Issues in Information Systems
Volume 26, Issue 4, pp. 78-91, 2025

DOI: https://doi.org/10.48009/4_iis_2025_108

A comprehensive case-based simulation approach to designing a graduate cybersecurity capstone project

Ping Wang, *Robert Morris University, wangp@rmu.edu*
Jing Hua, *Robert Morris University, hua@rmu.edu*
Noory Etezady, *Robert Morris University, etezady@rmu.edu*

Abstract

Increasingly sophisticated cybersecurity risks and challenges demand a well-trained and qualified cyber workforce with comprehensive knowledge, skills and abilities (KSAs) and competencies for effective and sustainable cyber defense. Graduate education in cybersecurity with quality assurance provides students with both technical and non-technical KSAs and professional competencies. A capstone project is a project-based learning activity offering an integrated learning experience to achieve outcomes and professional competencies for educational assessment and workforce development. This research proposes an enterprise case-based simulation approach to designing a portfolio-type project for the capstone course of a master's level graduate degree program in Cybersecurity in the United States. The proposed project design uses a realistic and sanitized enterprise security case for project simulation to provide students with the integrated learning experience of identifying and analyzing critical assets and security vulnerabilities as well as recommending, developing, and evaluating technical and non-technical solutions for security risk mitigation and management. The project design is expected to develop students' KSAs and competencies not only in understanding and application but also in higher levels of learning through critical analysis, evaluation, and creative development in Bloom's taxonomy. The proposed project design also includes the key components, objectives, deliverables, and a sample rubric for project assessment and contributes preliminary empirical data of implementing the capstone project design with sample graduate students in Cybersecurity.

Keywords: cybersecurity, graduate education, capstone project, project-based learning (PBL), KSAs, competencies

Introduction

Workforce demand for cybersecurity professionals continues to grow due to persistent cyber threats, attacks, and risks for public and private sectors and individual users. The market demand for information security analysts as a common cybersecurity career is projected to grow at 33% during 2023-2033, substantially higher than the 12% growth rate of all computer occupations and the 4% growth rate of all occupations (US BLS, 2025). In addition, cyber threats and attacks are increasingly sophisticated and complex and posing new challenges for cybersecurity professionals. The latest global cybersecurity workforce survey study among 15,852 cybersecurity practitioners and decision makers conducted by (ISC)2 (International Information Systems Security Consortium) has found that insufficient numbers of staff and the lack of the right range of skills among cyber professionals have placed organizations at significant

security risks ((ISC)2, 2024). Higher education degree programs remain as the major source of supply and professional development of skilled cybersecurity workers. The latest Cybersecurity Workforce Supply and Demand Report prepared by the National Center for Science and Engineering Statistics (NCSES) and published by the National Science Foundation (NSF) finds a rapid growth of the number of cybersecurity workers in the pipeline but other factors like lack of clear data on the skills, knowledge, and credentials needed in the workforce account for the gap between the demand for and the supply of skilled workers in cybersecurity (Hogan et al., 2024). Therefore, it is necessary and significant to have further research on the effectiveness and quality of curriculum design and outcomes of cybersecurity education programs for continuous improvement to meet the expectations of the cyber workforce.

A capstone project is often used as a culminating deliverable to develop and demonstrate students' KSAs and competencies as performance predictors for relevant careers. Project-based learning (PBL) can be effective in bridging the theoretical and practical gaps in education and developing both technical and non-technical skills and capabilities for students (Marta et al., 2024; Pham & Tran, 2021; Veselov et al., 2019). Cybersecurity professional competencies include industry-wide technical competencies and non-technical competencies such as academic competencies, workplace competencies, and personal effectiveness competencies at different tiers outlined in the U.S. Department of Labor Cybersecurity Industry Model (Wang et al., 2020). There has been substantial research progress on technical and computing education with a PBL approach or component but primarily for undergraduate level students (Etezady & Wang, 2025; Hooshangi et al., 2024; Malik & Zhu, 2023; Marta et al., 2024; Rahman et al., 2023; Veselov et al., 2019; Zhang & Ma, 2023). Graduate education should have more emphasis on higher levels of learning in Bloom's taxonomy for more advanced academic and professional competencies (Anderson & Krathwohl, 2021). This research will focus specifically on designing a comprehensive capstone project for master's level graduate students in the field of Cybersecurity. The purpose of this research is to contribute a case-based simulation approach to designing of a graduate level capstone project in Cybersecurity with initial empirical practice data on implementation.

The following sections of this paper will review relevant background for research, describe the proposed case-based simulation approach for project design, and present and discuss the sample design of the graduate cybersecurity capstone project. In addition, the research paper will present preliminary data of implementation using the capstone project in graduate cybersecurity education. The paper will conclude with suggestions for further studies on this topic.

Background

This section will review relevant background, including cybersecurity industry expectations, models, frameworks, and guidance to inform the discussion on cybersecurity education. The literature review will also include research on project-based learning (PBL) and competencies applicable to graduate education and this study on designing graduate level capstone project. Curriculum and course designs for cybersecurity education should be informed by the cybersecurity industry expectations for KSAs and professional competencies. The following are relevant and important models, frameworks, and guidelines that identify key KSAs and professional competencies for the cybersecurity industry and have practical implications for cybersecurity education. The Cybersecurity Industry Model published by the U.S. Department of Labor (DoL) includes five tiers of technical and non-technical competencies for the cybersecurity profession. The five tiers of competencies have no hierarchical order and are summarized as follows (US DoL, 2014; Wang et al., 2020):

1. **Tier 1** focuses on Personal Effectiveness Competencies or essential personal attributes such as interpersonal skills, ethical integrity and professionalism, and personal commitment to lifelong learning for continuous professional development.

2. **Tier 2** focuses on Academic Competencies such as well-rounded academic proficiencies and skills in communication, critical thinking, analytical thinking, as well as fundamental user skills in information technology.
3. **Tier 3** focuses on Workplace Competencies such as skills and abilities in teamwork, planning and organizing, creative thinking, problem solving and decision making, and fundamentals of business operations.
4. **Tier 4** emphasizes Industry-wide Technical Competencies such as KSAs in cybersecurity technology solutions, cyber risk management, as well as cyber incident response and remediation.
5. **Tier 5** emphasizes the Industry-sector Functional Areas such as industry specific provision systems, security operation and maintenance, threat investigation and profiling, defense and prevention strategies, data collection and analysis, and cybersecurity governance.

The DoL Cybersecurity Industry Model provides general competencies and KSAs that are still applicable to developing cyber professional qualifications and graduate education. In addition, cybersecurity leadership skills should be integrated in all tiers of the industry model as a relevant and necessary competency in the increasingly challenging cybersecurity work environment (Wang et al., 2020). The cybersecurity leadership skills also fit the general goals of graduate education in cybersecurity.

NCAE-CD Designation Requirements

In order to meet the expected qualifications for the cybersecurity workforce, it is essential to have established standards for quality assurance in cybersecurity education. The United States has led the world in establishing the National Centers of Academic Excellence in Cyber Defense (NCAE-CD) designation program as part of the overall NCAE-C (Cybersecurity) currently sponsored by the Department of Defense (DoD), National Security Agency (NSA), CISA (Cybersecurity and Infrastructure Security Agency), and FBI (Federal Bureau of Investigation). The NCAE-CD designation requires rigorous reviews and documentation for validation of the cybersecurity program of studies (PoS) and approval of the Cyber Defense (CD) designation. The NCAE-CD designation has been the most comprehensive and reputable national standard for certifying and maintaining the quality of cybersecurity education with specific metrics for program evaluation and assessment of cybersecurity knowledge units (Wang et al., 2018; Wang & Kohun, 2019). The NCAE-CD designation requires curriculum mapping to specific knowledge units (KUs) for cybersecurity PoS validation. The current KU requirements and codes are as follows (DoD Cyber Exchange Public, 2024; NCYTE, 2025):

- Three Foundational KUs for all degree programs (Associate's, Bachelor's, Master's, Doctoral)
    - Cybersecurity Foundations (CSF)
    - Cybersecurity Principles (CSP)
    - IT Systems Components (ISC)
- Five Technical Core KUs for all degree programs
    - Basic Cryptography (BCY)
    - Basic Networking (BNW)
    - Basic Scripting and Programming (BSP)
    - Network Defense (NDF)
    - Operating Systems Concepts (OSC)
- Five Non-Technical Core KUs for all degree programs
    - Cyber Threats (CTH)
    - Cybersecurity Planning and Management (CPM)
    - Policy, Legal, Ethics, and Compliance (PLE)
    - Security Program Management (SPM)
    - Security Risk Analysis (SRA)

- An additional number of Optional KUs selected from dozens of KUs on specialized topics. The required number varies with the degree program, such as 14 for Bachelor's degree programs but 7 plus Thesis/Capstone or equivalent for Master's degree programs.

More detailed descriptions and learning outcomes are provided for each of the KUs that are also regularly reviewed and updated by the NCAE-CD community (NCYTE, 2025). The KUs are closely aligned to professional qualifications for the cybersecurity industry. They are also mapped to the cybersecurity job categories, work roles, tasks, and specific knowledge, skills and abilities (KSAs) that are defined in the NCWF (NICE Cybersecurity Workforce Framework) published and updated by the U.S. NIST/NICE (National Initiative for Cybersecurity Education) (NICCS, 2024; NICE, 2020). In addition, the NCAE-CD program guidance provides more detailed options for Master's degree programs to fulfil the Optional KU requirement. Master's programs may include a traditional Master Thesis or Equivalency plus additional 7 Optional KUs. The main guidelines for the Master Thesis/equivalency are:

- Include one or more dedicated term-long course(s) indicated as "Thesis", "Project", "Capstone", "Experiential Learning", or "Practicum" preferably towards the end of the student's PoS.
- The project or equivalent should be supervised by a qualified faculty member.
- The student (or small group of up to two students) develops a final project/capstone and/or experiential learning as a paper and/or applied project that integrates best practices in the context of cybersecurity.
- The project or equivalent should have clear and specified concepts, standards, focused problem, measurable goals, and strategies for project implementation. (DoD Cyber Exchange Public, 2024).

DoD Cyber Framework

The U.S. Department of Defense (DoD) is among the largest employers in the world and the current lead sponsor of the NCAE-CD designation program. The DoD Cyber Workforce Framework (DCWF) published by the DoD Office of Chief Information Officer (CIO) describes the work expectations for a wide and full range of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages and incorporates the original NICE Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (US DoD CIO, 2025). The main contributions of the DCWF include the following (DoD Cyber Exchange Public, 2024):

- Established and defined 7 cyber workforce elements or categories: IT (Cyberspace), Cybersecurity, Cyberspace Effects, Intelligence (Cyberspace), Cyberspace Enablers, Software Engineering, and Data/AI.
- The cyber workforce elements are mapped to 33 specialty areas and 54 work roles.
- Each work role has a clear definition with a list of representative tasks, knowledge, skills and abilities (KSAs) needed to perform key functions.
- A defined proficiency level (Basic, Intermediate, Advanced) is applied to each coded work role.

In addition, the Workforce Identification and Coding Guide as a supplement to the DCWF provides a standardized approach to identifying, selecting, describing, and coding cyber work roles and corresponding proficiency levels for military, civilian, and contractor personnel. The guide serves as a workforce management methodology for cyber talent recruiting, development, and retention (US DoD Deputy CIO, 2024). The resources in the DCWF and the supplemental guide should be valuable resources for designing curriculum and project activities in cyber education and training. Project-based learning (PBL) is a student-centered active learning approach that involves students directly in dealing with realistic and complex problems in an interdisciplinary way, emphasizing the development of student skills in critical thinking, collaboration, and problem-solving (Piccolo et al., 2023). There has been extensive research on the PBL approach in education, which may help inform the design of a graduate cybersecurity capstone project.

Table 1 below highlights and summarizes relevant and significant research and findings on the use of PBL approach in education in the past five years.

Table 1. Summary of Research on Project-based learning (PBL)

Year	Authors	Methodology	Key Concepts, Findings, Contributions, Limitations
2025	DeLisi et al.	Case study with surveys, interviews, focus groups	• PBL helps to create personalized, engaging, and relevant experiences for STEM career pathways. • Alignment to industry expectations is important for PBL. • Study and data are limited to general STEM career pathways for an urban high school.
202	Ma & Wu	Case study	• PBL model integrates objectives, process, resources, and formative and summative assessment. • Integrated PBL effectively enhances core competencies, motivation, problem solving, innovation, and collaboration. • Study is limited to interior design for third-grade students.
2024	Marta et al.	Classroom Action Research (CAR)	• PBL approach improves cognitive growth, affective development, psychomotor skills, and interest and motivation in learning. • PBL model involves the steps of planning, implementation, observation, and reflection. • Study and data are limited to 30 likely undergraduate students in visual programming.
2024	Menezes et al.	Empirical study with AI intervention	• LLM-based AI-grading improves efficiency and effectiveness of PBL in software development projects. • AI-scoring improves student participation, contribution, and group collaboration in project development. • Study and data are focused on the role of AI and limited to software development students in computer science program.
2024	Redd et al.	Case design and quasi experimental study	• PBL case modules achieves significant increase in student knowledge of security and privacy concepts. • PBL case design should include student reflections and assessment of learning. • PBL in cybersecurity for capstone experiences helps create workforce with better sociotechnical cybersecurity principles. • Study is limited to undergraduate software development students.
2023	Piccolo et al.	Case study with case project designs	• PBL develops skills, problem solving, critical thinking, creativity, self-reflections, and collaboration. • Study and findings are limited to empirical experiences. • Best practices for PBL instructional design are still lacking.

Year	Authors	Methodology	Key Concepts, Findings, Contributions, Limitations
2023	Malik & Zhu	Educational design-based research (DBR)	• PBL with hands-on activities and flipped teaching enhance students' learning motivation and perceptions of learning. • Further research is needed on the impact of individual intervention on learning motivation and outcomes. • Study is limited to introductory undergraduate computer networks course for computer science and IT majors.
2022	Markula & Aksela	Multiple-case study	• PBL may promote skills with technical tools, artefact creation, collaboration, scientific research, presentation, and reflection. • Key characteristics of PBL should include a problem-centered driving question, learning goals, scientific methods, collaboration, using technological tools, and artefact creation. • Study is limited to K-12 science education.
2021	Netinant et al.	Case design and case study	• PBL approach to course design and planning improves success ratio of master's students. • Study and data are limited to an IoT course for a graduate master's degree in IT with minimal coverage on security content.
2021	Pham & Tran	Surveys, interviews, focus groups	• Results show majority student positive perceptions of PBL: More confidence and enhanced critical thinking, problem-solving, communication, collaboration, and overall quality of education. • Study and data are limited to undergraduate IT courses. • Study is focused on and limited to student perceptions of PBL.

The background review above shows the general consensus on the significance and benefits of using the project-based learning (PBL) approach in education, especially in science and technology education. These benefits include improvements and enhanced effects in students' interest and motivation in learning, subject matter knowledge, hands-on technical skills, creative and innovative work, as well as in critical thinking, problem solving, communication, collaboration, and personal reflections.

However, there is still a lack of best practices in project design cases in PBL research for education (Piccolo et al., 2023). In addition, the literature review indicates that the overwhelming majority of existing research on PBL is limited to undergraduate or lower levels of technical education and with minimal focus on graduate level cybersecurity and capstone projects. Therefore, this study will address the limitation and will focus on designing a graduate master's level cybersecurity capstone project using the PBL approach.

Methodology

This study uses a PBL case design methodology with simulation and empirical observation to present the design and initial implementation of a graduate cybersecurity capstone project. Case design is a form of

case study methodology that has been tested in prior PBL research in education (Ma & Wu, 2025; Malik & Zhu, 2023; Markula & Aksela, 2022; Piccolo et al., 2023; Redd et al., 2024). The case design approach to PBL also embraces Classroom Action Research (Marta et al., 2024). The PBL case design approach of this study will emphasize testing, identification, analysis, and mitigation of enterprise level cybersecurity vulnerabilities and risks. The cybersecurity issues for the graduate capstone project are realistic and complex for problem solving for specific industries but without identifying any specific organization due to potential risks and liabilities for disclosures of organizational security profile and data. Therefore, simulation is incorporated as part of the case design for project implementation. The case design methodology for this study will include the following additional characteristics:

Industry Specific: The cybersecurity case problem for each capstone project should be specific to a certain industry even though the identity of the organization is not disclosed. This feature will help identify the realistic cybersecurity vulnerabilities and risks for testing, analysis and mitigation in alignment with the industry expectations. This alignment is essential to designing, implementing, and assessing learning activities to meet the industry expectations for tasks, KSAs, and competencies (DeLisi et al., 2025).

Comprehensive Activities: The graduate capstone project should have various learning activities such as readings, discussions, hands-on work, research, presentations, and project reports to develop students' technical KSAs and competencies as well as non-technical skills including problem solving, critical thinking, communication, teamwork and leadership skills as expected in the US DoL Cybersecurity Industry Model, the NCAE-CD designation requirements, and DoD Cyber Framework (DCWF).

Research and Reflections: In addition to understanding and application, a graduate level capstone project should emphasize higher levels of learning through analysis, evaluation, and creativity in the updated Bloom's taxonomy (Anderson & Krathwohl, 2001). Student research and reflections will promote higher levels of learning. Student research and reflections are also appropriate for and enhanced by PBL projects (Markula & Aksela, 2022; Marta et al., 2024; Piccolo et al., 2023; Redd et al., 2024).

Assessment of Learning: Assessment of the project learning activities is essential for quality assurance and continuous improvement of cybersecurity education. A clear grading rubric for the capstone project is a useful tool for assessing student performance and competencies. The PBL approach would be more effective with assessment of student learning in the project design (Ma & Wu, 2025; Redd et al., 2024).

Project Design and Implementation

The integrated capstone project in this study is the core of the 3-credit graduate cybersecurity capstone course required for a master's degree program to emphasize project-based learning (PBL) as stated in the course syllabus and description. The capstone project design is based on individual case scenarios selected by students to test, detect, and assess security vulnerabilities and threats and develop and evaluate solutions to address the security risks for the organization in the individual cases. The case scenarios for the capstone project represent realistic industry organizations with security challenges and risks that need to be studied and addressed. The case scenario options represent a wide range of industries including banking, energy, healthcare, IT, manufacturing, professional services, public services, retail, travel and hospitality. The case organizations for security testing provided by SceniceSoft are some examples of the case scenarios for student selection for the capstone project (ScienceSoft, 2025). The case-based project approach reflects the project-based learning (PBL) emphasis of the course work to focus on realistic problem solving and to develop KSAs and competencies for cybersecurity professionals.

The design of the capstone project also reflects the simulation approach throughout the project work. For prevention of sensitive data disclosure and liabilities, each project case scenario has the actual organization name and identity redacted and provides limited and general cybersecurity challenges and needs facing the organization's business, services, and clients. Students are expected to conduct research into the industry area for the case to simulate the specific cybersecurity vulnerabilities and risks, conduct simulated security tests and assessment, and develop comprehensive solutions and recommendations. Individual students are encouraged to select different industry areas so as to maximize the coverage of industry topics and share the knowledge and findings with others in class. The capstone project design includes the following progressive deliverables for students to complete:

1. Project Plan
2. Progress Report
3. Project Presentation
4. Final Report

Each deliverable will have detailed directions and guidance for implementation and learning activities from the instructor. In addition, relevant readings, video presentations, tutorials and demos, and other study materials can be posted on a learning management system (LMS) for student review. This design reflects the flipped learning approach incorporated in PBL to enhance class efficiency and student motivation and perception of learning (Malik & Zhu, 2023). Flipped learning approach will also create more time for students to conduct in-depth research and preparation for better participation in class discussions, hands-on work, and better quality of the project deliverables.

Project Plan

The project plan is a brief 1-2 page document to summarize the initial planning for the capstone project. The expected content includes the specific industry case scenario selected for the project, its business services and clientele, critical assets, cybersecurity challenges (vulnerabilities, threats, risks), security testing and other tasks, technology solutions and tools needed, anticipated results, initial thoughts on solutions. Students are expected to conduct some initial research on the common security profile, challenges, and compliance regulations for the selected industry area to help with the completion of this deliverable. The instructor will review the project plans submitted and provide feedback on each individual plan and the selection of the project case to help the student to progress with the project.

The progress report is usually due by the mid-term of the course. Based on the initial project plan and instructor feedback, the progress report should provide updates with more details and documentation on the following aspects of the project:

- Identify and describe specific critical assets relevant to cybersecurity based on the selected case scenario and industry, including hardware, software, network services, data, and other assets.
- Identify, describe, and evaluate/prioritize the potential security threats, vulnerabilities, and risks related to the identified critical assets following a recognized security risk evaluation method.
- Provide more detailed descriptions of the features and limitations of the technologies and tools for the selected case study based on research and hands-on testing.
- Provide any initial results and challenges for any hands-on testing conducted so far.
- Include an initial Reference List at the end with at least 5 reputable sources to document the sources of important items in the progress report.

Project Presentation

The students are expected to present each project in class near the end of the semester when they are about to complete the project. This is a good opportunity to share the individual project work and findings with

the class for knowledge sharing and to hear questions and suggestions from fellow students and the instructor to improve the work for the final report. This is also a learning opportunity to practice students' communication skills in a cybersecurity subject context. Students should learn the different styles of communication between a presentation to an audience and a written report for close reading and review. The final report should be due by the end of the semester and include the following expectations:

- Detailed description of the simulation methodology including security technologies, tools, and techniques used.
- Detailed description of research, findings, and results on the security vulnerabilities and risks including screen captures of key lab results.
- Complete analysis and assessment of the security vulnerabilities, threats, and risks relevant to the selected case industry and organization and its critical assets.
- Proposed security solutions and recommendations to address the security risks associated with the selected case industry and scenario with support of research documentation.
- Include the final Reference List at the end with at least 10 reputable sources in APA or IEEE format.
- The final report should reflect clear and accurate academic writing to avoid confusion in communication. The suggested length of the final report is about 10 or more pages but is up to the individual instructor.
- Students also share their reflections on the project experience and its professional value

The final report should have the lion's share of the course grade. Therefore, a clear grading rubric is essential to guiding student work and for assessment and continuous improvement of the course design. Table 2 below provides a suggested grading rubric to grade and evaluate student work for the final project report. The performance indicators in the rubric represent expectations for competencies and KSAs related to the project and for the cybersecurity professionals. The KSAs include both technical and non-technical areas of performance, research skills, and communication skills. .

Table 2. Grading Rubric for Final Project Report

	Excellent	Good	Satisfactory	Below Expectations
Assets, Threats, Vulnerabilities, Risks (Weight: 40%)	**36-40 Points** Excellent identification, description, and assessment of critical assets, threats, vulnerabilities, and risks supported by research and data	**32-35 Points** Good identification, description, and assessment of critical assets, threats, vulnerabilities, and risks supported by research and data	**28-31 Points** Adequate identification, description, and assessment of critical assets, threats, vulnerabilities, and risks supported by research and data	**Below 28 Points** Inadequate identification, description, assessment, or research documentation of critical assets, threats, vulnerabilities, and risks
Security Solutions and Recommendations (Weight: 40%)	**36-40 Points** Excellent description, evaluation, and discussion of the security solutions and recommendations with strong research and data	**32-35 Points** Good description, evaluation, and discussion of the security solutions and recommendations with good research and data	**28-31 Points** Adequate description, evaluation, and discussion of the security solutions and recommendations with adequate research and data	**Below 28 Points** Inadequate description, evaluation, discussion, or research or data support of the security solutions and recommendations

	Excellent	Good	Satisfactory	Below Expectations
Writing & Formatting (Weight: 20%)	**18-20 Points** Excellent writing with very few or no errors in grammar, spelling, or formatting	**16-17 Points** Good writing with a few errors in grammar, spelling, or formatting	**14-15 Points** Acceptable writing with occasional errors in grammar, spelling , or formatting	**Below 14 Points** Poor writing or with frequent errors in grammar, spelling, or formatting

Preliminary Implementation and Findings

The case-based capstone project and expected deliverables have been used as the core assignments in the capstone course for a master's degree program in Cybersecurity at a U.S. university as preliminary implementation since fall 2023. The implementation of the capstone project has been supported by other teaching and learning activities and resources, including online readings, presentations, hands-on work, video demos, discussions, and individual consultations with the instructor. During the project implementation, the instructor provided special guidance and resources to facilitate technical and non-technical work for the project. The key guidance and resources provided on non-technical security risk assessment and management include the NIST Risk Management Framework (RMF) and the OCATVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Method Implementation Guide published by Carnegie Mellon University Software Engineering Institute (Alberts & Dorofee, 2001; NIST Computer Security Resource Center, 2025). The pre-built virtual machines of cybersecurity labs in various categories of more advanced levels from the NSF-funded SEED Labs are good examples of lab resources for simulated hands-on security testing for the capstone project (SEED Labs, 2025).

The findings form preliminary implementation of the capstone project indicate fairly consistent performance and success rates in the specific deliverables of the project among student participants. The total number of the student participants for the 3 semesters listed is 32 and fairly limited. Table 3 below displays the specific number of student participants and the aggregate performance and success rates in the four deliverables for the project from fall 2023 through spring 2025. The student success rate is defined as receiving a B (or 80%) or better grade for each deliverable including the final report.

Table 3: Preliminary Project Performance and Success Rates

	Participants (N)	Project Plan	Progress Report	Project Presentation	Final Report
Fall 2023	10	100%	100%	100%	100%
Spring 2024	10	100%	100%	100%	100%
Spring 2025	12	91.67%	100%	100%	100%

During the preliminary implementation, student participants also included their reflections and comments on the project experience and its professional value in the final project report and class discussions. The majority of the comments indicate students' in-depth and thoughtful reflections on the capstone project experience including both technical and non-technical components of the project. The reflections and comments indicate overall positive view of the value of the project work and experience to their current and future work related to cybersecurity. A few students also expressed their creative interest in selecting

their own actual employer organization for the case-based project but experienced the common difficulty of not being able to obtain their organizational approval for using any company-related data for the project.

Conclusion

Continuous improvement with best practices in cybersecurity education is necessary to address the shortage and skills gap of cybersecurity workers in meeting the professional expectations of the cybersecurity industry. Prior research on the project-based learning (PBL) approach to education in different fields shows effectiveness in improving students' knowledge and skills of the subject area and enhancing student motivation for learning as well as skills in problem solving, critical thinking, communication, research, and reflections. This study focuses on the PBL approach to designing a graduate level cybersecurity capstone project for a master's degree program using specific industry cases and simulations for security testing and risk identification, assessment, and mitigation.

The case-based capstone project design is comprehensive and simulates the technical, non-technical, and professional KSAs and competencies expected by the cybersecurity industry. The project has been implemented in three graduate classes. The performance data from the three classes in the three recent semesters indicate overwhelming and consistent student success rates in all four deliverables of the capstone project, including the final report with a detailed grading rubric for assessment. However, the preliminary implementation and observations have been limited to a fairly small number of student participants (32). Future studies will attempt to collect data from more student participants for more extensive quantitative and qualitative data for more in-depth analysis of student learning outcomes and experience. In addition, artificial intelligence (AI) has been increasingly used in education and presents new opportunities and challenges for PBL research as well (Zheng et al., 2024). Further research on the PBL approach to cybersecurity project design may include case designs, best practices, and empirical data on the effectiveness of using AI in enhancing learning outcomes in cybersecurity programs.

Acknowledgement

This research is supported by a grant award from the United States National Science Foundation (NSF) – NSF Grant ID 2234554.

References

Alberts, C., & Dorofee, A. J. (2001). *OCATVE method implementation guide (version 2.0)*. Retrieved on 5/3/2025 from https://www.sei.cmu.edu/library/octave-method-implementation-guide-version-20-volume-1-introduction/

Anderson, L.W., & Krathwohl, D.R. (2001). *A taxonomy for learning, teaching, and assessing, Abridged Edition.* Boston: MA: Allyn and Bacon.

DeLisi, J., Liu, Edward, & Fields, E. (2025). Implementing project-based learning in urban high school STEM career pathways. *Urban Education, 60*(5), 1361-1384.

DoD Cyber Exchange Public. (2024). *July 2024 NCAE-CD program guide*. Retrieved on 5/3/2025 from https://public.cyber.mil/ncae-c/documents-library/

Etezady, N., & Wang, P. (2025). Capstone project design for an undergraduate cybersecurity program. *2nd International Conference on Information Technology: New Generations (ITNG 2025), April 28-29, Las Vegas, USA. 1-6.*

Hogan, M., Lilienthal, K., Bean de Hernandez, A., McHugh, P., Arbeit C.A., & Sullivan, P. (2024). National Center for Science and Engineering Statistics (NCSES). 2024. *Cybersecurity workforce data initiative: Cybersecurity workforce supply and demand report*. National Science Foundation. Retrieved on 5/3/2025 from https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative

Ma, X., & Wu, X. (2025). Establishing a seamless integrated project-based learning framework mediated by an evidence-based project-based learning system. Sustainability 2025, 17, 2325. Retrieved on 5/3/2025 from https://doi.org/10.3390/su17052325

Malik, K. M., & Zhu, M. (2023). Do project-based learning, hands-on activities, and flipped teaching enhance student's learning of introductory theoretical computing classes? Education and Information Technologies (202328. 3581–3604

Markula, A., & Aksela, M. (2022). The key characteristics of project-based learning: How teachers implement projects in K-12 science education. *Disciplinary and Interdisciplinary Science ducation Research,(2022)* 4:2. https://doi.org/10.1186/s43031-021-00042-x

Marta, R., Riyanda, A. R., Samala, A. D., Dewi, I. P., & Adi, N. H. (2024). Innovative learning strategies: Project-based learning model for excelling in visual programming. *TEM Journal. 13*(1), 581-589. https://www.temjournal.com/content/131/TEMJournalFebruary2024_581_589.html

Menezes, T., Egherman, L., & Garg, N. (2024). AI-grading standup updates tomprove project-based learning outcomes. *ITiCSE 2024, July 8–10, 2024, Milan, Italy*, 17-23. https://doi.org/10.1145/3649217.3653541

Netinant, P., Narad, P., & Rukhiran, M. (2021). A case study of project-based learning on Internet of Things course. ICFET 2021, June 04–07, 2021, Bangkok, Thailand. 126-131. https://dl.acm.org/doi/10.1145/3473141.3473237

NCYTE (National Cybersecurity Training & Education Center). (2025). CAE-CD Resources. Retrieved on 5/3/2025 from https://www.ncyte.net/academia/institutions/centers-of-academic-excellence/cae-cd-resources

NICCS (National Initiative for Cybersecurity Careers and Studies). (2024, March). *NICE workforce framework for cybersecurity (NICE Framework).* Retrieved on 5/3/2025 from https://niccs.cisa.gov/workforce-development/nice-framework

NICE (National Initiative for Cybersecurity Education), NIST (National Institute of Standards and Technology. (2020, November). *NICE cybersecurity workforce framework (SP800-181r1)*. Retrieved on 5/3/2025 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800181r1.pdf

NIST Computer Security Resource Center. (2025). *NIST risk management framework (RMF).* Retrieved on 5/3/2025 from https://csrc.nist.gov/projects/risk-management/about-rmf

Pham, A. T. V., & Tran, T. H. (2021). The implementation of project-based learning approach in technical courses: An investigation into students' perceptions. *ICAAI 2021, November 20–22, 2021, Virtual Event, United Kingdom.* 124-129. https://dl.acm.org/doi/10.1145/3505711.3505728

Piccolo, L., Buzzo, D., Knobel, M., Gunasekera, P., & Papathoma, T. (2023). Interaction design as project-based learning: Perspectives for unsolved challenges. *EduCHI '23, April 28, 2023, Hamburg, Germany.* 59-67. https://doi.org/10.1145/3587399.3587462

Rahman, T., Nwokeji, J., Matovu, R., & Frezza, S. (2023). Project based learning: A study on the impact of IST&P on the computer science students learning and engagement. *SIGCSE 2023, March 15–18, 2023, Toronto, ON, Canada.* 1386. https://dl.acm.org/doi/10.1145/3545947.3576331

Redd, B., Tang, Y., Ziv, H., & Patil, S. (2024). Layering sociotechnical cybersecurity concepts within project-based learning. *ICER '24 Vol. 1, August 13–15, 2024, Melbourne, VIC, Australia*. 406-418. https://dl.acm.org/doi/10.1145/3632620.3671093

ScienceSoft. (2025). Selected success stories from our 4,000-project portfolio. Retrieved on 5/3/2025 from https://www.scnsoft.com/case-studies/security-testing

SEED Labs. (2025). Hands-on labs for security education. Retrieved on 5/3/2025 from https://seedsecuritylabs.org/

US BLS (Bureau of Labor Statistics). (2025). *Occupational outlook handbook: Information security analysts*. Retrieved on 5/3/2025 from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

US DoD CIO (Department of Defense Chief Information Officer). (2025). *The DoD cyber workforce framework (DCWF)*. Retrieved on 5/3/2025 from https://dodcio.defense.gov/Cyber-Workforce/

US DoD Deputy CIO. (2024, September 11). *DCWF workforce identification and coding guide, version 1.4.* Retrieved on 5/3/2025 https://public.cyber.mil/wid/dcwf/

US DoL (Department of Labor). (2014). Cybersecurity Industry Model. https://www.dol.gov/agencies/eta

Veselov, G. E., Pljonkin, A. P., & Fedotova, A. Y. (2019). Project-based learning as an effective method in education. *ICMET 2019, June 28–30, 2019, Nanjing, China.* 54-57. https://doi.org/10.1145/3341042.3341046

Wang, P., Dawson, M., & Williams, K.L. (2018). Improving cyber defense education through national standard alignment: Case studies. *International Journal of Hyperconnectivity and Internet of Things. 2*(1), 12-28.

Wang, P., Hayes, N., Bertocci, M., Williams, K., & Sbeit, R. (2020). The role of industry partnerships and collaborations in information technology education. *Advances in Intelligent Systems and Computing, 1134* (Chapter 2). Springer Nature Switzerland AG.

Wang, P., & Kohun, F. (2019). Designing a doctoral program in cybersecurity for working professionals. *Issues in Information Systems, 20*(1), 88-99.

Zhang, L., & Ma, Y. (2023). A study of the impact of project-based learning on student learning effects: A meta-analysis study. *Frontiers in Psychology, 14*(2023). https://doi.org/10.3389/fpsyg.2023.1202728

Zheng, C., Yuan, K., Guo, B., Mogavi, R. H., Peng, Z., Ma, S., & Ma, X. (2024). Charting the future of AI in project-based learning: A co-design exploration with students. *CHI '24, May 11–16, 2024, Honolulu, HI, USA*. 1-19. https://dl.acm.org/doi/10.1145/3613904.3642807