Spring 3-16-2024

Cybersecurity Course For Business: A structured Pedagogical Approach For Business Students

Ashraf Mady

Denise McWilliams

CYBERSECURITY COURSE FOR BUSINESS: A STRUCTURED PEDAGOGICAL APPROACH FOR BUSINESS STUDENTS

Ashraf Mady
University of North Georgia
ash.mady@ung.edu

Denise McWilliams
University of North Georgia
denise.mcwilliams@ung.edu

EXTENDED ABSTRACT

Cybersecurity continues to be an essential area of study due to the increasing reliance on digital technologies in the corporate world, as well as the pervasive nature of cybersecurity threats. The advancement of technology has elevated the importance of cybersecurity in research and practice, emphasizing the need for business students to develop a strong foundation in cybersecurity principles and practices (Mahmood, Chadhar, & Firmin, 2022). The growing prevalence of cyber threats in the digital landscape underscores cybersecurity education's critical importance for business students. Additionally, incorporating cybersecurity education into business majors is crucial, as it addresses the interdisciplinary nature of cybersecurity and its relevance to business operations (Cram & D'Arcy, 2016).

Research supports the importance of integrating cybersecurity studies in various business majors. For example, the increasing prevalence of cyber threats and attacks necessitates a comprehensive understanding of cybersecurity frameworks and information security standards for business students entering the management field (Taherdoost, 2022). The evolving digital landscape has brought forth challenges for the accounting profession, calling for an understanding of cybersecurity to mitigate potential risks (Haapamäki & Sihvonen, 2019). Additionally, the marketability of options for meeting the 150-hour requirement in public accounting firms has been explored, indicating the importance of cybersecurity knowledge for job candidates in the accounting field (Mauldin et al., 2013). The reliance on online platforms for marketing activities has heightened the importance of cybersecurity in protecting sensitive consumer data and ensuring the integrity of marketing operations (Fedele & Roner, 2021). In the finance field, understanding cybersecurity is essential in preventing fraudulent transactions and ensuring financial data security (Pang et al., 2019).

Research emphasizes the need for a collective effort to enhance cybersecurity education and awareness, particularly in the business context (Haney & Lutters, 2017). However, research shows that many students in business majors have little background or training in cybersecurity, making it difficult for them to grasp basic terminology and concepts without significant remediation (Holdford, Pontinha, & Wagner, 2022). There is a gap between the needed and produced graduates with holistic training suitable for effective cyber threat protection and response, indicating a challenge in cybersecurity education for business majors (Trumbach et al., 2022). As businesses continue to face cyber threats, it is imperative for business students to acquire a comprehensive understanding of cybersecurity principles and practices. This research aims to address this need by answering the question: How can cybersecurity topics be included in the curriculum of business disciplines? Sánchez et al. (2020) propose an integral pedagogical strategy for learning IoT cybersecurity, emphasizing the importance of a structured approach in higher education institutions. The National Initiative for Cybersecurity Education (NICE) established the Cybersecurity Workforce Framework (Petersen et al., 2020). This framework provides a comprehensive structure for understanding the skills and competencies required in the cybersecurity workforce, which is relevant for business majors (Newhouse et al., 2017). This work proposes a well-structured pedagogical approach recommended by researchers within the NICE framework provided by professionals to provide holistic training suitable for business students.

Keywords

Cybersecurity, education, workforce training, cyber skills, NICE framework, pedagogy.

REFERENCES

1. Cram, W. A., & D'Arcy, J. (2016). Teaching information security in business schools: Current practices and a proposed direction for the future. *Communications of the Association for Information Systems*, *39*(1), 3.
2. Fedele, A. and Roner, C. (2021). Dangerous games: a literature review on cybersecurity investments. *Journal of Economic Surveys*, *36*(1), 157-187. https://doi.org/10.1111/joes.12456
3. Haapamäki, E. and Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808-834. https://doi.org/10.1108/maj-09-2018-2004

4. Haney, J. M., & Lutters, W. G. (2017, May). The work of cybersecurity advocates. *In Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 1663-1670). https://doi.org/10.1145/3027063.3053134
5. Holdford, D. A., Pontinha, V. M., & Wagner, T. D. (2022). Using the business model canvas to guide doctor of pharmacy students in building business plans. *American Journal of Pharmaceutical Education, 86*(3), 8719. https://doi.org/10.5688/ajpe8719
6. Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies*, 2022, 1-11. https://doi.org/10.1155/2022/7384000
7. Mauldin, D., Braun, R., Viosca, R., & Chiasson, M. (2013). The marketability of options for meeting the 150-hour requirement: an empirical analysis of public accounting firm recruiting intentions. *Issues in Accounting Education, 28*(3), 537-553. https://doi.org/10.2308/iace-50448
8. Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST special publication, 800*(2017), 181.
9. Pang, G., Shen, C., & Hengel, A. (2019). Deep anomaly detection with deviation networks.. https://doi.org/10.1145/3292500.3330871
10. Petersen, R., Santos, D., Smith, M., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE framework)* (No. NIST Special Publication (SP) 800-181 Rev. 1 (Withdrawn)). National Institute of Standards and Technology.
11. Sánchez, J., Mallorquí, A., Briones, A., Zaballos, A., & Corral, G. (2020). An integral pedagogical strategy for teaching and learning IoT cybersecurity. *Sensors, 20*(14), 3970.
12. Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics, 11*(14), 2181. https://doi.org/10.3390/electronics11142181
13. Trumbach, C., Payne, D., & Walsh, K. (2022). Cybersecurity in business education: the 'how to' in incorporating education into practice. *Industry and Higher Education, 37*(1), 35-45. https://doi.org/10.1177/09504222221099389