Journal of Information Systems Education

Volume 34
Issue 1
Winter 2023

Aligning Cybersecurity in Higher Education with Industry Needs

Gelareh Towhidi and Jeannie Pridmore

Recommended Citation: Towhidi, G., & Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs. *Journal of Information Systems Education*, 34(1), 70-83.

Article Link: https://jise.org/Volume34/n1/JISE2023v34n1pp70-83.html

Received: January 9, 2022
Revised: March 9, 2022
Accepted: June 5, 2022
Published: March 15, 2023

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 34(1), 70-83, Winter 2023

Aligning Cybersecurity in Higher Education with Industry Needs

Gelareh Towhidi
Jeannie Pridmore
Department of Management and Management Information Systems
University of West Georgia
Carrollton, GA 30118, USA
gtowhidi@westga.edu, jpridmor@westga.edu

ABSTRACT

Cybersecurity is among the highest in-demand skills for Information Systems graduates and therefore is critical for the Information Systems curriculum. There is a substantial lack of skilled cybersecurity graduates. It is estimated that there is a global shortage of almost three and a half million cybersecurity professionals in 2022. Organizations are facing difficulties filling security positions. Thus, the Information Systems curriculum must be redesigned to meet business and industry needs and better prepare Information Systems graduates for cybersecurity careers. This study provides a model for designing a cybersecurity course that will align with industry needs to respond to the shortage of cybersecurity professionals. The proposed model is based on backward course design, aligned with the guidelines from the National Institute of Standards and Technology Cybersecurity Framework and The National Initiative for Cybersecurity Education Strategic Plan, and insights from interviews with industry professionals. We applied the model at a higher education institute in the USA, as higher education graduates fill most cybersecurity positions. The designed course was met with high levels of student satisfaction, positive industry feedback, and high levels of student success. Our proposed model can be applied to any educational institute and customized to desired needs of the institute, students, and the industry with minimal cost and time consideration.

Keywords: Cybersecurity, Backward design, CIS curriculum, Computing education

1. INTRODUCTION

Organizations encounter a great deal of difficulty finding skilled employees for cybersecurity positions. The number of unfilled cybersecurity jobs has increased by more than 50 percent between the years 2015 to 2021, and 62% of companies have reported that they are facing a lack of cybersecurity talent (ISACA, 2020). According to CyberSeek, a program funded by The National Initiative for Cybersecurity Education (NICE, 2019), there is a considerable cybersecurity talent gap for jobs in the United States. The shortage is estimated to be around 465,000 unfilled cybersecurity jobs in the United States (CyberSeek, 2021).

According to Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the shortage of cybersecurity professionals is a national security risk, and training for new cybersecurity professionals must be a priority (Shieber, 2019). The US government has responded to this challenge by forming several national initiatives that provide a reference for organizations and educators, such as The National Institute of Standards and Technology (NIST) Cybersecurity Framework, The Role-Based Cybersecurity Training Framework, and The National Initiative for Cybersecurity Education (NICE) Strategic Plan (NICE, 2019). Despite these endeavors, a need still exists for a practical approach based on founded learning theories that consider developing conceptual and practical skills in cybersecurity graduates to meet industry needs.

Designing educational courses based on successful theoretical learning models aligned with industry needs is complex. Past research has considered outcome-based educational systems a successful teaching and learning paradigm (Tan et al., 2018). The emphasis is on the outcomes or goals students should achieve by the end of the course. These educational outcomes determine the course content, teaching methods, and assessment process. Among the outcome-based educational design methods, backward course design is a deliberate and focused instructional course design method requiring an essential shift in education. This transformation involves thinking first about the learning objectives and then the teaching and learning activities (Wiggins & McTighe, 2005).

This research aimed to explore how to design a cybersecurity course that balances the technical, professional, and theoretical content to meet the industry needs and create excitement and interest for students to pursue a cybersecurity career. The goals are as follows:

- Design a cybersecurity course using the backward course design
- Align the course with industry cybersecurity needs to address the shortage of cybersecurity professionals
- Create excitement for pursuing a career in cybersecurity

This study develops an educational framework for the proposed cybersecurity course based on backward course design, aligned with the NIST Cybersecurity Framework, the NICE Strategic Plan guidelines, and insights from the interviews with industry professionals. The proposed cybersecurity course is a part of the "Networking and Cyber Security" concentration in the Bachelor of Business Administration (BBA) in Management Information Systems (MIS) at a medium-sized business school in the United States. This cybersecurity course (along with other courses in the concentration) aims to prepare graduates to fill the current gap in the cybersecurity market.

2. LITERATURE REVIEW

According to the ISACA professional association's state of cybersecurity 2020 report, the cybersecurity skills gap continues to be a real struggle for industry, and little progress is being made (ISACA, 2020). Previous studies have stated a continuous shortage of security professionals in government and industry (Burrell, 2020; Crumpler & Lewis, 2019). ISACA's Global State of Cybersecurity Survey—a survey of more than 2,000 cybersecurity professionals from more than 17 industries—reported the following.

- 62 percent reported that their cybersecurity team is understaffed
- 57 percent report having unfilled cybersecurity positions
- 70 percent say that fewer than half of their cybersecurity applicants are well qualified
- 73 percent reported that recent university graduates in cybersecurity lack practical experience and fundamental cybersecurity knowledge.

Information Systems (IS) education research stresses that IS curriculum should be designed to meet business and industry needs to prepare IS graduates for future careers (Tan et al., 2018). Any successful cybersecurity program must look to industry and consider the needs of the workforce to design and maintain its curriculum. Past literature in cybersecurity education has focused on two specific areas: the use of specific labs, platforms, and technology used in cybersecurity courses or provided examples of cybersecurity educational programs and curricula. Only a few studies have focused on pedagogical models or approaches for developing a cybersecurity course (Abraham & Shih, 2015; Hentea et al., 2006; Yuan et al., 2017). For example, the Process Oriented Guided Inquiry Learning (POGIL) model was proposed by Yuan et al. (2017) to enhance student technical skills and improve students' soft skills such as attitudes, motivation, and enjoyment of learning. The Holistic cybersecurity educational model was proposed based on integrative learning theory (Abraham & Shih, 2015).

Cybersecurity includes a wide possibility of topics, and deciding which cybersecurity topics to teach can quickly become overwhelming. Each program/instructor must decide and design what topics to cover and how best to cover those topics, given the time limitations of each semester. Over the last couple of decades, the United States Federal Government has established several programs explicitly focused on developing IS security policies, standards, and education guidelines, such as the National Security Telecommunications and Information Systems Security Policy. This work includes The National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2021), The Role-Based Cybersecurity Training Framework, The National Initiative for Cybersecurity Education (NICE) Strategic Plan (NICE, 2019), the National INFOSEC Education and Training Program, and the National Colloquium for Information Systems Security Education. These efforts have focused on involving colleges and universities in preparing individuals for IS security positions. However, no preceding research focuses on the theoretical foundations for developing a cybersecurity course based on industry needs. This paper aims to fill that gap.

3. INDUSTRY FRAMEWORKS

The National Institute of Standards and Technology (NIST) created a cybersecurity framework to enable all organizations to address and manage their cybersecurity needs (NIST, 2021). The NIST cybersecurity framework offers a comprehensive set of activities to be incorporated into a cybersecurity course, which can be customized to any organization's needs. Educational institutes can use the NIST Framework to design cybersecurity courses that address industry cybersecurity needs.

The core of the NIST cybersecurity framework consists of three parts: functions, categories, and subcategories. The core involves the five main functions representing the five primary pillars for a successful and holistic cybersecurity course: identify, protect, detect, respond, and recover. The categories are subdivisions of a function in groups of cybersecurity outcomes closely tied to programmatic needs and particular activities (Table 1). The identify function includes appropriate activities to understand organization cybersecurity risks. The protect function outlines appropriate safeguards to ensure the delivery of critical services. The detect function defines the appropriate activities to identify cybersecurity events. The respond function includes appropriate activities to act on a detected cybersecurity incident. The recover function identifies appropriate activities to maintain plans to restore services to normal operations.

3.1 National Initiative for Cybersecurity Education (NICE) Strategic Plan

Along with the Cybersecurity Framework, the National Institute of Standards and Technology (NIST) initiated the NICE project to respond to the growing demand for cybersecurity professionals. NICE Framework provides a framework and recommendations for educators to develop cybersecurity courses that enables training graduates with the necessary skills to meet industry cybersecurity needs. The NICE framework allows educators to develop a rigorous cybersecurity course that connects with industry needs (NICE Academic Spotlight, 2018). NICE has been used in recent pedagogical research to identify these needs. For example, recent research identified which knowledge, skills, and abilities fulfill the industry needs in the cyber defense area by using the NICE framework (Armstrong et al., 2020). As a central reference, NICE Framework plays a critical role in connecting cybersecurity education to industry needs in multiple ways. First, communication between cybersecurity educators, trainers/certifiers, employers, and employees is clarified using the NICE Framework's common lexicon. Second, the crucial analysis step identifies tasks critical for successful performance

with a given work role. Third, a proficiency analysis identifies the position's work roles and relevant tasks.

The NICE Framework includes categories, specialty areas, and work roles (Table 2). Categories provide the overarching organizational make-up of the NICE Framework. The National Institute of Standards and Technology (NIST) recommends that educational institutes map their courses to the NICE Framework to cover the industry gaps.

3.2 Industry Certificates

The importance of including industry certificates in cybersecurity education has been recently recognized (Ward, 2021). Mastering cybersecurity requires both knowledge and experience. While cybersecurity knowledge can be gained through education that provides the foundation for security concepts and tools, cybersecurity training such as industry certificates develops the necessary cybersecurity experience that delivers explicit skills (Bicak et al., 2015). The increasing focus on training and certification in cybersecurity has also been emphasized as an essential consideration in the National Initiative for Cybersecurity Education (NICE) framework developed by the National Institute for Standards and Technology (NIST).

Furthermore, certifications are commonly referenced as a requirement in job postings (Knapp et al., 2017). When evaluating graduates' qualifications, professional certifications are considered a highly regarded criterion by industry. It has been found that organizations employing cybersecurity professionals assess the candidate's qualifications based on the three indicators (Hentea et al., 2006) including, academic degree/diploma, professional certifications (Cisco Certified Network Associate (CCNA), Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP), GIAC Security Expert Certification (GSEC), …), and vendor-specific certifications (Cisco Certified Security Professional (CCSP), Computing Technology Industry Association (Comp TIA), Security+, …). Hence, it is critical for academic programs to expose students to theoretical concepts, hands-on experiences, and professional certifications to prepare graduates for jobs in cybersecurity.

An issue for IS courses in higher education has centered on teaching practical knowledge while not losing sight of theoretical knowledge. Fortunately, a fair amount of IS theory applies to practical IS skills. There are plenty of IS "training" centers in existence today. Training centers are facilities or online programs (such as Coursera) that provide a knowledge base to pass cybersecurity certification exams but do not include the theory of business or the management side of cybersecurity. Higher education must ensure they are distinguished from "training" centers by developing the proper mix of theoretical knowledge and practical skills to produce well-rounded and employable graduates. This could be solved in the IS security field by providing challenging theory and information that meets the practical skills in high industry demand.

There are many cybersecurity topics and certifications that could be covered. Technology changes, industry standards, workforce needs, government, and regulation should be considered in selecting the most relevant and suitable cybersecurity certificates for the educational program (Knapp et al., 2017). Given that most IS programs offer, at best, one cybersecurity course, which topics are the most important to include? Which topics will make an IS graduate the most marketable and best able to make an impact in the cybersecurity industry? We interviewed industry cybersecurity professionals to get insights into these questions.

Function	Category
Identify	Business Environment; Asset Management; Governance; Risk Assessment; Risk Management
Protect	Awareness and Training; Identity Management and Access Control; Data Security; Information Protection; Maintenance; Protective Technology
Detect	Anomalies and Events; Security Continuous Monitoring; Detection Processes
Respond	Response Planning; Communications; Analysis; Mitigation; Improvements
Recover	Recovery Planning; Improvements; Communications

Table 1. NIST Cybersecurity Framework Main Functions (adapted from NIST, 2021)

Categories	Description
Securely Provision (SP)	Conceptualizes, designs procures, and/or builds secure information technology (IT) systems, responsible for system and/or network development aspects.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Table 2. NICE Framework Main Categories (adapted from NICE, 2019)

4. METHODOLOGY

4.1 Backward Course Design

In general, designing an educational course is a complex process, and considering the best interests of all the parties (institute, students, and industry) make it more complex. Our methodology to design a cybersecurity course aligned with industry needs consists of establishing an education framework developed based on a successful theoretical course design model that aligns with the NIST Cybersecurity Framework, NICE Strategic Plan guidelines, and insights from industry professionals.

The step-by-step process of the proposed cybersecurity course design model includes the following:

- Define the appropriate course learning objectives that are aligned with industry needs
- Identify the appropriate instructional and pedagogical methods
- Identify the acceptable evidence and assessment criteria
- Develop educational content

The proposed model ensures the creation of an effective cybersecurity course that can apply to any cybersecurity educational or training program. The backward course design Model by Wiggins and McTighe (2005) has been considered a robust systematic method to course design that focuses on student learning. It has been used in multiple educational fields at the university level, such as science and liberal arts, with acceptable results. The proposed process connects course learning objectives throughout the curriculum path, assessments, and instructional practices to provide evidence that students have accomplished the course learning objectives. The backward course design model (Wiggins & McTighe, 2005) has three main stages (Figure 1).

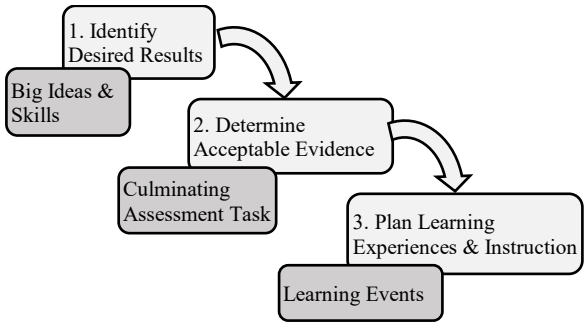


Figure 1. Backward Course Design Model

The first stage is to clearly articulate the final results of the course, i.e., course learning objectives. Phase two, the course assessment, provides evidence that students achieved the identified learning objectives. Stage three includes developing course content, student activities, homework, and lectures designed for each course learning goal.

Cybersecurity graduates need to master both knowledge and skills to be prepared for industry needs. Hence both cognitive and operational aspects of knowledge must be considered in designing any cybersecurity course. Cognitive aspects, remembering, understanding, applying, analyzing, evaluating, and creating, need to be considered with respect to different levels of knowledge, including factual, conceptual, procedural, and metacognitive knowledge (Krathwohl, 2002). Students need the metacognitive knowledge to adapt and apply it to new problems and contexts, particularly in the cybersecurity field. Bloom's Taxonomy was revised to provide a more comprehensive aspect of learning to consider cognitive and operational aspects (Krathwohl, 2002). A recent study suggests using the revised Bloom's taxonomy along with the NICE framework to support the educational development of cybersecurity curriculum (Ramsoonder et al., 2020). The revised Bloom's six cognitive levels are mapped to the NICE framework cybersecurity knowledge, skills, and abilities to identify cybersecurity skills gap and align cybersecurity courses to industry needs.

In line with the revised Bloom's taxonomy, Wiggins and McTighe (2005) believe that there are six facets of understanding: explain, interpret, apply, have perspective, empathize, and self-knowledge. Their framework includes both cognitive aspects of learning, and operational aspects, which makes it suitable for designing cybersecurity courses. We consider the proposed aspects of learning in developing our course learning objectives and will use the backward course design model (Table 3) to guide our redesign process.

To identify the correct course objects for stage one, we used the design stage questions as our guide. We investigated current IS security pedagogical research, reviewed current national standards, and interviewed three industry security experts to ensure the objectives align with industry needs.

4.2 Industry Review and Interviews

Organizations continue to struggle to find graduates with the right skillsets. They believe that having a degree does not necessarily indicate that a candidate is ready for the job. (ISACA, 2020). According to the ISACA report, more than 70 percent of cybersecurity enterprises believe that more than half of the graduates do not have the skills required by industry. Only 27 percent of the industry believes that recent graduates in cybersecurity are well-prepared.

The main concerned areas identified by the industry are as the following:

- Soft skills (32 percent)
- IT knowledge and skills gaps required for cybersecurity (30 percent)
- Insufficient business insight for cybersecurity (16 percent)
- Cybersecurity technical experience (13 percent)
- Insufficient cybersecurity hands-on training (10 percent)

Design Questions	Considerations	Filters (Criteria)	Accomplishes
Stage 1 • Worthy results? • Key desired learnings? • Understanding, knowing, and able to do? • Big Ideas?	- National and local standards - Regional opportunities - Teacher experience and interests	Big ideas and core challenges	Enduring understandings and essential Qs in related to clear goals and standards
Stage 2 • Evidence of desired results? • Evidence of desired understanding?	- Six facets of understanding - Continuum of assessment type	Valid, reliable, and sufficient	Credible and useful evidence of desired learning
Stage 3 • Learning activities and teaching?	- Research-based teaching strategies	Engaging and effective using WHERETO	Coherent learning and teaching activities to develop desired knowledge and skills

Table 3. Backward Course Design Matrix

Industry-emphasized technical skills are the main factor they consider when determining if a cybersecurity candidate is qualified. They rank the top three qualifications as the following:

- Hands-on cybersecurity experience (95 percent)
- Credentials (89 percent)
- Hands-on training (81 percent)

In addition to the insights from industry reports, we conducted interviews with three top cybersecurity professionals having more than twenty years of experience each (a nonprofit government (Gov) organization in the Southeast, a manufacturing (Manu) organization in the Midwest, and a service (Serv) organization in the West) to gain a more specific understanding of what cybersecurity companies are looking for in new cybersecurity hire and their security industry needs. We asked about current security needs and trends, future security needs and plans, and preferred/required qualifications for job candidates by US security companies. Semi-structured questions were constructed, and each interview lasted approximately 30 minutes. The answers were compiled and can be seen in Table 4. The critical interview findings are summarized below.

- High demand for graduates with cyber security hands-on skills
- High demand for cybersecurity graduates with networking knowledge
- High demand for cybersecurity graduates with industry certifications, especially Cisco
- High demand for cybersecurity graduates from business schools that understand the critical business processes and needs
- High demand for motivated graduates who are continuous learners and excited to be in the cybersecurity field
- High demand for graduates with knowledge of legal and regulatory compliance and the non-technical side of cybersecurity
- High demand for graduates with knowledge of the NIST framework

5. THE PROPOSED MODEL

The proposed cybersecurity course is required in our BBA in Management Information Systems (MIS) concentration of loT, Networking, and Cyber Security at a mid-sized AACSB accredited business school in the United States. This course is a 3-credit hour course offered to upper-division MIS major undergraduates and is designed to be offered partially online. This course requires a pre-requisite course, Introduction to Management Information Systems, a 3-credit hour course. In addition to the proposed cybersecurity course, other courses in the concentration are Introduction to Networks, Advanced Networking: Switching, Routing, and Wireless Essentials, and Advance Enterprise Network, Security, and Automation.

The course's principal objective is to prepare students for current cybersecurity market needs. This course delivers the foundation for understanding the critical issues related to defending information assets, defining the levels of defense and response to security events, and establishing a dependable, reasonable information security system with proper intrusion detection and reporting features. Furthermore, this course surveys essential skills in information security program design, networking and application security, the development of information security precautions and information security auditing, disaster recovery, policy development, identity management, and effective threat assessment. Our course aligns with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework to support the uniform communication language for cybersecurity education, training, and workforce development.

Based on the interviews with cybersecurity industry professionals, our school decided to join the Cisco Networking Academy as it provides cybersecurity and networking certifications that perfectly fit current industry needs. Students pursuing the loT, Networking, and Cyber Security concentration are encouraged to pursue professional certifications in Cisco Certified Network Associate (CCNA) and CyberOps Associate Certification to be prepared for a smooth entry into the workforce. Fully certified school instructors teach all the concentration courses in CCNA and CyberOps.

Question Topic	Answers Summary
Current Organizational Needs	• Almost 100% of our networking and cybersecurity technologies are based on Cisco technology. We need people who have experience with Cisco. (Serv) • We currently have to outsource almost all our cybersecurity work to Cisco because we have difficulty finding qualified people to hire. (Manu) • We need people to hire with hands-on experience with Cisco equipment and Cisco security programming. (Serv) • We need cybersecurity employees for analyst, policy, risk management, and networking positions. Our hiring split is around 65% technical - security engineers, architects, pen testers, incident handlers - and 35% management - governance risk and compliance focused. (Gov)
Future Organizational Needs	• We need people with security and networking knowledge and hands-on skills who want to stay with us. The market is so tight for good cybersecurity people. Most cybersecurity people can change jobs every 14 months and receive a substantial increase in pay. (Manu) • Finding good cybersecurity people who will stay. It is hard to find good cybersecurity hires who are willing to stay for more than two years. (Gov) • We need people who are open and continuous learners. Cybersecurity is a vast and ever-evolving space. From a governance, risk, and compliance perspective, new regulations and requirements are constantly being developed. From a technical perspective, threat actors are finding new ways to exploit systems, and new technology is being developed to combat and protect against such threats. (Serv)
Knowledge and skills Needed for new Hires	• Having hands-on with Cisco equipment and virtual lab experience. (Serv) • We look for CCNA and CISSP certifications. (Manu) • We look for people who can understand critical business needs and can understand how those needs relate to cybersecurity policies that make sense. (Serv) • We look for people who can understand risk management and network design from the business' point of view, meaning someone who can ask the right questions and know how to set up a network that would best support the most critical business processes. (Manu) • We look for hands-on experience followed by specific coursework. Industry certifications always help in the hiring process. (Gov) • Knowledge of the NIST framework. (Gov) • Fundamental knowledge of the OSI model and TCP/IP work and how packets move over the Internet. (Serv) • Understand the focus needs to be on the business and supporting the business and the users. (Manu) • Understanding the legal and regulatory compliance and the non-technical side of cybersecurity. (Gov)
What Stands out in Interviews	• We look for CISSP and Cisco certifications, but they are hard to find. (Manu) • Having hands-on experience with networking equipment and virtual labs would make an applicant very attractive. (Serv) • Have hands-on experience from internships, labs, or job shadowing. • Someone who is excited to be in the cybersecurity field. (Gov) • Membership in a professional organization such as ISACA as well as participating in industry events and competitions such as competitions. (Serv)

Table 4. Summary of Interviews

5.1 Step 1 - Identify Desired Results (Learning Objectives)

Course learning objectives guide students to navigate the material, learn the essential course elements, and develop the required ability. The first important task in designing a course is to align the course objectives to connect the course material to industry needs. This critical piece is missing from the current cybersecurity curricula, as most graduates need additional post-graduation training from companies hiring them.

We define the course learning objectives based on the following to ensure alignment with the industry needs:

- NIST Cybersecurity Framework's main functions and categories
- NICE Cybersecurity framework main categories and specialty areas
- The data from industry interviews and published reports

The backward course design model requires identifying "big ideas" and "core tasks" before identifying the "important to know" and the course learning objectives. We first identify the big ideas of the course. Then, NIST main functions (presented in Table 1) and NICE main categories (presented in Table 2) are used to identify core tasks. Then, course learning objectives are developed according to the detailed levels of both NIST and NICE frameworks. Table 5 shows the proposed course learning objectives mapped to the related NIST and NICE framework components, designed based on the backward course design model.

The final course learning objectives, according to the AACSB standard format, are as the followings:

- After completing the course, the student will be able to comprehend the major concepts of information security, including inspection and defense of information assets, detection of and reaction to threats, examination of pre- and post-incident procedures, technical and managerial responses, security planning, maintenance, and recovery, security legal and ethical issues, and staffing functions.

Proposed Learning Objective	NIST Framework	NICE Framework
Big Ideas - Cybersecurity risk assessment - Cybersecurity protection - Cybersecurity detection - Cybersecurity response and recovery - Cybersecurity planning	High-level & strategic knowledge of organization cybersecurity risk management: identify, assess, and respond to cybersecurity risk	Plan, implement and monitor a successful cybersecurity course
Core Tasks - Identify and assess cybersecurity risks & threats - Protect information security assets - Detect and respond to cybersecurity incidents - Plan, evaluate, and improve organization cybersecurity risk management and recovery.	NIST Main Functions - Identify (ID) - Protect (PR) - Detect (DE) - Respond (RS) - Recover (RC)	NICE Main Categories - Securely Provision (SP) - Operate and Maintain (OM) - Oversee and Govern (OV) - Protect and Defend (PR) - Analyze (AN) - Collect and Operate (CO) - Investigate (IN)
Important to Know (Course Learning Objectives (OB)) OB1. Data and Information security OB2. Risk assessment, mitigation, and improvement OB3. Cybersecurity threats & attacks OB4. Information asset protection processes, procedures, and technologies OB5. Cybersecurity incident detection processes, procedures, and technologies OB6. Cybersecurity incident analysis processes, procedures, and technologies OB7. Cybersecurity response processes, procedures, and technologies OB8. Cybersecurity recovery planning & improvement OB9. Cybersecurity maintenance OB10. Cybersecurity plan and policy OB11. Physical security OB12. Legal & ethical issues OB13. Managerial issues OB14. Security staffing functions OB15. Industry professional cybersecurity certificates	NIST Categories ID.AM - Asset Management ID. BE - Business Environment ID. GV- Governance ID. RA- Risk Assessment ID.RM- Risk Management PR. AC- Identity Management and Access Control PR.AT- Awareness and Training PR. DS- Data Security PR. IP- Information Protection Processes and Procedures PR. MA- Maintenance PR. PT- Protective Technology DE. AE- Anomalies and Events DE.CM- Security Continuous Monitoring DE. DP- Detection Processes RS. RP- Response Planning RS. CO- Communications RS.AN- Analysis RS.MI- Mitigation RS. IM- Improvements RC. RP- Recovery Planning RC. IM- Improvements RC. CO- Communications	NICE Selected Specialty Areas SP. RSK- Risk Management SP. SRP- Systems Requirements Planning SP. TST- Test and Evaluation SP.SYS- Systems Development OM. DTA- Data Administration OM. KMG- Knowledge Management OM. STS- Customer Service and Technical Support OM.NET- Network Services OM. ADM- Systems Administration OM.ANA- Systems Analysis OV. LGA- Legal Advice and Advocacy OV. TEA- Training, Education, and Awareness OV. MGT- Cybersecurity Management OV.SPP- Strategic Planning and Policy OV. EXL- Executive Cyber Leadership (EXL) OV. PMA- Program/Project Management PR.CDA- Cyber Defense Analysis PR. INF- Cyber Defense Infrastructure Support PR. CIR- Incident Response PR. VAM- Vulnerability Assessment and Management AN. TWA- Threat Analysis AN.EXP- Exploitation Analysis AN. ASA- All-Source Analysis CO.OPL- Cyber Operational Planning CO.OPS- Cyber Operations IN.INV- Cyber Investigation IN.FOR- Digital Forensics

Table 5. Course Learning Objectives Related to NIST and NICE Frameworks

- After completing the course, the student can identify cyber trends, threats, attacks, cybercrime, cybersecurity technologies, and procedures used to protect and defend networks by using the spectrum of security activities, methods, methodologies, and procedures.
- After completing the course, the student can monitor, detect, analyze, and respond to cybersecurity incidents using Cisco Network Academy cybersecurity hands-on tools.
- After completing the course, the student will develop critical thinking and problem-solving skills using real equipment and Cisco cybersecurity tools, labs, and packet tracers.
- After completing the course, the student can prepare for an industry professional cybersecurity certificate, Cisco Certification in CyberOps Associate.

Next, we must determine the correct mix of theory and hands-on skills. The industry's main concern was a lack of hands-on technical skills, based on the ISACA's 2020 report and the data from our interviews.We decided to integrate Cisco technology into our cybersecurity course for hands-on learning and practical skills-building to address this significant concern and better support student learning and engagement. Integrating the hands-on skills from Cisco into the course, a highly regarded certificate by industry, helps ensure that the student's learning is mapped to the highest level of creating and implementing the knowledge. Students can acquire the Cisco CyberOps Associates certificate by completing this course.

Table 6 represents the course units designed based on the learning objectives derived from the NIST and NICE framework and using the backward course design methodology. Each unit is designed to cover approximately 2 to 3 sessions in a 16-week one-semester 3-credit hour course. All the assignments, including case studies, projects, and labs, are spread along with the 16 weeks program. Estimates of class schedule and hours and related assignments are presented in Table 6.

Course Units	Cybersecurity Hands-On Skills	Learning Objectives	Schedule Estimates
Unit 1- Introduction to Cyber Security	1.1.6 - Lab - Cybersecurity Case Studies 27.1.5 - Lab - Convert Data into a Universal Format - Chapter exam	OB1, OB3, OB15	Week 1: 2 sessions, 3 hours
Unit 2- Information Security in Organization	1.0.6 - Class Activity - Top Hacker Shows Us How It's Done - Chapter exam	OB1, OB3, OB8, OB10, OB15	Week 2: 2 sessions, 3 hours
Unit 3- Legal, Ethical, and Professional Issues in Information Security	- Cyber security & privacy project - Chapter exam	OB10, OB12, OB13	Week 3: 2 sessions, 3 hours
Unit 4- Cyber Attacks, Cybersecurity Protection and Defense Systems	1.2.3 - Lab - Learning the Details of Attacks 1.3.4 - Lab - Visualizing the Black Hats 2.2.5 - Lab – Becoming a Defender 3.2.11 - Lab - Exploring Processes, Threads, Handles, and Windows Registry 14.1.11 - Lab - Anatomy of Malware 14.2.8 - Lab – Social Engineering 17.2.6 - Lab - Attacking a MySQL Database 25.3.10 - Packet Tracer - Explore a NetFlow Implementation 25.3.11 - Packet Tracer - Logging from Multiple Sources - Chapter exam	OB1, OB3, OB4, OB5, OB6, OB7, OB11, OB15	Weeks 4-5: 4 sessions, 6 hours
Unit 5- Cybersecurity Technology: Access Controls, Firewalls, and VPNs	3.3.10 - Lab - Create User Accounts 3.3.11 - Lab - Using Windows PowerShell 3.3.13 - Lab - Monitor and Manage System Resources in Windows 4.2.6 - Lab – Working with Text Files in the CLI 4.2.7 - Lab – Getting Familiar with the Linux Shell 4.4.4 - Lab – Locating Log Files 4.5.4 - Lab - Navigating the Linux Filesystem and Permission Settings 12.3.4 - Packet Tracer - ACL Demonstration 21.2.12 - Lab - Examining Telnet and SSH in Wireshark 21.4.7 - Lab – Certificate Authority Stores 26.1.7 - Lab - Snort and Firewall Rules - Chapter exam	OB3, OB4, OB5, OB6, OB7, OB11, OB15	Weeks 6-7: 4 sessions, 6 hours
Unit 6- Security Technology: Intrusion Detection and Prevention Systems	5.1.5 - Lab - Tracing a Route 5.3.7 - Lab - Introduction to Wireshark 7.2.8 - Packet Tracer – Verify IPv4 and IPv6 Addressing 8.2.8 - Lab - Using Wireshark to Examine Ethernet Frames 9.2.6 - Lab – Using Wireshark to Observe the TCP 3-Way Handshake	OB3, OB4, OB5, OB6, OB7, OB11, OB15	Weeks 8-11: 8 sessions, 12 hours

	9.3.8 - Lab - Exploring Nmap 10.2.7 - Lab - Using Wireshark to Examine a UDP DNS Capture 10.4.3 - Lab - Using Wireshark to Examine TCP and UDP Captures 10.6.7 - Lab - Using Wireshark to Examine HTTP and HTTPS Traffic 12.1.9 - Packet Tracer - Identify Packet Flow 15.0.3 - Class Activity – Network Monitoring- What's Going On? 15.2.7 - Packet Tracer - Logging Network Activity 17.1.7 - Lab - Exploring DNS Traffic 17.2.7 - Lab - Reading Server Logs 27.2.9 - Lab – Regular Expression Tutorial 27.2.10 - Lab - Extract an Executable from a PCAP 27.2.12 - Lab - Interpret HTTP and DNS Data to Isolate Threat Actor 27.2.14 - Lab - Isolate Compromised Host Using 5-Tuple 27.2.15 - Lab - Investigate a Malware Exploit - Chapter exam		
Unit 7- Physical Security	- Chapter exam	OB4, OB11, OB14	Weeks 12: 1 session, 1.5 hours
Unit 8- Cryptography	21.0.3 - Class Activity - Creating Codes 21.1.6 - Lab – Hashing Things Out 21.2.10 - Lab - Encrypting and Decrypting Data Using OpenSSL 21.2.11 - Lab - Encrypting and Decrypting Data Using a Hacker Tool - Chapter Quiz	OB4, OB5, OB6, OB15	Weeks 12-13: 3 sessions, 4.5 hours
Unit 9- Security Planning	- Business continuity plan - Chapter exam	OB2, OB8, OB9, OB10, OB11, OB13, OB14	Weeks 14: 2 sessions, 3 hours
Unit 10- Risk Management	- Risk management assignment - Chapter exam	OB2, OB8, OB13, OB14	Weeks 15: 2 sessions, 3 hours
Unit 11- Security Maintenance	27.2.16 - Lab - Investigating an Attack on a Windows Host 28.4.12 - Lab - Incident Handling - Chapter exam	OB8, OB9, OB10, OB13, OB14	Weeks 16: 2 sessions, 3 hours

Table 6. Course Units Related to the Learning Objectives

5.2 Step 2- Identify Instructional Methods

In the next stage of backward course design, instructional strategies and learning activities are designed that work best for the learning objectives and assessment methods (Wiggins & McTighe, 2005). For developing engaging and effective course instructional strategies, we use the WHERETO (Where is it going? Hook the students; Explore and equip; Rethink and revise; Exhibit and evaluate; Tailor to student's needs, interests, and styles; Organize for maximum engagement and effectiveness) elements suggested by Wiggins and McTighe (2005). In the following, we list the instructional strategies used in the cybersecurity course.

The backward course design model has three main types of instructional methods: direct, facilitative and constructive, as well as coaching. We leverage the various instructional strategies listed below.

Direct Instructional Methods

- Traditional lectures and presentations
- Flipped classroom method
  - D2L Course Management System
  - Cisco Networking Academy
- Effective educational videos

Facilitative and Constructive Methods

- Cooperative learning
  - Class Activities
- Discussion
  - Case studies
- Experimental inquiry
  - Hands-on Skill Simulation labs and Packet Tracers
- Problem-based learning
  - Hands-on Skill Labs and Packet Tracers
- Writing process
  - Research paper

Coaching Methods

- Traditional and online office hours
- Guided practice and feedback
- National and local industry guest speakers

The flipped classroom method has been used for years as an effective method to help improve student learning. "Flipping the classroom" means that students do the lower levels of cognitive work (gaining knowledge and comprehension)

outside of class and focus on higher forms of cognitive work (application, analysis, synthesis (create), and/or evaluation) in class, with the support of their peers and instructor (Bloom, 1956). Two recent meta-analyses found that a flipped classroom is significantly more effective in enhancing student learning than other traditional instructional methods (Galindo-Dominguez, 2021; Hew & Lo, 2018). There have been mixed findings regarding student preference and liking of the flipped classroom. For example, a recent study found an overall positive student perception of a flipped classroom (Francis et al., 2020). While another recent study found that using a flipped classroom may not improve students' subjective liking of the course, as measured by student evaluations (Gren 2020). A meta-analysis by Galindo-Dominguez (2021) suggests that increasing student motivation, self-efficacy, and engagement may be more beneficial. However, this approach demands self-discipline and motivation, and many students may not have experienced flipped learning before (Francis et al., 2020). Hence, there is still a need for more research on this method concerning student perception, liking, and preference.

But one of the main principles of a flipped classroom is that it promotes deeper learning through hands-on activities. The flipped classroom enables instructors to provide online instructional videos, slides, and other materials that can be learned and referred to at their own pace and at any time and location that is convenient to the student. This approach suits individuals' learning needs instead of the traditional class lectures that may be too fast for some while others can become bored. And the class time can be used more effectively, adjusting to students' needs, such as having labs, helps sessions, and discussions.

In the field of cybersecurity, hands-on security analysis and response simulation activities are very effective in helping students to organize their conceptual knowledge in ways that facilitate retrieval and application. When students gain basic knowledge through online lectures, their classroom time can be spent deepening their understanding and increasing their hands-on skills using their cybersecurity knowledge.

5.3 Step 3- Identify Acceptable Evidence (Assessment)

In the next stage of the backward course design model, appropriate assessments for each learning goal are designed to demonstrate understanding and learning (Wiggins & McTighe 2005). It is essential to use a wide range of assessment methods matched to the learning objectives, and there will be a combination of several different assessment methods.

In this stage, the acceptable evidence is designed to show that students have learned the desired knowledge and skills. What is accepted as evidence that students are making progress toward the course's learning objectives? According to the backward course design model, to ensure that all the learning objectives are tested, a wide range of assessment methods (essay tests, term papers, short-answer quizzes, homework assignments, lab projects, problems to solve, etc.) need to be considered, which means that the assessments should match the learning objectives to attain the correct evidence.

According to the backward course design model, we designed the course assessments in relation to stages one and two, meaning that all the assessments were created in relation to their course learning objectives. All the assessments were developed by answering the stage three questions and related to the learning objectives defined in stage one. Thus, succeeding in each assessment, measured by assessment grade, directly represents succeeding in the related course learning objective.

In this process, there are important questions that need to be answered:

Direct Evidence:

- What will count as evidence of success for learners?
- What are the key observable indicators of short- and long-term progress?

Indirect Evidence:

- What other data (e.g., achievement gaps; staff understandings, attitudes, practices; organizational capacity, etc.) should be collected?

As direct evidence, we use chapter quizzes and exams, hands-on lab assignments, case studies and projects, final exam, and final skills assessments. Additionally, as indirect evidence, we will track student success for those who take the Cisco certification exam. Accordingly, we design our assessment methods presented in the following:

Worth being familiar with learning objective group

- Online quizzes (MC and T/F)
- Real-world case studies

Important to know learning objective group

- Online quizzes (MC and T/F)
- Chapter exams
- Cisco CyberOps packet tracer & lab assignments
- Research project
- Final Exam

Enduring knowledge learning objective group

- Cisco CyberOps packet tracer & lab assignments
- Hands-on risk management assignments
- Cyber security project
- Cyber privacy project
- Term project on a business continuity plan
- Final exam
- Final hands-on skills assessment test

The course assessments are designed to cover technical cybersecurity skills and general soft skills required by industry. As suggested by research, hands-on cybersecurity learning opportunities help students to develop both analytical and soft skills, such as problem-solving skills and communication skills (Crumpler & Lewis, 2019). The designed assessments not only examine students' technical skills, but by completing them, students develop essential soft skills, such as critical thinking, problem-solving, and written and verbal communication.

6. EVALUATION

According to understanding by design (Wiggins & McTighe, 2005), ultimate students' performance is achieved by continuous results reviews followed by revising the course accordingly. Feedback from students and peers must be used to revise the course and adjust the design and teaching approaches. The three stages of the backward course design process are followed by a "unit design cycle" to help design, edit, critique, peer-review, share, and improve the designed course. The unit design cycle model is shown in Figure 2.

There are two stages in the unit design cycle model: design and trial. We first defined the course learning goals in the design stage and studied the current gaps. Next, we used three stages of the backward course design model (as presented in the proposed model section) to design the course. We worked in a team with the school's instructors and industry representatives to design the proposed model.

Next, instructors and industry representatives reviewed the proposed model against NIST/NICE standards and industry needs. In the trial (or evaluation) stage, we used three criteria to evaluate the proposed course and revised it accordingly. The three criteria include student feedback, expert reviews (NIST guidelines, industry representatives, and instructor peers review), and our observations of students' work and comments. In the following, we discuss the three evaluation criteria and explain how each evaluated the proposed course model.

6.1 Evaluation Criteria 1 - Course Evaluations and Student Feedback

We modified the proposed feedback items by Wiggins and McTighe (2005) and created a questionnaire using a 5-point Likert Scale to get students' feedback. The proposed course was taught in three sections across two semesters, including two sections in Spring 2019 and one section in Spring 2020. A summary of students' end-of-the-course evaluations based on the Wiggins and McTighe's (2005) questionnaire for all three courses is presented in Table 7.

6.2 Evaluation Criteria 2 - Expert Review

In accordance with the NIST framework, we followed the "NIST evaluation requirements" as our first guide to an expert review of a cybersecurity course designed for industry needs. According to NIST, evaluating a cybersecurity course's effectiveness has four distinct but interrelated purposes to measure:

- The extent to which conditions were right for learning and the learner's satisfaction.
- What a student has learned from the course or training event, i.e., learning effectiveness.
- A pattern of student outcomes following the course, i.e., teaching effectiveness.
- The value of the class or training event, i.e., course effectiveness.

Accordingly, four levels of evaluation are offered by NIST for organizational cybersecurity training events, as the following:

- Level 1: end of the course evaluations (student satisfaction)
- Level 2: objective testing (learning and teaching effectiveness)
- Level 3: job transfer skills (performance effectiveness): applies only to employee training courses
- Level 4: organizational benefit (training course effectiveness): applies only to employee training courses.

This designed cybersecurity course is offered as a part of an MIS higher education program (not an organizational training course). Thus, we only use the first two first levels of evaluations that apply to the educational courses. Level 1 of the evaluations is presented as the student end of the course evaluations in Table 7 and the student end of the course comments. And level 2 of the evaluation is presented as students' grades in Table 8 (or the analysis of student work in the unit design cycle model).

In addition to the NIST evaluation criteria, we asked industry experts to review the final designed course to verify it is aligned with their current cybersecurity needs. All three industry representatives confirmed that the course is designed according to their requirements and meets their current needs. We also asked academic peers to review the final designed course to validate that the planned requirements were implemented appropriately. The two peer instructors confirmed that the planned goals and requirements are covered and implemented appropriately in the course.

Evaluation Criteria	Spring 2019	Spring 2019	Spring 2020
Class discussions and/or activities helped me to understand the subject matter.	4.5	4.7	4.3
Course assignments helped me to understand the subject matter.	4.6	4.8	4.4
Course content was presented effectively.	4.6	4.8	4.5
Required course texts and/or materials helped me to understand the subject matter.	4.6	4.7	4.4
Test content was representative of the assigned material.	4.5	4.9	4.6
Tests and/or assignments required problem-solving, critical thinking, and/or creative thought.	4.5	4.8	4.4
The instructor demonstrates knowledge of his/her discipline.	4.6	4.7	4.5
The instructor clearly explains course expectations.	4.6	4.8	4.7
The instructor clearly explains how students will be evaluated.	4.6	4.7	4.6
The instructor evaluates and returns tests and assignments in a reasonable period of time.	4.5	4.8	4.6
The instructor presents the material in an organized manner.	4.7	4.6	4.6
The instructor communicates effectively.	4.5	4.7	4.5
The instructor demonstrates respect for students.	4.7	4.8	4.6
The instructor is receptive and responsive to the sharing of ideas during course discussions.	4.6	4.8	4.6

Table 7. Summary of Student's Feedback

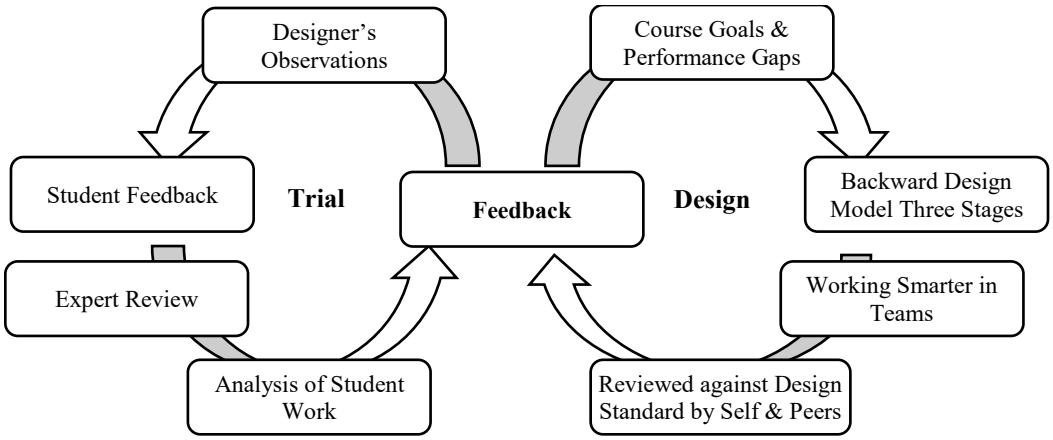


Figure 2. The Unit Design Cycle for Evaluating the Proposed Model

6.3 Evaluation Criteria 3 - Designer Observations

While teaching the newly designed cybersecurity course, we observed students' performance and captured student feedback. A summary of the student comments received from the end of the course evaluations is presented below.

Many students mentioned that they learned about the following:

- All the important cybersecurity concepts, principles, and the key issues
- The important cybersecurity tools and hands-on practices
- Cybersecurity management and related business issues and technology capabilities
- Cybersecurity attacks and threats
- Cybersecurity response and recovery
- Network security and measures
- The knowledge and skills required for a future career in cybersecurity
- Using the knowledge and skills in the course in my current job

And:

- They are planning to work in the cybersecurity field
- They got motivated for more in-depth Cybersecurity classes
- They earned the Cybersecurity certificate in this course which is valuable in the job market

The observation of student work was very satisfactory. Overall, 91% of the students passed the course with grades A or B, meaning they gained mastery-level knowledge and skills based on the designed acceptable assessment criteria related to course objectives. As shown in Table 8, all students passed the course in the three sections, with the following grade distribution, 56% A's, 35% B's, 7% C's, and 2% D's.

7. DISCUSSION AND LIMITATIONS

In response to the industry's massive shortage of cybersecurity graduates, we designed a cybersecurity course to meet industry needs using the backward course design model aligned with the NIST Cybersecurity Frameworks and NICE guidelines and with valuable insights from industry's top-ranked professionals. The proposed cybersecurity course is developed as part of the cybersecurity concentration at a medium-sized business school in the United States. Our proposed model provides a solid foundation for any educational institute to design a cybersecurity course for industry and academic needs. The main contributions of our paper are summarized in the following:

- First, we propose an educational design model with a step-by-step process to design a cybersecurity course aligned with the industry's needs in response to the current massive shortage of cybersecurity professionals.
- Second, the proposed model is based on the related learning theories (such as revised Bloom's taxonomy) integrated with highly regarded industry certificate hands-on skills to meet the current industry needs for hands-on technical skills for cybersecurity graduates.
- Third, the methodology used to develop the proposed model is based on the highly successful outcome-based course design model that draws on Wiggins and McTighe's (2005) backward course design model.
- Fourth, the learning objectives, content, instructional methods, and assessment evidence are designed in alliance with the NIST Cybersecurity Framework, NICE Cybersecurity Strategic Plan, and the insights from interviewing cybersecurity professionals.
- Fifth, the results were highly satisfactory, evaluated by multiple criteria (following the unit design cycle) according to industry guidelines, students' feedback, and the designer's observations.
- Sixth, the proposed model can be used by any other higher education institute to design a cybersecurity course aligned with industry needs.

Course	Passed	A	B	C	D	Failed
Spring 19-01	100%	36%	54%	4%	7%	0%
Spring 19-02	100%	50%	46%	4%	0%	0%
Spring 20-01	100%	78%	9%	13%	0%	0%
All	100%	56%	35%	7%	2%	0%

Table 8. Students' Performance (Final Grades)

There are limitations to this study that can be addressed in future works. This course is designed to prepare MIS graduates with a cybersecurity concentration for the United States cybersecurity workforce needs. When applying the proposed course model to a different cybersecurity market/industry, course content, learning objectives, instructional methods, and assessment criteria modification is necessary to align with the target market/industry needs. Considering the fast pace of technological advances in cybersecurity, continuous improvement to the course content, assignments, and certification paths is needed to stay aligned with current industry needs. To stay aligned with industry needs, having regular contact with industry professionals, and including them in the educational program, such as having regular industry guest speakers or talent day, are suggested. The proposed course model is designed using the backward course design methodology, and other methods can be used to compare the results.

Similarly, different offering methods can be used to compare the results instead of the flipped classroom method and partially online. Further efforts can be made as extracurricular activities to increase students' interest in the cybersecurity field, such as annual hackathons events. The certification exam vouchers are currently offered for students who perform well in the course at a discount. After a while, further cost and benefit analysis can be done to examine graduates' success rate who take the certification exam and are successful.

8. CONCLUSION

In this study, we present the step-by-step process of this complex task. We first look to the literature on cybersecurity needs and interview cybersecurity professionals. Then we investigate the appropriate course design methodology with proven results based on the fundamental learning theories. We use backward course design principles to align the course with industry needs. The proposed model uses the three main stages of backward course design: identifying desired results, determining acceptable evidence, and planning learning experiences and instruction.

In stage one, course educational outcomes and learning objectives are redesigned to align with the industry needs. In stage two, all the course assessment criteria and acceptable evidence are designed to support the updated learning objectives, and in stage three, instructional methods and learning activities are redesigned. The course learning objectives are developed in alliance with the NIST main functions and categories, the NICE workforce categories and specialty areas, and the industry professionals' insights. Course content, instructional methods, and assessment criteria are designed based on backward course design to produce the expected knowledge and skills (learning objectives). The highly regarded Cisco Cybersecurity Operations certificate and the related hands-on skills are used along with the theoretical concepts. Lastly, we assess the proposed design's success by evaluating the student's knowledge and skills, student's feedback and perception of the course, expert review, and the designer's observations. The evaluation outcome is highly satisfactory.

9. REFERENCES

Abraham, S., & Shih, L. (2015). Instructional Perspective: Towards an Integrative Learning Approach. Cybersecurity Education. *Information Security Education Journal*, 2(2), 84-90.

Armstrong, M. E., Jones, K. S., Namin, A. S., & Newton, D. C. (2020). Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals. *ACM Transactions on Computing Education (TOCE)*, 20(4), 1-25.

Bicak, A., Liu, X. M., & Murphy, D. (2015). Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program. *Information Systems Education Journal*, 13(3), 99-110.

Bloom, B. S. (1956). *Taxonomy of Educational Objectives.* Vol. 1: Cognitive Domain. New York: McKay, 20-24.

Burrell, D. N. (2020). An Exploration of the Cybersecurity Workforce Shortage. *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1072-1081). IGI Global.

Crumpler, W., & Lewis, J. A. (2019). *The Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS).

CyberSeek (2021). Cybersecurity Supply/Demand Heat Map, September 3. *https://www.cyberseek.org/heatmap.html*

Francis, N., Morgan, A., Holm, S., Davey, R., Bodger, O., & Dudley, E. (2020). Adopting a Flipped Classroom Approach for Teaching Molar Calculations to Biochemistry and Genetics Students. *Biochemistry and Molecular Biology Education*, 48(3), 220-226.

Galindo-Dominguez, H. (2021). Flipped Classroom in the Educational System. *Educational Technology & Society*, 24(3), 44-60.

Gren, L. (2020). A Flipped Classroom Approach to Teaching Empirical Software Engineering. *IEEE Transactions on Education*, 63(3), 155-163.

Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education: Research*, 5(1), 221-233.

ISACA (2020). State of Cybersecurity 2020 Part 1: Workforce Development, February, 24, 2020*:* https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2020/isacas-cybersecurity-study-reveals-struggles-with-hiring-and-retention-persist-more

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.

Krathwohl, D. R. (2002). A Revision of Bloom's Taxonomy: An Overview. *Theory into Practice*, 41(4), 212-218.

NICE (2019). National Initiative for Cybersecurity Education (NICE) Strategic Plan, National Institute of Standards and Technology (NIST), Editor. NIST: Washington, DC.

NICE Academic Spotlight (2018). *Using the NICE Cybersecurity Workforce Framework to Develop a Cybersecurity Legal Awareness Course*. NIST: Washington DC. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-summer-2018-enewsletter#Academic%20Spotlight

NIST (2021). *Cybersecurity Framework*. National Institute of Standards and Technology (NIST), Washington DC. https://www.nist.gov/cyberframework/getting-started

Ramsoonder, N. K., Kinnoo, S., Griffin, A. J., Valli, C., & Johnson, N. F. (2020). Optimizing Cyber Security Education: Implementation of Bloom's Taxonomy for future Cyber Security workforce. *2020 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 93-98). IEEE.

Shieber, J. (2019). The Lack of Cybersecurity Talent Is 'a National Security Threat,' says DHS office. *Disrupt SF 2019*, Tech Church.

Tan, Y. L., Nakata, K., & Paul, D. (2018). Aligning IS Master's Programs with Industry. *Journal of Information Systems Education*, 29(3), 169-182.

Wiggins, G., & McTighe, J. (2005). *Understanding by Design*. ASCD.

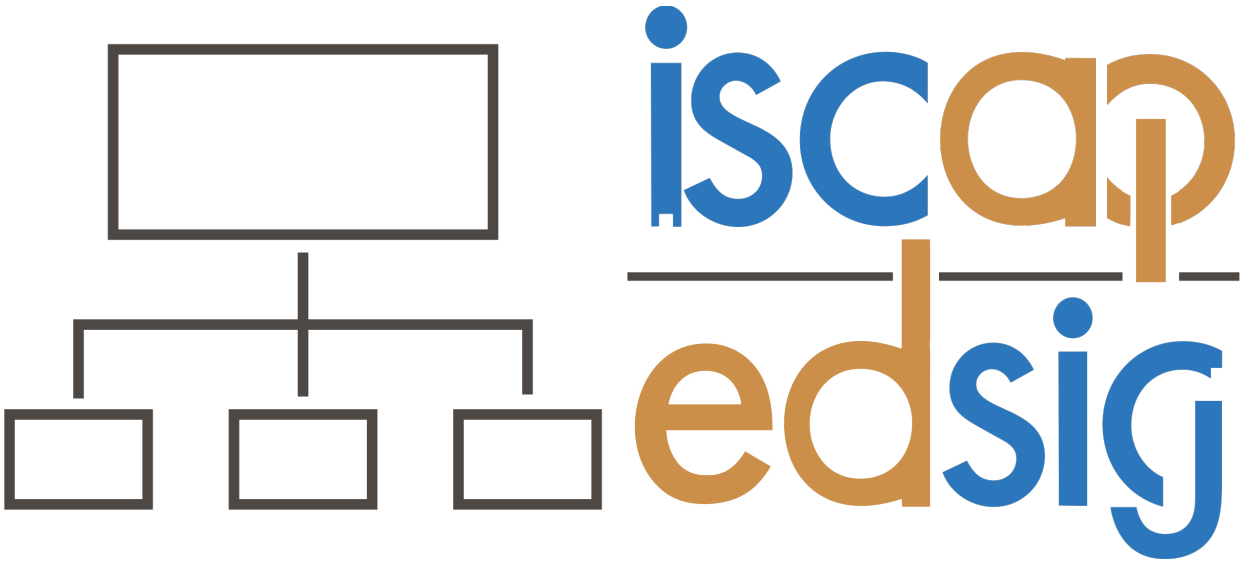
Ward, P. (2021). Constructing a Methodology for Developing a Cybersecurity Program. *Proceedings of the 54th Hawaii International Conference on System Sciences* (p. 44).

Yuan, X., Yang, L., He, W., Ellis, J. T., Xu, J., & Waters, C. K. (2017). Enhancing Cybersecurity Education using POGIL. *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education* (pp. 719-719).

AUTHOR BIOGRAPHIES

Gelareh "Ellie" Towhidi is an assistant professor of management information systems in the Richards College of Business at the University of West Georgia. She received her Ph.D. from the University of Wisconsin-Milwaukee. She teaches Web Programming, Enterprise Systems, Business Intelligence, Networking, and Cybersecurity courses. She is a Cisco certified instructor in CCNA 1, 2, 3, and CyberOps; and SAP TERP 10 and ERPsim certified instructor. Her current research interests include big data, business analytics, user behavior, and information systems education.

Jeannie Pridmore is a professor of management information systems in the Richards College of Business at the University of West Georgia. She received her Ph.D. from Auburn University. She teaches Enterprise Systems, Business Intelligence, Networking, and Cybersecurity courses. She is a Cisco certified instructor in CCNA 1, 2, 3, CyberOps, DevNet; and SAP and ERPsim certified instructor. Her research includes virtual teams, decision-making, and innovative education.



Information Systems & Computing Academic Professionals

Education Special Interest Group

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)