An Interdisciplinary Approach to Experiential Learning in Cybersecurity and Agriculture Through Workforce Development

Kellie Johnson (Kelliej@vt.edu)
Dr. Tiffany Drape (Tdrape@vt.edu)
Dr. Joseph Oakes (Jcoakes@vt.edu)
Dr. Joseph Simpson (Jjsimpson@vt.edu)
Dr. Anne M. Brown (Ambrown7@vt.edu)
Dr. Donna Westfall-Rudd (mooredm@vt.edu)
Dr. Susan Duncan

Virginia Polytechnic Institute and State University
Agricultural Leadership and Community Education

175 West Campus Drive
Blacksburg, VA 24061
(404) 643-0063

Introduction

Cybersecurity in food and agriculture (F+A) is a steadily growing industry that increasingly needs individuals to enter the workforce. The increase in vulnerabilities of the current food supply can potentially threaten the global food system (Duncan et al., 2019). To combat these potential threats, professionals should have the necessary training and ability to build relationships and communicate across multiple disciplines and organizations to develop solutions (Richardson et al., 2019). However, due to the high advancement of technologies in cybersecurity in F+A, gaps exist in the training and development for professionals entering the field. Students enrolled in colleges of agriculture and life sciences have limited opportunities to integrate data management and security into (F+A) areas of study. There is a growing need for individuals in agricultural and life sciences fields to be more prepared and versed in topics related to data and cybersecurity (Drape et al., 2020). These gaps can lead to data security risks and information transfer in various technologies. Studies show that graduates from cyber studies should possess the necessary soft skills, critical thinking, and capabilities to solve problems and obtain transferable skills needed in the workforce (Jones et al., 2018, as cited in Payne et al., 2020).

This qualitative study aimed to deliver an experiential learning-focused course that integrated the interdisciplinary areas of data sciences and agriculture with early-career undergraduates interested in learning about and pursuing a career around cybersecurity in F+A. The research questions guiding this study were: What do students seek to understand about cybersecurity in F+A and workforce development? How do students conceptualize which skills learned in class to be transferable to the workforce?

Theoretical Framework

The theoretical framework for this study relies on the Experiential Learning Theory (EL) developed by David Kolb (1984). EL theory theorizes the process of learning and obtaining knowledge cultivated through experiences, perception, and cognitive behavior (Kolb, 1984, as cited in Fai Ng et al., 2018). Kolb proposed a four-stage cycle model of knowledge and development; concrete experience, reflective observation, abstract conceptualization, and active experimentation (Yardley et al., 2012). This study proposed to use a scalable EL-based course to integrate data science, F+A, and industry partners in a novel learning experience. This study utilized the first three steps of the model; concrete experience, reflective observation, and abstract conceptualization.

Methodology

This study population consisted of nine undergraduate students from Virginia Tech who participated in a course taught alternately by the professor of record, teaching assistant, workforce and career development professionals, and F+A cybersecurity experts. Weekly reflections were assigned at the end of each class. The data consisted of 12 weeks of responses, geared toward different aspects of the course content. As part of the coding

process, *in vivo* was conducted to determine what meaningful patterns were emerging to make up sub-categories of data based on the conversation and other audio-based recordings and by-products collected using Atlas ti (Charmaz, 2006). The data was first open-coded, categorized into major themes, and then focused coding was conducted to identify any repeating patterns to understand the multi-layer meaning (Creswell et.al., 2007). The resulting codes began to explain larger data segments related to perceptions of cybersecurity in F+A. Focused coding helped determine the adequacy of the *in vivo* codes (Charmaz, 2014). Axial coding was conducted as the final step of the coding process, helping the researchers bring all the data together and determine themes based on the research questions (Corbin and Strauss, 2008). The development of the codebook emphasized the action-oriented nature of language in which participants discussed experiences of being a participant in this interdisciplinary course from their viewpoint (Roth, 2008).

Findings

Three themes emerged from the data: 1) students gained industry knowledge related to their academic engagement, 2) students established internship expectations and aspirations, and 3) workforce training and development were essential for students to succeed in future career placement. A participant articulated a gain in industry knowledge by stating, “It was most helpful to have discussions with industry professionals and hear their opinions and experiences from a professional point of view.” Additionally, a participant was able to identify internship expectations by stating, “Having clear guidance and understanding of the day-to-day functions of the organization and supervisory support is important”. Lastly, a participant found that workforce training and development were essential by stating, “Resume building, internship performance, and effective communication skills in the workplace were the most important tools needed to enhance their all-around development for entering the workforce.” The results of the experiential learning course consisted of an overview and analysis of the workforce development training in the area of cybersecurity in F+A and how those skills transfer over into students' internship experience.

Conclusions and Recommendations

The interplay between students across disciplines is essential for careers in cybersecurity within food supply chains, technology adoption, and efficiencies in F+A. Considering the lack of knowledge and training available for young professionals entering the cybersecurity workforce in F+A, future professionals need to integrate more experiential learning teaching and learning strategies around agriculture, cybersecurity, and training (Drape et al., 2020; Duncan et al., 2019). Therefore, engagement with industry professionals, workforce development workshops and training, and autonomy in addressing professional needs to be successful in the workforce are important themes to consider when building an experiential learning-based experience for students in higher education. Developing a knowledgeable workforce will benefit several sectors in cybersecurity-related fields and expand workforce development opportunities for students when they complete their degree programs and enter the workforce.

References

Angyalos, Z., Botos, S., & Szilagyi, R. (2022). The importance of cybersecurity in modern agriculture. *Journal of Agricultural Informatics*, 12(2). https://doi.org/10.17700/jai.2021.12.2.604 (Original work published June 15, 2021)

Charmaz, K. (2014). *Constructing grounded theory*. Sage Publications.

Corbin, J., & Strauss, A. (2008). Strategies for qualitative data analysis. *Basics of Qualitative Research. Techniques and procedures for developing grounded theory*, *3 195-228*

Creswell, J., & Plano Clark, V. (2007). *We are designing and conducting mixed-methods research*. Sage Publications.

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system. *Frontiers in Bioengineering and Biotechnology*, *7*. https://doi.org/10.3389/fbioe.2019.00063

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R. S., & Duncan, S. E. (2020). Assessing the role of cyberbiosecurity in agriculture: A Case Study. *Frontiers in Bioengineering and Biotechnology*, *9*. https://doi.org/10.3389/fbioe.2021.737927

Fai Ng, Y., Chan, K. K., Lei, H., Mok, P., and Leung, S. Y. (2019). Pedagogy and innovation in science education: A case study of an experiential learning science undergraduate course. *The European Journal of Social & Behavioral Sciences* Issue 2. https://doi.org/10.15405/ejsbs.254.

Jones, K. S., Namin, A. S., and Armstrong, M. E.(2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Trans. Comput. Educ.* 18, no. 3. https://doi.org/10.1145/3152893.

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Englewood Cliffs, N.J: Prentice‐Hall.

LeClair, J. (2015). *Protecting Our Future, Volume 2: Educating a Cybersecurity Workforce.* v. 3. Hudson Whitman/ Excelsior College Press. https://books.google.com/books?id=bgVCzQEACAAJ.

Payne, B. K., Cross, B., and Vandecar-Burdin, T. (2022). Faculty and advisor advice for cybersecurity students: Liberal arts, interdisciplinarity, experience, lifelong learning, technical skills, and hard work, *Journal of Cybersecurity Education, Research and Practice,* 2021, 17.

Richardson, L. C., Lewis, S. M., & Burnette, R. N. (2019). Building capacity for cyberbiosecurity training. *Frontiers in Bioengineering and Biotechnology,* 7. https://doi.org/10.3389/fbioe.2019.00112

Roth, W. M. (2008). The nature of scientific conceptions: A discursive psychological perspective. *Educational Research Review*, *3*(1), 30-50.

Yardley, S., Teunissen, P. W. & Dornan, T. (2012) Experiential learning: AMEE Guide No. 63, *Medical Teacher,* 34:2, e102-e115, DOI: 10.3109/0142159X.2012.650741