Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #49459

Integrating Industry Certifications into Cybersecurity Education: A Case Study of Professional Certifications in a Foundations of Cybersecurity Course

Christopher Freeze, The University of Oklahoma

Integrating Industry Certifications into Cybersecurity Education: A Case Study of Professional Certification Curriculum in a *Foundations of Cybersecurity* Course

I. The Case Study Introduction

Within the ever-evolving field of cybersecurity, one facet has not changed – a person's need to develop analytical skills, think critically, and solve problems is paramount for success (Sauls & Gudigantala, 2013). For companies seeking to invest in cybersecurity professionals, especially newly graduated students, establishing well-defined onboarding criteria is vital to an organization's and student's long-term success. Similarly, developing and producing industry-ready graduates is a pressing challenge for academic institutions that requires well-defined criteria (Ouh & Shim, 2021). One measure for evaluating an institution of higher learning's cybersecurity program's effectiveness is whether students acquire the knowledge necessary to pass an entry-level cybersecurity industry certification. One widely recognized industry cybersecurity certification is the CompTIA Security+ exam (CompTIA, 2024).

Industry certifications are common among job postings for cybersecurity and information technology positions. Although academic institutions have been advised against teaching solely towards passing a certification exam, the domains covered in these exams can offer valuable insights into evolving industry needs (Knapp et al., 2017). Ngo-Ye and Choi (2016) summarized a few benefits of achieving an industry certification: demonstration of an applicant's competency, skills, and abilities; differentiation among applicants; and development of an applicant's confidence and self-efficacy. One international survey found that "90% of respondents who got a cybersecurity certification before their first job in cybersecurity found it

valuable or very valuable for their career" while 65% say "certifications are the best way to prove knowledge and understanding of concepts" (ISC2, 2024, p. 25).

This case study intends to relate the intentional steps taken by a major mid-western university to incorporate the CompTIA Security+ certification exam topics into an undergraduate, junior-level, *Foundations of Cybersecurity* semester-long course. The program was the first offering of the class in a new undergraduate degree in cybersecurity. The undergraduate degree is housed in the university's Polytechnic Institute. The institute "focuses on high-demand, advanced and applied technology-based education" (OUPI, 2024). Ebneyamini et al. (2018) explained that the use of a case study was valuable in explaining the "how" and "why" questions around a complex single case, particularly in the areas of technology and innovation.

This guidance proved particularly relevant, as intentional decisions were frequently made in response to these two higher-order questions, which consistently demanded explanation, reasoning, and deeper understanding rather than opting for the most readily available solution. Given the early stage of the case, the long-term results or in-depth research needed to provide a detailed assessment is left for future study. The proposition for this case study is identifying what intentional choices were made to integrate an industry certification into a cybersecurity curriculum while meeting the overall learning goals of the class. While the certification qualification itself was not incorporated into the curriculum, the *Foundations of Cybersecurity* course included an expectation that the material would help prepare the students for the certification exam.

II. The Case for Industry Certifications

Integrating industry certifications

Integrating industry certifications into cybersecurity or information security courses is not a new concept. Hentea et al. (2006) produced one of the earliest and most often cited works discussing professional certifications and academia. They concluded that a significant gap often existed between the competencies organizations required of new employees and the capabilities of recently hired graduates, largely due to universities failing to equip students with the necessary knowledge, skills, and abilities to contribute effectively from the outset. Bridging this gap requires a reimagined approach to curriculum development, moving beyond traditional methods that often remain static and outdated. A more holistic approach is necessary that integrates the needs of industry employers, students' educational requirements, and the university's pedagogical priorities.

Towhidi and Pridmore (2023) attempt to address this need for a more holistic approach by acknowledging that successful cyber-related programs must train students to be technically successful in their careers, but also to design a curriculum that incorporates three things: Bloom’s taxonomy, clearly defined outcomes; and diverse instructional methods. Their conclusions come from a study that found curriculum fell into one of two camps: 1) the traditional camps that focus on technology and related labs and exercises, and 2) in much smaller numbers, camps that take a pedagogical approach including building both the technical skills and “skills such as attitudes, motivation, and enjoyment of learning” (p. 71). The two camps represent the dilemma Nilson (2010) highlighted when she advocated that higher education take

"a different and rather novel goal: to educate as many as possible rather than to screen [out all but the best academic students]."

Towhidi and Pridmore's (2023) research underscores the finding that incorporating industry certifications is not considered a panacea while Ouh and Shim (2021) explained that integrating certifications into a curriculum required an intentional, purposeful, and well-thought-out approach that benefited students, faculty, and industry and, as such, the public. Further, industry organizations regularly seek well-rounded employees of which certifications are simply one part of the whole. For example, Tran et al. (2023) identified three hiring criteria among organizations seeking to hire cybersecurity graduates: 1) an academic degree, 2) professional certification(s), and 3) work experience. The professional certifications provide the employer with assurance that as of a certain moment in time, an individual has the requisite knowledge to pass a particular certification exam. However, one challenge in incorporating certifications is the fluidity of cybersecurity and the need to constantly adapt and change curriculum to maintain relevancy (Justice et al., 2022). Consequently, the dynamic interplay between curriculum and certification should continuously drive the learning process forward.

The relevance of industry certifications has been incorporated into the National Initiative for Cybersecurity Education (NICE) Workforce framework through the National Initiative for Cybersecurity Careers and Studies (NICCS) (NICCS, 2024). CompTIA specifically aligns its Security+ certification with the NICE Workforce Framework (CompTIA, 2024). A second challenge in incorporating certifications into curriculum is the potential misalignment between curriculum content and certification topics, which may not correspond on a one-to-one basis. The lack of alignment may necessitate that students not only complete the course curriculum but also study and complete additional materials which were not part of the curriculum to pass the

certification exam. Balancing a full academic course load while studying for the industry certification, scheduling a convenient time to take the certification exam, and paying for the cost of taking the exam adds additional burdens and demands to the students (Ouh & Shim, 2021). Finding ways to alleviate these and other student demands while adhering to a rigorous and comprehensive curriculum should be a goal of higher education institutions.

Considering student study demands

One concern with integrating additional professional certification requirements is the risk of burnout and disengagement among students who may already be taking a full course load, working a part- or full-time job, and navigating the challenges of being a first-generation student. Independently, each of these issues may demonstrate skills valued by employers. However, collectively, without a framework of delineating between study resources and demands, students face the potential of not meeting their academic or career goals (Clements & Kamau, 2018). One framework for helping identify the resources and demands students have available is the Study Demands-Resources (SD-R) theory.

SD-R was popularized by Salmela-Aro and Upadyaya (2014) and based on the Job Demands-Resources theory developed by Demorouti et al. (2001) to study and evaluate burnout. SD-R theory recognizes that effective studying requires time, effort, and motivation, but is often complicated by confusing assignments and unclear learning objectives, which can potentially limit a student's potential. Conversely, students who have effective resources that encourage motivation, buffer student demands, and enhance learning are more likely to achieve their goals and have higher levels of well-being (Bakker & Mostert, 2024).

The challenge of integrating industry certifications and encouraging students to dedicate additional study time to pass a challenging certification exam lies in providing resources that enhance a student's interest and motivation while giving them the flexibility and autonomy needed to achieve their academic and professional goals on their own timetable. Students should not experience undue stress or a sense of failure due to the additional workload (Salmela-Aro & Upadyaya, 2014; cf. Bakker & Mostert, 2024). This case study provides insights into how integrating an industry certification exam into a foundational cybersecurity course curriculum served as a resource and not an additional demand. The lessons learned guided further analysis to determine whether: (1) the course effectively integrates certification requirements into the curriculum, (2) two separate courses are necessary to fully achieve these goals, or (3) an alternative approach, such as embedding certification objectives across multiple courses, would be more effective.

III. The Case for Applied Curriculum

The University of Oklahoma created a Polytechnic Institute (OUPI) in May 2022 to address the high demand for advanced and applied technology in the northeast region of Oklahoma. Placed on the university's Tulsa campus, OUPI was designed as a polytechnic to be "a hands-on education in a digital world, fueling innovation by embracing technology, and educating and enriching students" (OUPI, 2024). To gain approval by the Oklahoma State Board of Regents, the course curriculum was drafted by the university's computer science department and followed a more traditional approach of studying which was heavy on computer theory and traditional curriculum approaches.

After OUPI hired its inaugural director in March 2023, response from industry to the announcement of the first Bachelor of Science in Cybersecurity was positive but cautioned that graduates needed to have an education geared toward the practical application of cybersecurity. Consequently, a comprehensive review of the curriculum was undertaken to better meet industry needs. Specifically, the curriculum for the introductory cybersecurity class, *Foundations of Cybersecurity*, was reviewed and intentional choices made to address not only the technical concepts of cybersecurity, but also to provide the students with opportunities to develop their employability skills, professional knowledge, and competencies.

As a result of these intentional choices, the foundations course had three main objectives: 1) providing an introduction and overview of the cybersecurity field (e.g., nomenclature, threats, vulnerabilities, cryptography, network security, and incident response); 2) offering multiple opportunities to work individually and collaboratively to draft executive summaries on cybersecurity-related media topics and make corresponding oral presentations; and 3) establishing a structured approach for the CompTIA Security+ industry certification exam.

The first cohort of students began their program in August 2024. The initial cohort of students consisted of 25 students with an average age of 26.6 and a median age of 24. The group was diverse with 24% identifying as women and 64% coming from minoritized populations. Notably, 44% of the students qualified as first-generation college students. Expectedly, the majority, 92%, claimed Oklahoma as their residency with nearly three-fourths of the students having attended Community College prior to enrollment. The combined cohort had a GPA of 3.22 upon being admitted to OUPI. Importantly, while the group received significant financial aid, 64% of students still faced unmet financial needs. In addition to the *Foundations of*

Cybersecurity, the cohort completed courses on *Hardware Security, Introduction to Linux, and Applied Statistics for Computing*. The majority of students were enrolled full-time, with many also balancing part- or full-time jobs.

IV. The Case Dynamics

The problem

The case study was created to study and review the mechanics for integrating an industry certification into a foundations of cybersecurity course. The integration was one of three course objectives with the other two being: 1) providing an overview of the cybersecurity field, and 2) developing the students' team and presentation abilities.

Regarding the integration of the industry certification, specifically the CompTIA Security+ exam, students faced two primary challenges: 1) studying additional material than might otherwise be expected in an overview or foundational course on a topic at the undergraduate level, and 2) identifying the appropriate resources for managing the course material while balancing the overall undergraduate program demands. Unsurprisingly, faculty faced the same two challenges of including more material than might otherwise be necessary as well as providing appropriate resources to the students without contributing unnecessarily to their demands (i.e., time, abilities, load).

The solution

To address the primary issue of integrating the industry certification into the course curriculum, an online textbook from zyBooks was utilized that was designed for studying for the CompTIA Security+ exam. The textbook was selected for three reasons which helped address

the concern around providing resources instead of additional demands: First, zyBooks systematically covered each of the sections identified as Security+ exam material with material presented in a concise, summary format. Second, the textbook provided extensive multiple-choice questions similar to those on the Security+ exam, providing students with valuable practice. Third, zyBooks enabled the instructor to track student engagement by measuring time spent on readings and exercises. Analysis of test results indicated a strong correlation between time spent on these activities and student performance. The time-tracking feature also provided opportunities for the instructor to identify students who might benefit from additional help (zyBooks, 2024).

Given the chosen textbook and the goal of integrating industry certification, the instructor tailored the course lectures, discussions, and learning objectives to emphasize the Security+ topics. To accommodate diverse learning preferences, videos and handouts were incorporated that provided opportunities for students to engage the course material through multiple sources. This approach proved beneficial when students selected media articles and prepared their executive summaries as they were able to utilize concepts, terminology, and ideas from both the textbook and lectures in their written and oral presentations.

To prepare for the quizzes, mid-term exam, and final exam, all of which followed the Security+ exam format, the instructor provided study guides, notes, and practice questions with detailed explanations for both correct and incorrect explanations. The value of providing these resources became apparent in the students' ability to recall information during class discussions and in their higher quiz scores when these materials were provided as compared to when such material was not provided.

While results were not yet available for students' performance on the Security+ exam, as most had not yet taken it, other indicators suggested strong potential for success. First, 92% of students earned a grade-point average of 3.0 or higher, with 54% achieving a 4.0. Second, students who completed two practice exams attained passing scores on the material covered in class. Third, students expressed their intent to take the Security+ exam and reported satisfaction in the university's course evaluations with the depth and quality of information provided in the course.

Limitations

This case study is subject to several limitations. First, since students have not yet taken the CompTIA Security+ exam, correlations between course performance and certification exam results are unavailable. While preliminary indicators are promising, final observations and recommendations cannot be made without actual exam outcomes. Second, the course was not exclusively designed to prepare students for the Security+ exam. Consequently, less time was allocated for direct exam preparation, as course lectures and discussions covered broader cybersecurity topics and goals alongside certification requirements. A more focused approach could have been implemented if the sole objective had been certification attainment. Finally, given the constraints and administrative requirements involved in establishing a new Bachelor of Science degree program, time was limited for selecting textbooks, creating syllabi, and identifying learning objectives. Additional time, along with the insights from efforts like those described in this study, would have benefited the program's development.

V. Case Study Conclusion

Lessons learned

This case study yielded three key lessons learned. First, aligning course textbooks with industry certification exams enhances the potential for student success. Ensuring synergy between textbooks and certifications serves as a valuable resource, helping to mitigate the additional demands of studying for certification exams. Second, balancing course content with additional learning objectives requires careful planning. Incorporating every textbook chapter as well as including additional outcomes such as team building or presentation skills reduced the time available for in-depth exploration of cybersecurity topics. While integrating these interpersonal and professional skills was beneficial, greater alignment or clearer expectations could have better supported learning the certification material. Third, enhancing student study habits and recall ability is essential. Identifying a theory or mechanism for improving students' study strategies and retention would have further strengthened their ability to master both course content and certification exam material.

For example, the textbook addresses incident response as the 14th of 15 chapters. In hindsight, moving this chapter to the beginning of the course or integrating its core concepts earlier in the curriculum would have provided a foundational framework – a 'trunk'- upon which the remaining topics could be structured as 'branches.' Cybersecurity as a profession exists to counter threats and adversaries that seek to compromise the confidentiality, integrity, and availability of data. Consequently, nearly every aspect of a cybersecurity professional's role involves preventing or responding to an incident. Introducing incident response earlier in the course, rather than later, offers a structured framework for learning, enhancing comprehension, recall, and a practical application of the course material.

Integrating industry certifications into a cybersecurity curriculum presents both opportunities and challenges. This case study demonstrated that aligning course content with certification objectives can enhance student outcomes but poses multiple challenges. The intentional structuring of course materials, along with the use of sufficient resources, can help mitigate additional study burdens and supported student success. While preliminary indicators suggest positive outcomes, further research is needed to assess long-term impacts, refine curriculum design, and explore alternative approaches for integrating certifications effectively across multiple courses.

Further research

Multiple opportunities exist for additional research. First, after incorporating the lessons learned, IRB approval should be obtained to conduct quantitative research on the key variables of burnout, goal theory, and study habits to assess whether students have sufficient resources to meet the demands of learning cybersecurity and certification topics in a single course. Second, when multiple sections of the course are offered, establishing a control group that uses a different textbook with a singular focus on learning cybersecurity—without the objective of passing a certification exam—could help evaluate the effectiveness of integrating industry certifications into a *Foundations of Cybersecurity* course. This approach could also determine whether students would benefit more from two separate courses. Third, research could explore whether students would benefit more from integrating certification exam preparation across multiple cybersecurity courses rather than concentrating it within a single course.

Bibliography

Al-Rawi, A., & Lansari, A. (2008, June). Integrating the Security+ exam objectives into information technology curricula. In *2008 Annual Conference & Exposition*.

Bakker, A. B., & Mostert, K. (2024). Study demands–resources theory: Understanding student well-being in higher education. *Educational Psychology Review*, *36*(3), 92. https://doi.org/10.1007/s10648-024-09940-8

Boehler, J. A., Larson, B., & Shehane, R. F. (2020). Evaluation of information systems curricula. *Journal of Information Systems Education*, *31*(3), 232-243.

Clements, A. J., & Kamau, C. (2018). Understanding students' motivation towards proactive career behaviours through goal-setting theory and the job demands–resources model. *Studies in Higher Education*, *43*(12), 2279-2293. https://doi.org/10.1080/03075079.2017.1326022

CompTIA, (2024). "CompTIA Security + ". https://www.comptia.org/certifications/security (accessed 09 December 2024).

CompTIA, (2024). "CompTIA and NICE: Setting the standard for safe cyber practices." https://www.comptia.org/content/tools/comptia-and-the-national-initiative-for-cybersecurity-education (accessed 11 December 2024).

Demerouti, E., Bakker, A. B., Nachreiner, F., & Schaufeli, W. B. (2001). The job demands-resources model of burnout. *Journal of Applied psychology*, *86*(3), 499-512.

Erickson, M., & Kim, P. (2021). Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning. *Issues in Information Systems*, *22*(4). https://doi.org/10.48009/4_iis_2021_9-21

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Hentea, M., Dhillon, H. S., & Manpreet, D. (2006). Towards changes in information security education. *International Journal of IT Education,* 5, 221-233.

ISC2. (2024). *2024 ISC2 Cybersecurity Workforce Study*. ISC2.org. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

Justice, C., & Sample, C., Loo, S. M., Ball, A., Hampton, C., (2022, March). Future needs of the cybersecurity workforce. In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 81-91).

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education*, *28*(2), 101-114.

National Initiative for Cybersecurity Careers and Studies (NICCS). (2024). "Cybersecurity Certifications." https://niccs.cisa.gov/education-training/cybersecurity-certifications (accessed 11 December 2024).

Ngo-Ye, T. L., & Choi, J. (2016). Preparing students for security certification: an exploratory experiment. *Issues in Information Systems*, *17*(3), 59-69. https://doi.org/10.48009/3_iis_2016_59-69

Nilson, L. B. (2010). *Teaching at its best: A research-based resource for college instructors* (3rd ed). John Wiley & Sons.

Ouh, E. L., & Shim, K. J. (2021, October). Integration of information technology certifications into undergraduate computing curriculum. In *2021 IEEE Frontiers in Education Conference (FIE)* (pp. 1-9). IEEE.

OUPI. (2024). The Polytechnic Difference. The University of Oklahoma. OUPI.edu. https://www.ou.edu/polytechnic (accessed 16 December 2024).

Salmela-Aro, K., & Upadyaya, K. (2014). School burnout and engagement in the context of demands–resources model. *British journal of educational psychology*, *84*(1), 137-151. https://doi.org/10.1111/bjep.12018

Sauls, J., & Gudigantala, N. (2013). Preparing information systems (IS) graduates to meet the challenges of global IT security: Some suggestions. *Journal of Information Systems Education*, *24*(1), 71-74.

Ward, P. (2021). Constructing a methodology for developing a cybersecurity program. *Proceedings of the 54th Hawaii International Conference on System Sciences* (pp. 44–53). Honolulu, HI: University of Hawaii at Manoa, Hamilton Library.

ZyBooks. (2024). Introduction to Security with CompTIA Security+ zyLabs Version. ZyBooks.com. https://www.zybooks.com/catalog/introduction-to-security-with-comptia-security-zylabs-version/ (accessed 17 December 2024).