CYBERSECURITY INDUSTRY NEEDS AND THE CSEC ABET CURRICULUM ANALYSIS

by

Sienna Bates

A Thesis

Submitted to the Faculty of Purdue University
In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology
West Lafayette, Indiana
August 2022

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Marcus Rogers, Co-Chair
Department of Computer and Information Technology

Dr. Umit Karabiyik, Co-Chair
Department of Computer and Information Technology

Dr. Ida Ngambeki
Department of Computer and Information Technology

Dr. John Springer
Department of Computer and Information Technology

Approved by:
Dr. John A. Springer

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

A+ - CompTIA A+

ABET - Accreditation Board for Engineering and Technology

CAC - Computing Accreditation Commission

CASP+ - CompTIA Advanced Security Practitioner

CCNA - Cisco Certified Network Associate

CCNP - Cisco Certified Network Professional

CCO – Center for Career Opportunities

CISA - Certified Information Systems Auditor

CISM - Certified Information Security Manager

CISO – Chief Information Security Officer

CISSP - Certified Information Systems Security Professional

CIT – Computer and Information Technology

CNIT – Computer and Information Technology

CS – Computer Science

CSEC – Cybersecurity

CSV - comma-separated values

CySA+ - CompTIA Cybersecurity Analyst

ICS2 - International Information Systems Security Certification Consortium

IS – Information Systems

ISACA - Information Systems Audit and Control Association

IT – Information Technology

KSA – Knowledge, Skills, Abilities

KST – Knowledge, Skills, Tasks

Network+ - CompTIA Network+

NICE – National Initiative for Cybersecurity Education

NIST – National Institute of Standards and Technology

Pentest+ - CompTIA Pentest+

PPI – Purdue Polytechnic Institute

RSA – Rivest, Shamir, and Adleman

SANS/GIAC - Global Information Assurance Certification

Security+ - CompTIA Security+

ABSTRACT

In the recent years, companies in the IT/cybersecurity industry have expressed their concerns about the lack of knowledge entry level cybersecurity employees are experiencing after graduating from a four-year cybersecurity program. Organizations such as National Initiative for Cybersecurity Education (NICE) which is led by the National Institute of Standards and Technology (NIST) provides a framework to map certain knowledge, skills, and tasks that have provided a way for universities to build their cybersecurity course curriculums. By following this framework at the competency level, it can be used to ensure students are adequately prepared for industry level jobs upon graduation from a four-year cybersecurity program. The goal of this study was to explore if there are gaps in terms of workforce development for cybersecurity competencies that graduates from ABET-accredited four-year bachelor's cybersecurity -IT programs (Degrees and Majors) have? For this research, there were three phases: a gap analysis, a survey, and a comparison. A gap analysis was conducted to assess the current cybersecurity curriculum for Purdue University's undergraduate four-year program. The survey was conducted amongst a list of companies, obtained from Purdue University's Center for Career Opportunities (CCO) who have previously hired students from the four-year cybersecurity program in the Polytechnic Institute. Finally, a comparison was done to show what the gap analysis was, what was originally thought to be missing from the current curriculum, what industry said was missing, what was the same and what was different. It has been determined that a gap does exist, and this survey's results concluded there were three common issues with hiring new cybersecurity talent as well as identified what competencies were originally thought to be missing based on the gap analysis and the industry survey. Also, while industry certifications are not required to secure entry level positions at the companies who responded to the survey, they certainly are preferred. This research can help make students from the four-year undergraduate cybersecurity program at Purdue University be more competitive when applying for entry-level cybersecurity industry positions upon graduation.

1. INTRODUCTION

1.1 Background

It can be difficult to keep up to date with new and upcoming cybersecurity skills, threats, and tools. New threats are emerging every day that require cybersecurity professionals to have a solid understanding of common practices and standards within the cybersecurity industry. Now industry professionals are already expected to have a baseline understanding of these, but how these standards and practices are being taught in university programs with cybersecurity degrees, majors, and programs needs to be explored further.

Many organizations offer training courses and certifications of proficiency for cybersecurity professionals to stay up to date on specific areas and topics. These industry certifications are typically preferred for entry-level professionals but not always required to make a student stand out who might already have a cybersecurity degree. These certifications, on top of a degree aim to show a student is willing to make the extra effort to show proficiency in what they have learned in their degree program. Organizations such as the National Initiative for Cybersecurity Education (NICE) which is led by the National Institute of Standards and Technology (NIST) provide cybersecurity education, training, and workforce development for those in the cybersecurity industry. NICE provides a framework to map certain knowledge, skills, and tasks (competencies) that can be used as a way to build a cybersecurity course curriculum to adequately prepare students for the industry upon graduation (NICE Cybersecurity Workforce Framework, n.d.). This framework has been mapped to identify 38 different competencies in the Purdue University Bachelor of Science four-year undergraduate Cybersecurity degree in the Computer and Information Technology department. This is important because having these competencies met in a four-year cybersecurity degree curriculum can set a prospective student up for success within an entry-level position in the industry after graduating with a degree in cybersecurity (ABET approves accreditation criteria for Undergraduate Cybersecurity programs, 2018).

The most important aspect of these knowledge, skills, and tasks (competencies) is that there are so many of them it can be difficult to make sure each is adequately covered within a four-year cybersecurity program. For this, a comparison would need to be made to ensure all are being covered and if not, to identify any gaps that may exist that need to be addressed. By identifying if there are gaps, what is missing can be isolated and it can be easier to target how to fit those competency(s) into an already existing curriculum.

1.2 Problem Statement and Significance

Over the past several years, companies in the IT industry have expressed their concern over the lack of knowledge their newer employees seem to be experiencing while having graduated from four-year cybersecurity programs. This study aims to explore whether there are any gaps in the cybersecurity knowledge, skills, and tasks (aka competencies) that graduates from ABET-accredited four-year bachelor's cybersecurity-IT programs (degrees and majors) have. For the purposes of this research study, competencies helped determine what the competencies were, and this study will take place at the competency level. Similar studies have been done in other states about industry needs requirements for what they are looking for in new hires from students with cybersecurity and similar technical degrees from four-year institutions, but none have taken place in more rural areas such as the Midwest into account (California, 2018). The contribution of this study will be to find any deficiencies in the ABET-accredited four-year programs curriculum that can be adjusted to better fit the needs of companies while still maintaining the necessary ABET requirements. Current literature suggests that some cybersecurity curriculums derive from both the National Institute of Standards and Technology (NIST) and the National Initiative for Cyber Education (NICE) or to be substituted with certifications as a replacement or substitution for a degree (Morgan State University, 2021). Cybersecurity is still a relatively new field, which indicates that the industry has not had ample time to deep dive into the most important aspects a general professional should be familiar with before deciding what discipline in the field to move towards.

In this study, the goal is to understand if students are lacking the Cybersecurity competencies that the industry is looking for after graduating from four-year programs prior to entering the cybersecurity industry. Follow-up questions that arise based on that goal are what cybersecurity knowledge, skills, and tasks (competencies) are missing from current curriculums and how ABET programs might modify their curriculum to ensure all competencies are being taught?

1.3 Research Question

The current study will include the following research question:

Are there gaps in terms of workforce development for cybersecurity competencies that graduates from ABET-accredited four-year bachelor’s cybersecurity -IT programs (Degrees and Majors) have?

1.4 Hypothesis

A gap exists between the industry level competencies expectations for recent graduates from ABET-accredited four-year cybersecurity programs and what is being taught in the curriculum for these same ABET-accredited four-year cybersecurity programs.

1.5 Assumptions

The assumptions of this study include:

- Four-year undergraduate Majors and Degrees are comparable
- Curricular materials provided were accurate
- The industry survey will be valid for use as a baseline for desired competencies
- The data set will be generated from collected responses for the survey
- There will be enough data to show a statistically significant result
- Data sets will be accurate and complete

1.6 Limitations

- All respondents will accurately reflect their company’s standards and desires
- All respondents will be over 18 years old
- Based in the US, no other countries
- Convenience sample
- Restricted to Purdue’s cybersecurity mapping
- Only looking at ABET-accredited cybersecurity IT programs, NOT computer science or engineering ABET cybersecurity programs

1.7 Delimitations

- ABET-accredited four-year undergraduate cybersecurity programs.
- Using the NIST/NICE framework for this study.
- Four-year programs with cybersecurity majors or degrees are being assessed.

1.8 Summary

In this chapter, an overview has been provided describing the background, problem statement, significance, research question, hypothesis, assumptions, limitations, and delimitations. The main purpose of this study is to provide insight and understand if students are lacking the Cybersecurity competencies that the industry is looking for after graduating from four-year programs prior to entering the cybersecurity industry. This study is focused on understanding the best practice to get students graduating from these types of programs to be prepared for industry-level jobs in this field. This study will consist of a survey that will intend to provide understanding and insight into what skills and knowledge industry-level professionals are looking for in their new hires from these ABET-accredited four-year programs and how universities can ensure their curriculum best helps prepare their students for these types of positions.

2. LITERATURE REVIEW

2.1 Overview

Cybersecurity has become an increasingly popular term within the information technology industry; however, the term has become more of an umbrella with various career paths and specializations that one "cybersecurity" professional is not enough. The companies that are hiring recent graduates from cybersecurity programs and majors are expecting their entry-level employees to have a plethora of knowledge (Western Governors University, 2021). It is becoming more apparent that there is a knowledge gap between what companies deem to be the industry standard and the curriculum being taught within the four-year cybersecurity programs. The aim of this study is to identify any potential gaps in knowledge and skills that entry-level cybersecurity professionals may have after graduating from four-year programs prior to entering the cybersecurity industry. It is imperative for these gaps in knowledge to be identified to alter the standard for what recent graduates should know or the curriculum of these cybersecurity programs. By bridging this gap, it will become easier to see where the current curriculum is falling short of teaching students what the current industry standard frameworks are (National Cybersecurity Workforce Framework, n.d.). The information technology industry is changing so rapidly compared to other fields, which can make it challenging for a university curriculum to keep up with what new programs, technologies, and software is the most current or preferred within the industry (Rainie & Anderson, 2020). This paper will focus on the curriculum of four-year cybersecurity programs and how they compare to industry standards, potential knowledge gaps, industry needs lack of focus for cybersecurity and the use of certifications as additions or substitutions for cybersecurity degrees.

This literature review covers a wide scope of sources mostly from the industry and academia standpoint for cybersecurity-related needs. There are several intertwining aspects for the field of cybersecurity. There is no one solid definition formed for what all encompasses cybersecurity, it can be described as "the organization and collection of recourses, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign jedur from de facto property rights" (Craigen, et al., 2014). The current literature states there is no way to measure the knowledge gaps between recent graduates from four-year cybersecurity programs and industry standards (California, 2018). This study aims to bridge that gap by surveying the companies from the past 10 years that have hired students from our computer and information technology/cybersecurity major we can work directly with the industry to see where the curriculum is lacking. The absence of a solution will cause a disconnect between academia and industry, meaning that students will be unprepared and have difficulties finding suitable jobs. A study completed in California was able to identify three major hiring issues across nine roles: “lack of qualified candidates in general, lack of relevant work experience, and lack of required technology skills” (California, 2018). Since there is no current standard for what curriculum future cybersecurity professionals are being taught, the study will use Purdue’s Computer and Information Technology (CIT) undergraduate cybersecurity major’s curriculum, which is ABET-accredited to measure student preparedness for industry jobs. These courses can include basic computer courses and then get into more specialized fields such as digital forensics, incident response, and penetration testing.

There has been a dramatic increase in the number of cyber-attacks that target governments, organizations, and users over the past several years, with a particular uptick in COVID-related targeted attacks (Jeffery & Ramachandran, 2021). This is becoming especially problematic with “BYOD” or bring your own device and work from home capabilities. Some believe that there are three potential approaches to covering as much of the umbrella term of cybersecurity in a curriculum can boil down to educational, industry, and homeland security (Mouheb et al., 2019). Some cybersecurity curriculums derive from the NIST (National Institute of Standards and Technology) and NICE (National Initiative for Cybersecurity Education) frameworks (Morgan State University, 2021). These are the industry standard frameworks that about 30 percent of US organizations use currently and that number is expected to rise in the years to come. There is also the “importance of developing critical thinking and problem-solving skills in addition to technical skill since these competencies are important to assess risk, detect an emergent threat, respond to attacks, and identify potential adversaries” (Mouheb et al., 2019). There is a constant need in cyber industries to require employees to be able to communicate cybersecurity knowledge and concepts to both a technical and non-technical audience. Being able to communicate with a non-professional is one of the most basic interview questions in this field and it is not something that is typically taught in a classroom setting. "Most cybersecurity experts will concur that the greatest challenge to effective security is the weakness in human behavior in compromising the technical approach, and not the strength of a technical solution" (Patterson, et al., 2016). However, future cyber professionals need to be able to understand ethical and moral issues related to this field and how to draw those lines and boundaries when they are not clearly outlined (Macnish & Ham, 2020).

2.2 Standards for Cybersecurity Education

2.2.1 NIST

This study uses the National Initiative for Cybersecurity Education (NICE) framework to map the knowledge, skills, and tasks (competencies) taught in Purdue University's Computer and Information Technology Bachelor of Science in Cybersecurity curriculum. NICE is led by the National Institute of Standards and Technology (NIST) that provides a partnership between government, academia, and the private sector. The goal of NICE is to provide cybersecurity education, training, and workforce development for those in the cybersecurity industry. IT also supports those who are already in and those who are trying to enter the field of cybersecurity. The NICE framework has the purpose of "improving communication needed to identify, recruit, and develop cybersecurity talent" (Petersen, et al., n.d.). The NICE framework also aims to use a "more consistent, comparable, and repeatable approach to select and specify cybersecurity roles for positions within organizations" (Petersen, et al., n.d.).

Using this framework can also help educators develop curriculums, courses, or degree programs that cover the knowledge, skills, and tasks (competencies) described within the framework (Petersen, et al., n.d.). These knowledge, skills, and tasks (competencies) are described as "attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training" (Petersen, et al., n.d.). The framework described knowledge as a body of information applied directly to the performance of a function. Skill is described for cybersecurity in this context as the application of tools, frameworks, processes, and controls that can impact the cybersecurity needs of an organization or individual. Tasks are defined in the framework as a specific piece of work that combined with another task creates the work in a specialty area or work role.

2.2.2 ABET and CAC

ABET accreditation "provides assurance that a college or university program meets the quality standards for the profession for which that program prepares graduates" (ABET approves accreditation criteria for Undergraduate Cybersecurity programs, 2018). More academic institutions were creating undergraduate cybersecurity programs, the Computing Accreditation Commission (CAC) of ABET noted that cybersecurity needed to be recognized as a formal academic discipline. ABET accreditation was both proposed and created due to prior work such as the NICE Cybersecurity Workforce Framework. Since ABET has released a proposed accreditation criteria for engineering programs, the program criteria for cybersecurity will complement existing ABET criteria for engineering programs and "focus on fundamental knowledge and principles of cybersecurity cast into engineering discipline" (*ABET seeks feedback on proposed accreditation criteria for Cybersecurity Engineering Academic programs*, 2017).

Cybersecurity programs would seek accreditation under the CAC general criteria, which applies to all programs accredited by an ABET commission, while program criteria are discipline specific. Cybersecurity programs must satisfy all general program criteria, the CAC also has specific criteria for disciplines such as information technology (ABET approves accreditation criteria for Undergraduate Cybersecurity programs, 2018). Cybersecurity programs looking to seek accreditation would need to go under an 18-month process which required newly accredited programs to submit requests for evaluation (ABET approves accreditation criteria for Undergraduate Cybersecurity programs, 2018). Specifically for cybersecurity and similarly named computing programs, graduates of the program will need to meet the student outcomes. Student outcomes in this context describe what students are expected to know and be able to do by the time of graduation (Criteria for Accrediting Computer Programs, n.d.). These relate back to the knowledge, skills, and tasks (competencies) that students will gain as they progress through their undergraduate cybersecurity program. The student outcomes specific for cybersecurity and similarly named computing programs must have the following criteria met:

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
6. Apply security principles and practices to maintain operations in the presence of risks and threats. [CY]

List above from: (Criteria for Accrediting Computer Programs, n.d.)

Obtaining ABET accreditation means students and employers can be confident that the undergraduate cybersecurity program at a university is preparing their graduates for success in the workforce for their given industry.

2.2.3 NICE

The NICE Framework has both higher and more in-depth levels of competency mapping such as category, specialty area, work role, competency grouping, and KSA. Now, while this study focuses on competencies, it is understood that ABET based student outcomes do not directly correlate one-to-one to the NICE KSA's. ABET based student outcomes and learning objectives are more of an academic focus and NICE focuses on knowledge, skills, and tasks combined into competencies for the cybersecurity industry. Using the NICE framework KST's at the competency level can be used to map to back to ABET's cybersecurity student outcomes. The reasoning behind using these 38 competencies is that this level of depth works as a translation table for industry requirements for job postings in this field. These are the types of requirements and preferences that will be listed for jobs in the cybersecurity field that are most easily mapped back to the NICE Framework. The competencies, listed in Phase 3 of the Methodology section, are able to be linked back to the competencies for each competency which is what would be considered a learning outcome or course objective in an ABET-accredited four-year cybersecurity program. This is why competencies are the right level of depth to be analyzed for the purpose of this study. Below is a table listing an example of how these competencies translate to the KST's.

Table 1: Competencies to KST's

Competency	KST's
Business Continuity	This area contains KSAs that relate to the planning and preparation of a company to make sure it overcomes serious incidents or disasters and resumes its normal operations within a reasonably short period
Client Relationship Management	This area contains KSAs that relate to the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative).
Collection Operations	This area contains KSAs that relate to executing collection using appropriate strategies and within the priorities established through the collection management process
Computer Forensics	This area contains KSAs that relate to the tools and techniques used in data recovery and preservation of electronic evidence.
Computer Network Defense	This area contains KSAs that relate to the defensive measures to detect, respond, and protect information, information systems, and networks from threats.
Critical Thinking	This area contains KSAs that relate to the objective analysis of facts to form a judgment
Data Analysis	This area contains KSAs that relate to collecting, synthesizing, and/or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence
Data Management	This area contains KSAs that relate to the development and execution of data management plans, programs, practices, processes, architectures, and tools that manage, control, protect, deliver, archive, dispose of, and enhance the value of data and information assets.
Data Privacy and Protection	This area contains KSAs that relate to the relationship between the collection, storage and dissemination of data while simultaneously protecting individuals' privacy.
Database Administration	This area contains KSAs that relate to managing and maintaining database management systems (DBMS) software
Database Management Systems	This area contains KSAs that relate to the use of database management systems and software to control the organization, storage, retrieval, security, and integrity of data.

Table 1: Competencies to KST’s Continued

External Awareness	This area contains KSAs that relate to identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization
Identity Management	This area contains KSAs that relate to the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons"
Information Assurance	This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
Information Management	This area contains KSAs that relate to where or how to gather, organize, maintain, or modify information or information management systems to effectively process, store, and/or distribute information
Information Systems/Network Security	This area contains KSAs that relate to the methods, tools, and procedures, including development of information security plans to prevent information systems vulnerabilities and to provide or restore security of information systems and network services.
Information Technology Assessment	This area contains KSAs that relate to the principles, methods, and tools (for example, surveys, system performance measures) to assess the effectiveness and practicality of information technology systems.
Interpersonal Skills	This area contains KSAs that relate to developing and maintaining effective relationships with others; relating well to people from varied backgrounds and different situations. Considering and responding appropriately to the needs, feelings, and capabilities of subordinates, peers, and seniors.
Legal, Government, and Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Mathematical Reasoning	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Operations Support	This area contains KSAs that relate to the policies and procedures to ensure production or delivery of products and services, including tools and mechanisms for distributing new or enhanced hardware and software.
Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth
Organizational Awareness	This area contains KSAs that relate to understanding an organization’s mission and functions, its social and political structure and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization.

Table 1: Competencies to KST's Continued

Policy Management	This area contains KSAs that relate to the process of creating, communicating, and maintaining policies and procedures within an organization
Presenting Effectively	This area contains KSAs that relate to the activity in which someone shows, describes, or explains something to an audience.
Problem Solving	This area contains KSAs that relate to determining the accuracy and relevance of information and using sound judgment to generate and evaluate alternatives; making well-informed, objective decisions that take into account facts, goals, constraints, and risks while perceiving the impact and implications of decisions.
Project Management	This area contains KSAs that relate to the principles, methods, or tools for developing, scheduling, coordinating, and managing projects and resources, including monitoring, and inspecting costs, work, and contractor performance.
Risk Management	This area contains KSAs that relate to the methods and tools used for risk assessment and mitigation of risk.
Strategic Planning	This area contains KSAs that relate to formulating effective strategies consistent with the objective, vision, and competitive strategy of the organization and/or business unit.
Systems Testing and Evaluation	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.
Target Development	This area contains KSAs that relate to the systematic examination of potential target systems, their components and the elements which make up each component in order to determine the importance, priority, weight of effort, and appropriate weapons selection for specific target systems.
Teaching Others	This area contains KSAs that relate to imparting knowledge of or giving information about or instruction in (a subject or skill)
Technology Awareness	This area contains KSAs that relate to keeping up-to-date on technological developments and making effective use of technology to achieve results
Third-Party Oversight/Acquisition Management	This area contains KSAs that relate to the process of analyzing and controlling risks presented to your company, data, operations, and finances by parties other than your own company.
Threat Analysis	This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks.

Table 1: Competencies to KST's Continued

Vulnerabilities Assessment	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.
Web Technology	This area contains KSAs that relate to the principles and methods of web technologies, tools, and delivery systems, including web security, privacy policy practices, and user interface issues as they apply to development.
Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.

There are other standards that were ultimately decided against being used for this study such as ABET CAC and CSEC 2017 (Cybersecurity Curricula, 2017). It was decided to not use the CSEC 2017 model framework or ABET CAC because it is primarily focused on computer science and not information technology (IT) focused. CSEC 2017 framework also focused heavily on cryptography and discreet mathematics. The reasoning for not using ABET CAC Engineering and CS is that the ABET competencies are slightly different across the different ABET programs and NICE.

2.3 Certifications

The biggest issue is that current curricula do not match the industry's needs (Leaser, 2019). There are numerous aspects to consider but how can we differentiate which ones are the most important to cover? There may be skeptics that say even a four-year generalized cybersecurity program is not enough to prepare for an industry job (Leaser, 2019). Currently, industry lacks a way to be able to test a student's knowledge. The only basis is a potential degree in a direct or related field and the way they answer interview questions. It has been noted that students tend to lack focus on ethical hacking courses. A study done at Bournemouth University showed that after the authors reviewed the design of current coursework, they found that students are more engaged in technical skills but are not engaged with the underlying practices (Faily, n.d.). The authors then redesigned the course to incorporate more real-life scenarios for students to demonstrate the cybersecurity practices and principles they had learned. This was proven to have a more constructive outcome and required the revision of some learning outcomes (Faily, n.d.). With Purdue's Computer and

Information Technology major in cybersecurity program, like other programs, run into the same issue that there is a lack of faculty for teaching security, scarcity of effective teaching resources, and insufficient room in a general computer security curriculum to accommodate every aspect of security. Most universities look at security as a disciplinary for a computer focus when security is more of a multidisciplinary field. Therefore, universities are running into challenges when trying to keep up with the industry standard (Lewis, 2019).

Cybersecurity programs can initially plan their curriculum around the NIST and NICE frameworks but from the industry standpoint, ongoing learning and education is crucial (Rashotte, 2020). These professionals can bolster their current knowledge on a topic or even go on another disciplinary path by obtaining professional cybersecurity certifications. Companies like the EC-Council, CompTIA, ICS2 provide certifications that are comparable with degrees. CompTIA also offers specific pathways for becoming a professional such as the cybersecurity pathway. Certifications such as CompTIA A+, CompTIA Network+, CompTIA Security+, CompTIA Cybersecurity Analyst (CySA+), CompTIA PenTest+ and CompTIA Advanced Security Practitioner (CASP+), the CompTIA Cybersecurity Career Pathway helps technical specialists achieve cybersecurity proficiency, from beginning to end (CompTIA Career Pathway, n.d.). Each of these certifications can help relate back to the KST competencies such as the Pentest+ can assist with threat analysis and vulnerability assessment, the Security+ can assist with information systems and network security and information technology assessments, and Network+ can be mapped back to understanding of information systems/network security and risk management and threat analysis. This is the common way to show any kind of proficiency in a cybersecurity discipline. Preferences for jobs will go to candidates with both degrees and certifications, so many argue that it is within a candidate's best interest to pursue a professional certification regardless (McGill and Dixon, 2005; Rob, 2014; Wireschen and Zhang, 2010). "Academics should encourage students to pursue certification. There are hundreds of cybersecurity-related certifications and navigating through a confusing array can be a daunting challenge" (Wright, 2015). Knapp (2017) states that if these certifications are so valuable then it would be important to prepare students for certification exams by incorporating the certification objectives into the overall program curriculum. CompTIA did a study in 2015 and concluded there are five major reasons why employers look for IT certifications: they help employers fill positions, most companies have

IT staff that hold certifications, those with certifications make great employees, IT certifications are growing in importance, and training alone is not enough (HR perceptions of it training and certification, n.d.) These certifications are not meant to replace experience or education however they seem to meet the mark when university curriculums do not.

2.4 Specialization/Focus

It can be challenging to incorporate industry needs into a university curriculum because they change so rapidly. However, there has been little to no change in the feedback received from companies hiring students. Companies are having difficulties finding suitable personnel to fill a cybersecurity role because they are unsure of what they are looking for in a cybersecurity professional (Rayome, 2017). The cybersecurity industry lacks one focus or any specialization. These companies are looking at cybersecurity as a catchall when it is more multidisciplinary. Hiring agencies for these companies make it clear they want someone who specializes in all areas instead of just one. Training employees becomes expensive but this industry “needs trained technicians capable to identify potential cybersecurity threats and are able to respond adequately when an attack is identified” (Karampidis, et al., 2019). That need is an ideal that would need several professionals from multiple disciplines not a requirement for a single individual. Therefore, many graduates have difficulties finding employment after graduating from four-year cybersecurity programs (Knutson, 2020).

Like most cybersecurity programs, Purdue’s Computer and Information Technology Bachelor of Science degree in Cybersecurity/Information Technology follows ABET (Accreditation Board for Engineering and Technology) standards which indicate the university models its curriculum around the foundational skills of information security. Conklin (2014) states that the biggest gap between industry and academia is the lack of sufficient hands-on skill sets that prepare them for the workforce. The cybersecurity industry heavily expects their workers to be able to work on their equipment and be an immediate asset to strengthen their company. It is expected that new workers can easily adapt to the changing environment, which poses challenges when students have limited resources in their education curriculum (Knutson, 2020). Students learning minimal programming languages, software, and tools in their cybersecurity degree program can run into issues where those same tools and software may not be best practice or even used at all by the time they are applying for jobs. This is discouraging for those who are pursuing a degree or even higher education in a cybersecurity field since students are trained and familiar with tools and applications that the industry no longer uses. Aufman and Wang (2019) state that graduate schools in the US are facing the challenge and opportunity to meet the demand of producing qualified workers for the cybersecurity industry. There will potentially be an "estimated shortfall of 1.8 million workers by the year 2022 and the global cybersecurity workforce needs are acute, broad, and growing" (Burley, 2019). To resolve this potential shortage, employers need to collaborate with academic institutions to develop better cybersecurity programs that will create better, more knowledgeable industry workers. Leaving these positions unfilled will "complicate the securing the nation's networks and may leave the US ill-prepared to carry out conflict in cyberspace" (Libicki, et al., 2014)

2.5 Adequate Preparedness

Cybersecurity educational programs in four-year institutions still fall short of the standard set by the industry as more specializations arise (Lewis, 2019). The NICE Cybersecurity Workforce Framework identifies 38 competencies, 33 specialty areas, and seven categories for jobs in cybersecurity fields. Bicak (et al. 2015) notes that both training and education are crucial to developing a cybersecurity knowledge base. More than half of the NICE specialty areas involve nontechnical or nonprogramming tasks. Education is shifting to focus on "educating students from both technical and nontechnical backgrounds" this addresses interdisciplinary training to diversify the new age workforce (Chang, et al., 2020). By diversifying the workforce through interdisciplinary areas of the cybersecurity field it can assist in bridging the gap between the current knowledge and the industry standards. Recent studies also show that globally employers found that 82 percent reported a shortage of cybersecurity skills and 71 percent believe the knowledge gap could hurt their company overall (Crumpler & Lewis 2020). A potential reason there is such a big gap in knowledge and expectation is due to the lack of a standard definition of what cybersecurity is and means.

There are several definitions for cybersecurity, most of them "highly variable, context-bound, subjective, and uninformative" (Craigen, et al., 2014) However, there needs to be an industry-standard definition of cybersecurity that all companies adhere to. This will allow for easier identification in the areas that are missing but necessary, which will lead to curriculum adjustments. To find where current students are lacking in specific areas, surveying the companies that hire those students will aid in where the industry needs workers to excel the most. Similar studies also compare to the NIST/NICE frameworks from small four-year liberal arts undergraduate cybersecurity programs (Hoag, 2013) over the course of several years, graduate cybersecurity programs (Bicak, et al., 2015), and iSchools or information schools (Chang, et al., 2020).

This study will gather information and data about what competencies are missing directly from the companies that hire students from Purdue University and other ABET-accredited institutions with cybersecurity programs and majors, which will vary from previous studies. Purdue is one of the top-ranked schools for cybersecurity in the US, having this data will be able to identify the knowledge gap for students from one of the best universities in the country (2022 Best Undergraduate Cybersecurity Programs, n.d.). Using information and responses directly from companies that hire Purdue University graduates from the four-year cybersecurity program will aid in finding out where the current curriculum falls short of industry expectations. That way both industry partners and a cybersecurity curriculum can work directly together to ensure all needs are being met to minimize any knowledge gaps any entry-level worker might have.

Recent cybersecurity program graduates are not the only industry professionals lacking soft skills, a panelist at the 2021 RSA conference examined key findings from ISACA’s 2021 State of Cybersecurity that reports “56% of more than 3,600 surveyed security professionals identified soft skills – including communication, flexibility and leadership – as one of the biggest skills gaps among today’s cyber pros, up by four percentage points from last year” (Zurier, 2021) (State of Cybersecurity, 2021). Entry level professionals also tend to lack prior practical experience as well as a solid understanding of computing and information security fundamentals. This means many workers need extensive training prior to beginning their jobs. According to Shoemaker’s (et al. 2020) The Cybersecurity Body of Knowledge aids faculty members, administrators, CISOs, policy makers, and stakeholders involved in the cybersecurity workforce initiatives to understand computing foundational skills and essential knowledge. By combining all those aspects from education to industry, gaps can both be more easily identified then filled. Thames and Schafer (2017) also indicate how cybersecurity has an impact on the industry and how to address technological foundations of cybersecurity within a given scope.

Current research shows that cybersecurity curricula do not meet industry standards (Lewis, 2019). It can be difficult to identify where those knowledge gaps are without directly communicating with the companies that are hiring students as "cybersecurity professionals." Accommodations to make up for these gaps can be filled with short intensive courses or certifications from industry approved companies such as CompTIA or EC-Council.

This study aimed to bridge that gap and find if there are knowledge gaps for four-year cybersecurity programs are from the current ABET-accredited cybersecurity curriculums. It will also survey companies who have directly hired graduates from the cybersecurity program directly asking questions related to what knowledge and skill set their entry-level people have. The survey will also ask what skills and knowledge they are looking for in their entry level people. The data taken from this survey will be compared to the learning objectives taught in Purdue University's ABET-accredited current cybersecurity curriculum and see where amendments and adjustments need to be made to better prepare graduates from other ABET-accredited institutions. Considering most cybersecurity programs need to be ABET-accredited and align with the NIST/NICE frameworks set for industry standards, this will be easy to identify where the current curriculum is falling short. The survey will focus on identifying what companies are expecting of graduates from these programs and what competencies they have. By comparing these qualifications to their job description and requirements for cybersecurity-related positions, the study will identify if any gaps exist. If gaps are identified, this information can be used to improve or modify the curriculum.

3. METHODOLOGY

3.1 Research Questions

This study included the following research question to be answered: Are there gaps in terms of workforce development for cybersecurity competencies that graduates from ABET-accredited four-year bachelor's cybersecurity -IT programs (Degrees and Majors) have? The research question helped formulate the hypothesis that needed to be tested in order to perform this study.

3.2 Hypothesis

This study aims to both understand and provide insight on whether students are lacking the Cybersecurity competencies that the industry is looking for after graduation from four-year programs prior to entering the cybersecurity industry. The research question being explored is: are there gaps in terms of workforce development for cybersecurity competencies that graduates from ABET-accredited four-year bachelor's cybersecurity-IT programs (Degrees and Majors) have?

Based on the literature review, no similar studies found a connection between university curriculums that follow NIST/NICE frameworks that also meet industry standards for entry-level positions. Since there are no similar studies on this topic, this is an exploratory study. Due to the lack of previous knowledge and experience in this area, the hypothesis for this study aimed to answer the research question of "Are there gaps in terms of workforce development for cybersecurity competencies that graduates from ABET-accredited four-year bachelor's cybersecurity -IT programs (Degrees and Majors) have?":

> *A gap exists between the industry-level expectations for recent graduates from ABET-accredited four-year cybersecurity programs and what is being taught in the curriculum for these same ABET-accredited four-year cybersecurity programs.*

3.3 Gap Analysis

3.3.1 Syllabi

For this gap analysis the 38 competencies identified were taken from the undergraduate upper-level cybersecurity specific courses listed for Purdue University's four-year undergraduate cybersecurity degree (Table 2). Purdue University ranks in one of the top 10 undergraduate cybersecurity programs in the country which is why it was chosen for this study as well as the author completed all the requirements and graduated from this undergraduate cybersecurity program in 2020 (2022 Best Undergraduate Cybersecurity Programs, n.d.). What can be found from an analysis of this program should be generalizable to other ABET-accredited four-year undergraduate cybersecurity courses. Twenty-one courses had the syllabus and learning objectives analyzed in order to identify which competencies were being taught within that course. These competencies were taken from the NICE framework. Using this framework was due to its familiarity within the cybersecurity industry. It is a framework which is more of an outlined suggestions of topics that should be covered in an education or academic setting. The competencies were the most comprehensive level to do the analysis for this study on as they were both specific enough to identify within this four-year undergraduate cybersecurity program but also general enough to make assumptions that could be applied to other ABET accredited four-year undergraduate cybersecurity programs.

Table 2: Purdue University Undergraduate Upper-Level Cybersecurity Courses Analyzed

Course #	Course Title	Year
CNIT 320	Policy, Regulation, and Globalization in Information Technology	Junior
CNIT 322	Research Methodology and Design	Junior
CNIT 422	Cyber Criminology	Senior
CNIT 581	Social Engineering	Senior

3.3.2 Curriculum

There are twenty-one cybersecurity courses in the undergraduate four-year cybersecurity program at Purdue University. Each of these courses (Table 2) is required in order to obtain the baccalaureate degree for this program at this university. This curriculum was chosen as it was familiar to the author as they completed the program prior to this study. This curriculum was also the most accessible to the author to view each of course syllabi in order to assess and examine the learning objectives and competencies taught within this university program.

3.3.3 Verification with Faculty

After each course's competencies were identified, they were then compared to the list of NICE framework competencies. There are sixty nice competencies and thirty-eight of them are currently being taught in Purdue University's four-year undergraduate cybersecurity degree. Fourteen competencies remain that are not being covered in cybersecurity specific courses. A confirmation email was sent out to the associate Computer and Information Technology department heads to ensure that the fourteen competencies are not being covered in any of the undergraduate cybersecurity programs. This ensured nothing was missed during the previous analysis of the syllabi and curriculum for each of the undergraduate cybersecurity courses. The faculty then confirmed that these are not currently covered in any courses. With confirmation that fourteen competencies are not being taught it allows for a gap analysis to be done to see if these missing competencies cause students to be at a deficit upon graduation from this four-year cybersecurity program.

3.4 Survey

3.4.1 Survey Design

The survey for this study consists of a 25-question online questionnaire (see Appendix). This survey has received IRB approval (IRB-2019-314). The survey design entails a combination of different response methods such as closed and open-ended questions. The design of the questions is a mixture of single and multi-response questions, as well as some open-ended responses answers. This survey was also adopted from a previously conducted survey within the state of California about their cybersecurity labor market in 2018 and was shown to have good validity due to the tests done on it (California, 2018). It was then modified to fit the needs of this study by adding questions about work roles and competencies

The first set of questions consists of eight questions dealing with industry demographics such as if the company employs cybersecurity/information technology/information systems workers who require some level of cybersecurity skills, if their company hires graduates from university cybersecurity programs, and how many they hire per year. The questionnaire also asked if they plan to hire any cybersecurity and/or IT/IS workers in the next year and if the participant is familiar with the current hiring criteria for these types of employees at their organization. This section also discussed if the participant's company prefers cybersecurity industry certifications for new hires and if so which ones.

The second section of three questions focuses on the work gap which asks whether the participants feel their new hires that come from university cybersecurity programs have adequate knowledge and skills. It is also asked which top 10 knowledge, skills, and tasks competencies do the participants believe are the most preferred for entry-level cybersecurity professionals to have. The final question in this section is an open response asking if the participant has any advice that they would like to provide to university programs to better align the graduates with workforce requirements.

This next section consists of six questions and aims to dive deeper into work role-related questions. For the following set of questions, we ask the participants to try to equate their business or organization's specific position titles with the more general work roles. It asked when the organization or business faces difficulty hiring qualified candidates, how they responded, and to specify which challenges they faced while hiring for these types of cybersecurity/IT/IS positions. The respondents also identify the minimum education requirements and work experience required for qualified candidates. They are also asked to specify the top three soft skills that are the most important for these types of roles and on average if the percentage of time spent on cybersecurity/security issues increased within the past twelve months.

The fourth set of questions has four questions about the industry demographics of the participants responding, in this section no personal or identifying information is asked. The questions in this survey are completely anonymous, although at the end there is a section providing an email address if the participant wishes to be contacted in the future. Since these demographic questions are not necessarily specific to the participant, but the company they work for, demographic questions include inquiries about what industry is the participant's firm most strongly associated with and how is the business/organization involved with cybersecurity. It also asked about how many permanent employees work at the specific location of the respondent including part-time, full-time, and remote as well as how many employees do, they expect to have at their location in the next year, including part-time, full-time, and remote.

The final set of questions is five demographic questions that inquire about the participant's company with regards to their hiring of cybersecurity and information technology or information systems employees. These questions do not personally identify the individual or company that the participant works for. In this block, we asked which state the participant's business or company is located in and to describe the primary functional work area their company falls under. This block asked about how many employees are at the participant's company as well as the company's annual revenue. The block concludes by asking about what percentage of the organizations operating budget is spent on cybersecurity. The survey wraps up with a single open-ended closing question asking about any comments or feedback from the survey.

3.4.2 Sample

For this survey, a convenience sample was used and consisted of individuals who had an affiliation with Purdue University's four-year Computer and Information Technology cybersecurity program either directly through the program or through Purdue's CCO. A list of companies was provided for this study through Purdue's CCO and the department of Computer and Information Technology past career fair participants. To qualify for this study, participants must be over 18 years of age and current United States residents. As this study uses a convenience sample, it has limitations and is not completely random selection of participants, the results could lead to sampling error issues. Another limitation for this sample size is that it does not fully represent the entire population of companies hiring graduates from four-year cybersecurity programs, this group can represent the population enough for an accurate representation for this study's purpose. Additionally, another limitation would be that this study only looked at IT programs and did not include any computer science or engineering cybersecurity programs. The anticipated number of responses is 60 respondents with usable responses to be interpreted for the results. This number is large enough to get an accurate reflection for comparison about what diverse types of companies are looking for in their new hires as well as what knowledge, skills, and tasks (competencies) they require for their new hires.

3.4.3 Procedure

Phase 1:

- Recruitment by email

Phase 2:

- Qualtrics survey sent to participants
- Data Collection

Phase 3:

- Data Exploration - usable
- Data Analysis
- Results

Phase1

This survey was sent out via a recruitment email to potential participants from a list gathered by Purdue University's Center for Career Opportunities (CCO). This list consisted of companies who have hired recent graduates from Purdue Polytechnic's four-year cybersecurity program in the past for entry-level positions at their company. This recruitment email was able to gather potential respondents who are willing to answer a 25-question survey about aspects of their company, the company's relationship to cybersecurity, whether they are hiring any new people for entry-level cybersecurity positions, and what cybersecurity knowledge and skills the respondents might be looking for in a new hire.

Phase 2

This study began with a survey adapted from a labor market analysis study done in California that surveyed similar aspects of cybersecurity from California employers

(California, 2018). This survey was created and distributed through Qualtrics. Qualtrics is a web-based survey creation, collection, and analysis software tool and can be used for the creation of open surveys, targeted (panel) surveys, and open polling (Qualtrics, n.d.). The survey consisted of several types of questions in various blocks to combine alike questions. The survey consisted of 25 questions, with the idea of being fast paced so participants will not become inattentive or exit the survey early. Since the survey was 25 questions long, the goal was to have participants be alert and actively answer every question. As most of the questions have multiple choice answers, the participants were able to move through the survey quickly. This survey was also kept anonymous, meaning that all identifying and personal information will not be collected about the participants responding to this survey. Each participant received an email with an anonymous link to the survey that was provided by Purdue's Center for Career Opportunities who have hired graduates from the Purdue Polytechnic Institute's four-year cybersecurity program in the past or had an affiliation with Purdue's CCO or CIT department. Personal email addresses were unknown as the email will be sent out to a general group distribution list. The survey did not ask any questions that will be able to identify the individual personally who is responding to this survey, nor will the exact company name be asked for.

Phase 3

After the results were gathered, data exploration and analysis were performed on the usable responses from the participants. This survey was looking to bring in about 60 usable responses to analyze to accurately represent the cybersecurity industry, however, only three were able to be analyzed. The analysis was conducted using frequency analysis for the most chosen responses for each question.

A knowledge, skills, and tasks (competencies) mapping had already been completed by the author for Purdue Polytechnic's four-year cybersecurity classes within the cybersecurity major to see how the competencies were being met in each class for the cybersecurity curriculum. This mapping showed the breakdown of the major competencies that are both taught in each cybersecurity class and are needed by each individual student to show proficiency in each area. The first analysis is to compare the mapping previously completed to the NICE competency matrix to determine any gaps or weaknesses in the curricula for Purdue University's CIT four-year cybersecurity program.

The first analysis would be a gap analysis to compare the results of the survey to the mapping previously done in order to see which competencies are lacking or missing completely. This comparison was made to identify the gap that exists between what cybersecurity industry companies are looking for in new hires and the knowledge, skills, and tasks (competencies) that are being taught in ABET-accredited four-year cybersecurity programs. For this study the knowledge, skills, and tasks (competencies) have been mapped to the following 38 competencies:

- Business Continuity
- Client Relationship Management
- Collection Operations
- Computer Forensics
- Computer Network Defense
- Critical Thinking
- Data Analysis
- Data Management
- Data Privacy and Protection
- Database Administration
- Database Management Systems
- External Awareness
- Identity Management
- Information Assurance
- Information Management
- Information Systems/Network Security
- Information Technology Assessment
- Interpersonal Skills
- Legal, Government, and Jurisprudence
- Mathematical Reasoning
- Operations Support

- Oral Communication
- Organizational Awareness
- Policy Management
- Presenting Effectively
- Problem Solving
- Project Management
- Risk Management
- Strategic Planning
- Systems Testing and Evaluation
- Target Development
- Teaching Others
- Technology Awareness
- Third-Party Oversight/Acquisition Management
- Threat Analysis
- Vulnerabilities Assessment
- Web Technology
- Written Communication

3.5 Gap Survey Comparison

3.5.1 Analytical Method

The first part of this study was a gap analysis of the results of the survey to what was already thought to be missing and what cybersecurity industry professionals believe to be missing. The second part of this study was to compare the previously identified competencies from Purdue University's cybersecurity curriculum for the required security course to the NICE competencies. This will aid in identifying what competencies are already thought to be missing from the current curricula. The data from the survey was exported from Qualtrics into a CSV file once the survey has concluded. Once the data has been exported, any missing or incomplete responses will be removed. The results were interpreted using a frequency analysis.

3.6 Summary

This chapter provided an overview of the methodology of this study. The hypothesis, survey design, sample, procedure, and analytical method were both outlined and described in detail. The survey took place via Qualtrics, an online collection tool from Purdue University. It was distributed to participants from an email list of companies who have previously hired graduates from Purdue's CIT cybersecurity program provided by Purdue's CCO or were affiliated with Purdue's CIT department directly. After the responses were collected, a frequency analysis was conducted. Once the results were found, a comparison from the previously identified competencies from Purdue University's cybersecurity curriculum for the required security course will be compared to the list of NICE competencies to identify any gaps or weaknesses in the current curricula.

4. ANALYSIS AND RESULTS

4.1 KST's Competencies Comparison

An analysis from the NICE framework of KST's being mapped to competency level as well as competencies mapped using that framework for all upper-level classes in Purdue University's undergraduate cybersecurity degree was performed in order to assess what knowledge gaps might already exist. The NICE framework identifies 60 different competencies, while Purdue's undergraduate cybersecurity program only teaches 38 of these competencies. This still leaves about 14 competencies that are not being covered by any of the upper-level classes within this program. Now, Purdue's undergraduate cybersecurity program does not need to cover every one of these topics, some may be covered in some lower-level classes, electives, or even classes in other departments. The NICE framework is exactly that, a framework that most aspiring industry professionals should show proficiency in, or at least have some competency in, before entering the workforce. The more competencies that can be taught in the classes offered to these students, the more potential they have for success upon graduation.

Table 3 shows the different competencies that are taught in Purdue University's undergraduate cybersecurity programs that are mapped to the competencies from the NICE framework. These 38 competencies are taught in the upper-level classes that are more focused on cybersecurity. The 38 competencies are also being measured in the gap analysis from the survey conducted. By understanding what is already being taught in this program it will be easier to identify which competencies need to be focused on more or need to be added.

Table 3: Purdue University Undergraduate Cybersecurity Program Competencies

Business Continuity	**Mathematical Reasoning**
Client Relationship Management	**Operations Support**
Collection Operations	**Oral Communication**
Computer Forensics	**Organizational Awareness**
Computer Network Defense	**Policy Management**
Critical Thinking	**Presenting Effectively**
Data Analysis	**Problem Solving**
Data Management	**Project Management**
Data Privacy and Protection	**Risk Management**
Database Administration	**Strategic Planning**

Table 3: Purdue University Undergraduate Cybersecurity Program Competencies Continued

Database Management Systems	**Systems Testing and Evaluation**
External Awareness	**Target Development**
Identity Management	**Teaching Others**
Information Assurance	**Technology Awareness**
Information Management	**Third Party Oversight/Acquisition Management**
Information Systems/Network Security	**Threat Analysis**
Information Technology Assessment	**Vulnerabilities Assessment**
Interpersonal Skills	**Web Technology**
Legal, Government, and Jurisprudence	**Written Communication**

Some of the competencies that might need more coverage or to be added is risk management, incident management, operating systems, knowledge management, and computer forensics. Risk management is glossed over already in various upper-level classes in Purdue's cybersecurity course curriculum however it is something that needs to be addressed in more depth and how risk management looks differently depending on the type of work being done. Incident management is also taught but the class that goes into the most depth of this topic focuses more heavily on writing an incident response recovery plan rather than how to handle different types of incidents as they come up. Operating systems are something that is not covered in more simplistic terms such as the options and differences between them; however, Windows and Linux are mostly utilized in this cybersecurity program. Knowledge management is addressed in such a way that prior understanding is the expectation but not best practices for how to stay up to date, finding, contributing, and documenting knowledge in a way that allows for decision making or sharing purposes. Computer forensics is taught in a singular undergraduate cybersecurity course as well as a graduate elective course and needs to be covered as much as some of the other high-level topics are.

Many of the competencies that could also be labeled as "soft skills" allow for areas for improvement such as interpersonal skills, oral communication, presenting effectively, problem solving, teaching others, and written communication. While these are required and practiced as routine in each class, how to do each of them effectively and efficiently is rarely ever discussed, especially with regard to the cybersecurity industry.

Table 4 shows the 60 competencies from the NICE framework. Thirty-eight of these competencies are being taught currently in the undergraduate cybersecurity program in Purdue University's Computer and Information Technology department in the upper-level cybersecurity courses. The 38 competencies are shown in Table 3, Table 5 also shows which competencies are not currently being taught in the upper-level cybersecurity courses. These 60 competencies are the level that need to be measured at to ensure students are meeting the required learning objectives for ABET standards. Since not all the competencies are currently being taught, it is possible there will be a knowledge gap for students in this program. Even with all of them being taught, it may be difficult to cover 60 competencies effectively and in enough depth within only the upper-level cybersecurity course requirements Purdue University's CIT department has.

Table 4: NICE Framework Competencies

Asset/Inventory Management	**Incident Management**	**Process Control**
Business Continuity	**Information Assurance**	**Project Management**
Client Relationship Management	**Information Management**	**Requirements Analysis**
Collection Operations	**Information Systems/Network Security**	**Risk Management**
Computer Languages	**Infrastructure Design**	**Software Testing and Evaluation**
Computer Forensics	**Information Technology Assessment**	**Software Development**
Computer Network Defense	**Intelligence Analysis**	**Strategic Planning**
Computers and Electronics	**Interpersonal Skills**	**Systems Administration**
Conflict Management	**Knowledge Management**	**Systems Integration**
Contracting/Procurement	**Legal, Government, and Jurisprudence**	**System Testing and Evaluation**
Critical Thinking	**Mathematical Reasoning**	**Target Development**
Data Analysis	**Modeling and Simulation**	**Teaching Others**
Data Management	**Network Management**	**Technology Awareness**
Data Privacy and Protection	**Operating Systems**	**Telecommunications**
Database Administration	**Operations Support**	**Third Party Oversight/Acquisition Management**
Database Management Systems	**Oral Communication**	**Threat Analysis**
Encryption	**Organizational Awareness**	**Vulnerabilities Assessment**
Enterprise Architecture	**Policy Management**	**Web Technology**

Table 4: NICE Framework Competencies Continued

External Awareness	**Presenting Effectively**	**Workforce Management**
Identity Management	**Problem Solving**	**Written Communication**

Table 5 shows the 14 competencies that are not included currently in Purdue University's four-year undergraduate cybersecurity programs. It is important to note these differences because that is where a gap may exist within the current curriculum. While these competencies may be covered in other courses that make up the undergraduate degree at Purdue University, they are not covered in the cybersecurity specific courses, or they would be listed in Table 3. Being taught these competencies in other courses may be beneficial to learn about and understand; however, not understanding how these competencies work from a cybersecurity standpoint may create a knowledge gap for these students.

These competencies listed in Table 5 were sent to faculty in Purdue University's Computer and Information Technology department where the cybersecurity undergraduate degree is listed. The faculty then confirmed that none of these fourteen competencies are currently being covered in any of the courses required for the undergraduate cybersecurity degree in this department. Students may need to take additional courses or elective courses that would cover some of these competencies.

Table 5: Missing Competencies from NICE Framework competencies that are not included in Purdue's undergraduate cybersecurity curriculum

Asset/Inventory Management
Computers and Electronics
Conflict Management
Contracting/Procurement
Intelligence Analysis
Knowledge Management
Modeling and Simulation
Operating Systems
Process Control
Requirements Analysis
Software Development
Software Testing and Evaluation
Systems Integration
Workforce Management

4.2 Results of Survey

4.2.1 Descriptives

This survey included some qualification questions in the "Industry Hiring Questions" section, these questions would eliminate perspective participants from the study if a certain answer was chosen. Some of the questions included if the participant employs any Cybersecurity and/or Information Technology/Information Systems workers who require some level of cybersecurity skills, if the company hires graduates from university cybersecurity programs, and if they are familiar with the current employment numbers, work roles, and hiring criteria for workers in the cybersecurity/IT/IS industry. If the participant answered "No" to any of these questions they would immediately be sent to the end of the survey. If participants had answered "No" to if there are preferences for cybersecurity industry certifications for new hires, they would be sent to the next block of questions inquiring about the workforce gap. Participants who did not meet this criterion would have their responses removed as they were then considered invalid. Other participants did not complete the survey in its entirety, which gave a total of 3 complete responses (N = 8 and n = 3).

When breaking down the demographics of the participants there were two categories, industry demographics about the company the participant was responding to on behalf of and the demographics of the participant. Results for these questions showed an even split between three categories for which primarily describes the respondents functional work area at their company – senior manager, manager, and human resources. All of the respondents are located within the Midwest region, mostly coming from Indiana or Illinois. The respondent's organization or business is involved with cybersecurity as providers

4.2.2 Respondents Industry Demographics

The respondents of this survey had a range of industries within the field of cybersecurity they were most closely associated with. The three industries were mining, health care and social assistance, and information such as (IT, IS, ISP providers, etc.) which can be shown in *Figure 1*. Given that this study surveyed companies that hired students from undergraduate cybersecurity programs; it is important to know which industry the responding companies are from in order to see what skills are most needed within that industry. The respondents were given nineteen different options and if none of those were an accurate representation of the industry that they are related to then they had the option to fill in with a description more representative. The different options for the respondents were the following: mining, construction, agriculture, wholesale trade, retail trade, transportation/warehouses/utilities, information/IS/IT/ISP/etc., finance/insurance, real estate/rental/leasing, professional/scientific/technical services, administrative/support/waste services, educational services, health care and social assistance, arts/entertainment/recreation, accommodation and food services, federal government, state government, local government, and other.

It also goes to show that there is a variety of types of industries within cybersecurity and it is not limited to just technology or IT/IS companies that need the skill sets of recent graduates from undergraduate cybersecurity programs. The importance of identifying which industry respondents is coming from makes it easier to determine if different skill sets and qualifications are preferred for the same types of positions. If they are different, that has the potential to impacts what kinds of classes, courses, and certifications students might be looking to take or improve upon prior to graduation in order to be appropriately qualified for a given industry cybersecurity position.

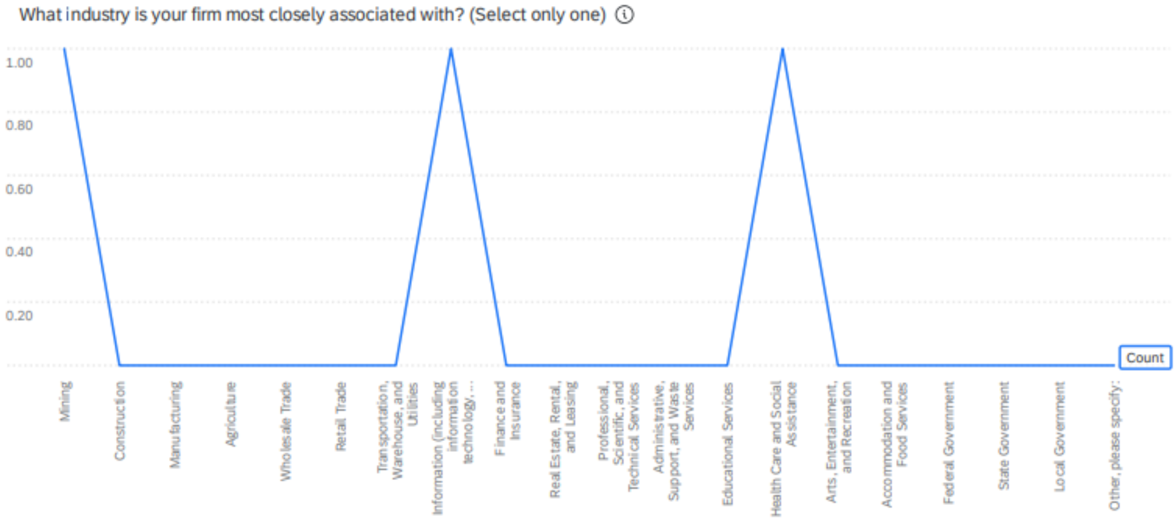

Figure 1: Q16 What industry is your firm most closely associated with? (Select only one)

Respondents were also asked to disclose in what capacity their business or organization is involved with cybersecurity in question seventeen shown in *Figure 2.* There were five options to choose from and respondents were instructed to choose all that apply to their business or organization. The five options included: creator/producer of cybersecurity products, provider of cybersecurity products and/or services, user of cybersecurity products/services, other involvement with cybersecurity, or regulated industry. There were four responses in total for this question, two of which noted they were users of cybersecurity products or services. One responded they were a provider of cybersecurity products or services. The last responded they were a member of regulated industry. It was relevant to include this question to see how the respondents are familiar with or their association with cybersecurity at their business or organization.

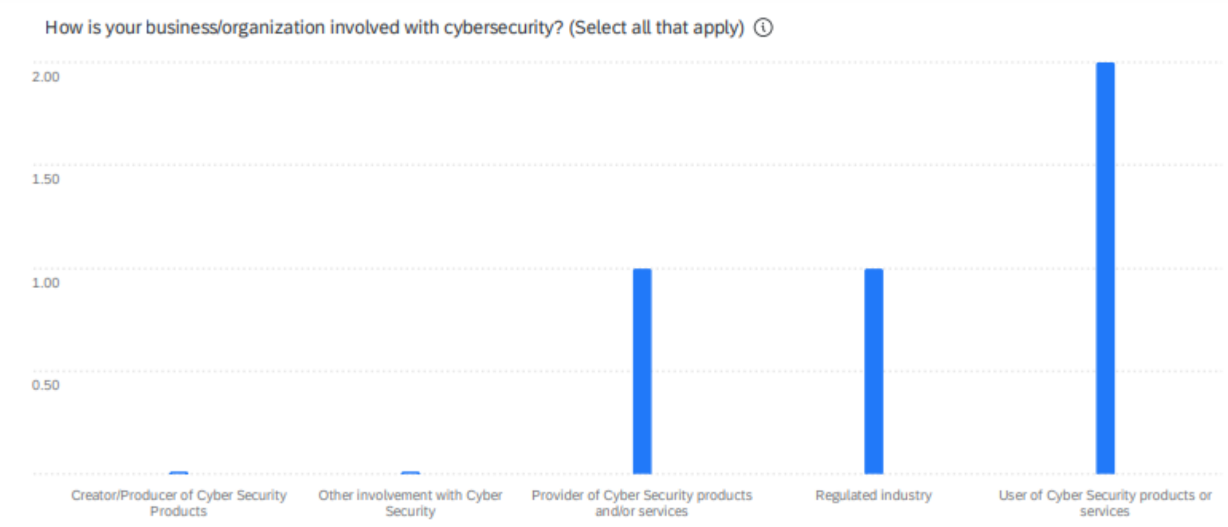

Figure 2: Q17 How is your business/organization involved with cybersecurity? (Select all that apply)

Question eighteen inquired about how many permanent employees there are at the respondent's company location. This included full-time, part-time, and remote workers. Including all these types of workers was the best way to get an accurate estimate of the size of the respondent's company where their location currently resides. Respondents had the option to fill in a textbox listing how many permanent employees their location has. The responses were 120 employees, 1500 employees, and 28,000 employees. This allowed the study to account for small, mid-size, and large branch locations to consider what traits these different types of companies are looking for when hiring new graduates from four-year cybersecurity programs for entry-level positions. How many employees at a given location could also change depending on the HQ and team locations of that company. There might only be one cybersecurity team at the location the respondent came from, or the company might have cybersecurity professionals at multiple locations. The respondents also noted that they mostly expected to hire the same number of employees or more at their given location 12 months from now, including part-time and full-time employees.

A similar question was asked later in the survey *Figure 3* pertaining to how many employees there were in the company overall. The range of answers available to choose from were under ten, ten to fifty, fifty-one to one hundred, one hundred to one thousand, one thousand to five thousand, five thousand to ten thousand, and more than ten thousand. Responses were represented for companies that had one hundred to a thousand employees, one thousand to five thousand employees, and more than ten thousand employees. Two respondents disclosed their company's annual revenue from question 23. One noted their company brings in ten million to fifty million and the other noted they bring in over 100 million annually. It is also important to note that one company disclosed from question 24 that they spend less than ten percent of their organization's operating budget on cybersecurity.

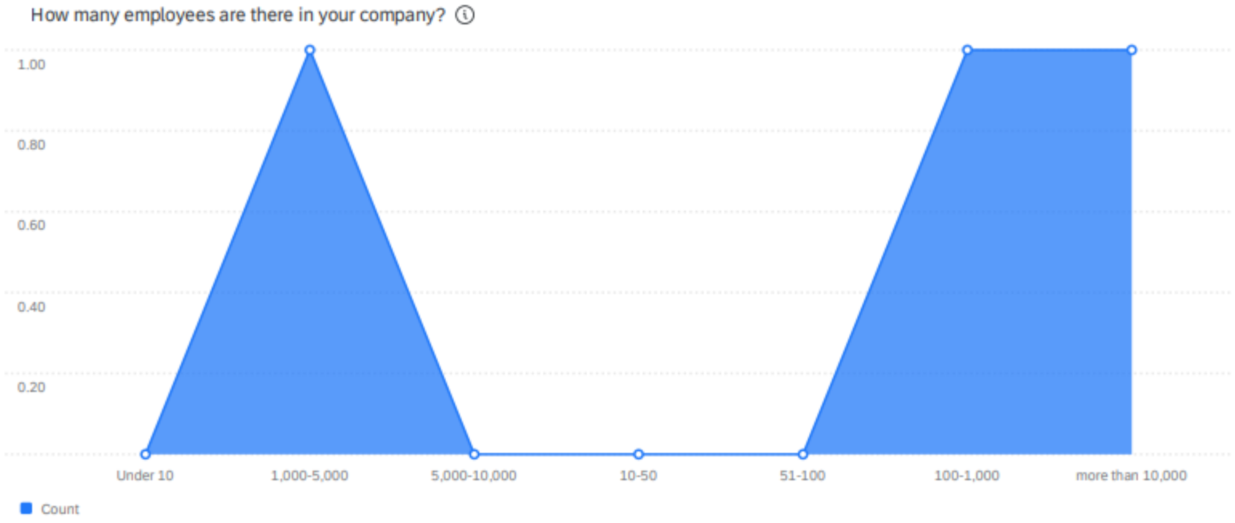

Figure 3: Q22 How many employees are there in your company?

4.2.3 Industry Certification Preferences

Question six of this survey showed about 50 percent of respondents preferred that their new hires for cybersecurity and like positions have cybersecurity industry certifications. The following question, question 7, shows the results for which certifications are preferred amongst the respondents. The survey provided them to choose from a list of nine current industry certifications that many cybersecurity professionals hold. Respondents could choose between the following: CISSP, CCNA, CCNP, CompTIA Pentest+, CompTIA Security+, Ethical Hacker, SANS/GIAC, CISA, CISM, or provide another preferred certification within a text box.

The results of this question were very evenly split as seen by *Figure 4*. Respondents preferred their new hires to have either of the CompTIA certifications, the ethical hacker, the CISCO certifications (CCNS/CCNP), or the CISSP. While it would be ideal for all candidates for a cybersecurity position to have some sort of industry certification, this is not possible for everyone. Some of these certifications require outside preparation course participation, study time, and can even be rather costly. The requirements needed to take some of these certifications may not be feasible or accessible to some. This means it is important to note while these industry certifications are preferred, they should still maintain being a preference rather than shift to a requirement for a given entry-level cybersecurity program.

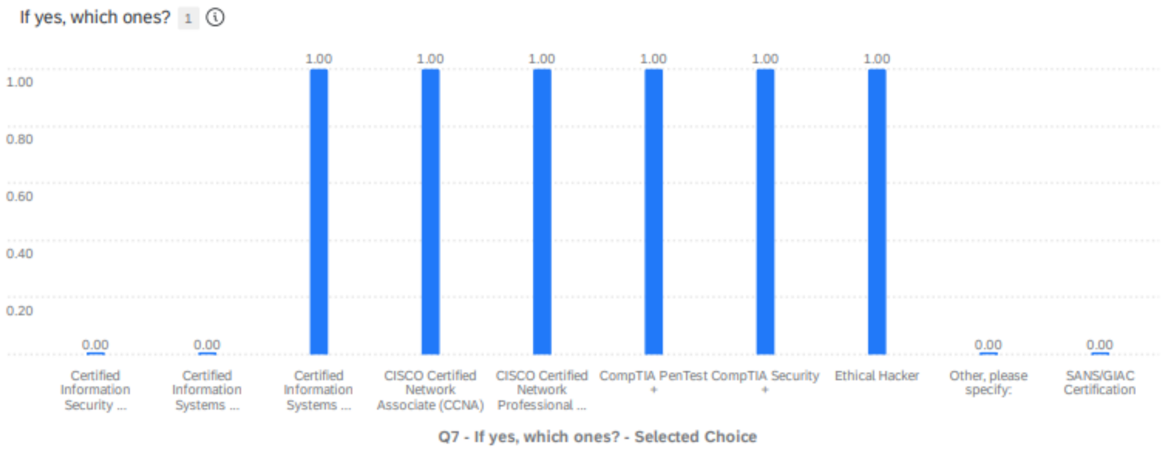

Figure 4: Q7 Which Certifications?

4.2.4 Adequate Preparation from University Cybersecurity Programs

Question eight (*Figure 5*) results dive into whether or not the respondents feel their new hires coming from university cybersecurity programs have adequate cybersecurity related knowledge and skills. Two answered somewhat and one answered yes. This also notes that none of the respondents answered that they felt their new hires did not have adequate cybersecurity knowledge and skills. It might have been beneficial to have included a follow-up question about their proficiency with the skills required or particular skills for an entry-level position at their company. It is the ideal goal of most university programs regardless of the field to ensure their graduates are ready and prepared to enter the workforce. Knowing these results shows that the current structure and focus of the undergraduate cybersecurity program is teaching students the necessary skills to be successful in an entry-level cybersecurity position.

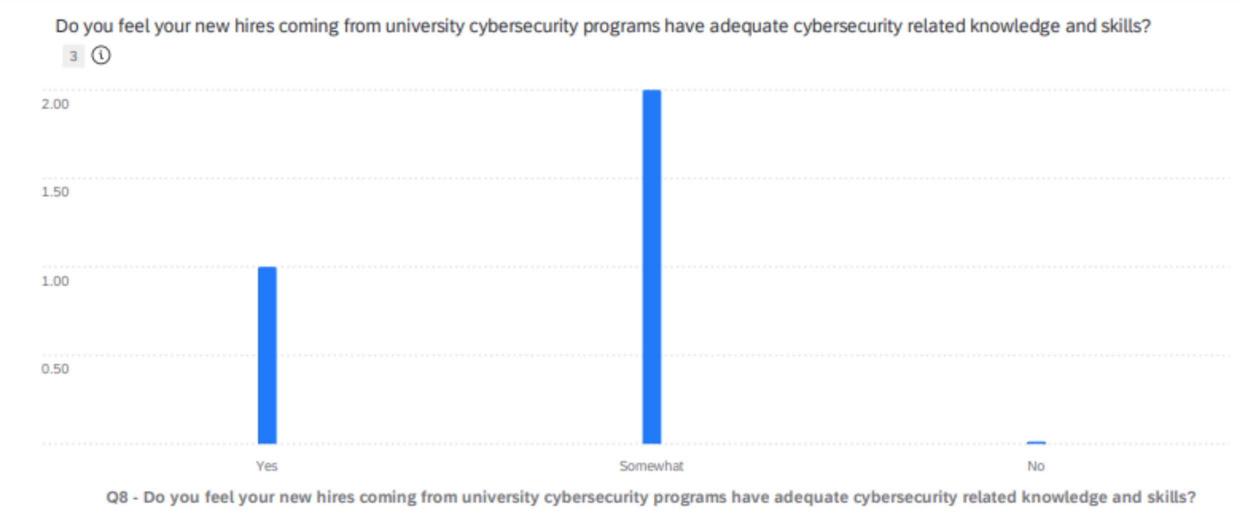

Figure 5: Q8 Do you feel new hires coming from university cybersecurity programs have adequate cybersecurity related knowledge and skills?

4.2.5 Cybersecurity Competencies Industry Preferences

Question nine (*Figure 6*) is perhaps the most important question of the survey. This question explores what the top ten competencies' respondents most preferred an entry-level cybersecurity professional to have. The 38 competencies that are identified as currently being taught in Purdue University's undergraduate cybersecurity program. These competencies can be seen in Table 3. The respondents were instructed to pick their top choices in no particular order as the question allowed for multiple responses. One response was cast for the following competencies: client relationship management, computer forensics, critical thinking, data analysis, database administration, identity management, information technology assessment, interpersonal skills, project management, strategic planning, and written communication. Two responses were recorded for computer network defense, data privacy and protection, information systems/network security, oral communication, problem solving, threat analysis, and vulnerabilities assessment. The highest number of responses for this question was recorded for risk management with three responses.

This question was the most important because it was to confirm the original competencies mapping that was done for the first part of this study. There was speculation about what was already missing or lacking in Purdue University's four-year undergraduate cybersecurity program and the purpose of this survey was to find out what industry companies thought was missing. From there a comparison can be made about what was already thought to be missing or lacking, to what industry believes is missing or lacking and see how the results differ.

One of the suggestions that came from the following question in the survey, question ten, regarded asking respondents for feedback for university programs to better align their graduates with workforce requirements. The suggestion was made to work with major industry companies to have them evaluate the current curriculum in order to see if they align. That is in fact the purpose of this study. By asking the companies which competencies they feel are missing or lacking, it can be easier to see where the knowledge gap is and how an undergraduate cybersecurity program might amend their curriculum to bridge the gap.

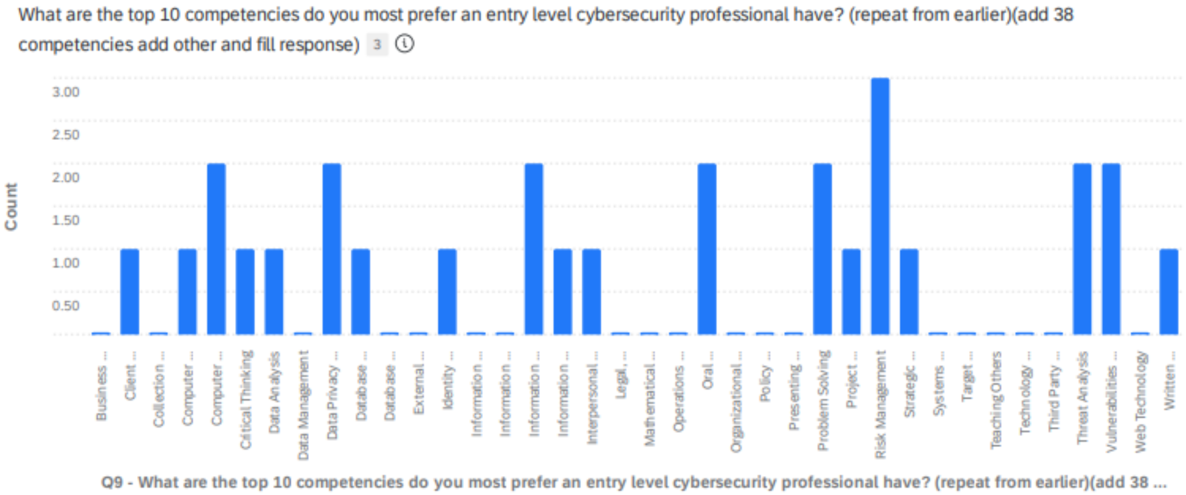

Figure 6: Q9 What are the top 10 competencies do you most prefer an entry level cybersecurity professional to have?

4.2.6 Challenges for Hiring Cybersecurity Professionals

Industry professionals also have their own set of challenges to consider when hiring new candidates for positions. Question eleven shows what challenges or issues the respondent's business or organization face when hiring cybersecurity professionals. *Figure 7* shows which options respondents had to choose from such as lack of relevant work experience, lack of required education, lack required technology skills, lack of qualified candidates in general, lack of qualified candidates with necessary security clearance, and other with an option to fill in something not previously specified. One response was recorded for each of the following options: candidates lack relevant work experience, candidates lack required technology skills, and lack of qualified candidates in general.

Noted from question ten in the survey which was also discussed in section 4.5 asked what advice, if any, would the respondent give to university programs to better align their graduates with workforce requirements. Respondents suggested that student's network as much as possible in order to learn as much as they can. There was also a recommendation that students work on "passion projects" outside of the classroom. The final suggestion was to work with major companies to have them evaluate the academic curriculum. Conveniently, working with major companies to have them evaluate our curriculum is the purpose of the survey and this study. However, while having the exact university cybersecurity curriculum evaluated by these types of companies may not be possible or effective due to university or other standard requirements, the survey is intended to measure what aspects of the current curriculum could use work or modification. By being able to identify what aspects and what specific competencies are lacking, there can be potential amendments made to the curriculum or learning outcomes and objectives for a class that can help produce more qualified candidates in general who also have the required technology skills for these cybersecurity positions. *Figure 8* and *Figure 9* will discuss further about responses and current university approaches to prepare students with relevant work experience.

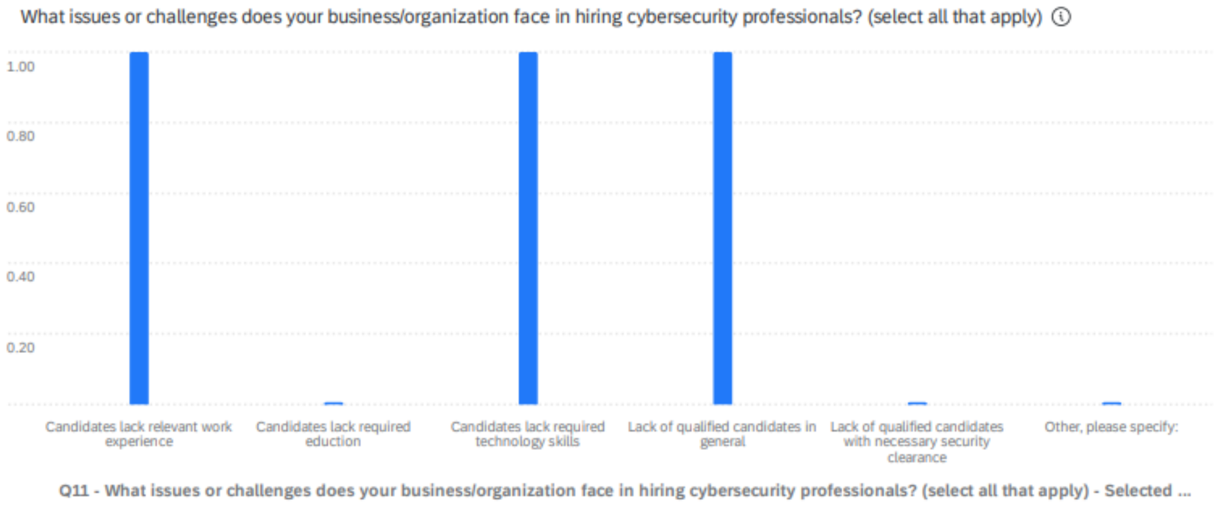

Figure 7: Q11 What issues or challenges does your business/organization face when hiring cybersecurity professionals?

4.2.7 Minimum Requirements for Cybersecurity Professionals

Question twelve delves into what the minimum required education for qualified cybersecurity professionals is. Respondents were given six options: no formal education credential, high school diploma or equivalent, some college/no degree, associate degree, bachelor's degree, master's degree or higher. Two of the respondents said they require a bachelor's degree for their cybersecurity professionals to be considered qualified. Another respondent noted that they only require a high school diploma or equivalent. These results are both shown in *Figure 8.* It is also not specified in this question whether certifications are desired from industry on top of these minimum education requirements, but preferred certifications from these respondents can also be found in *Figure 4*.

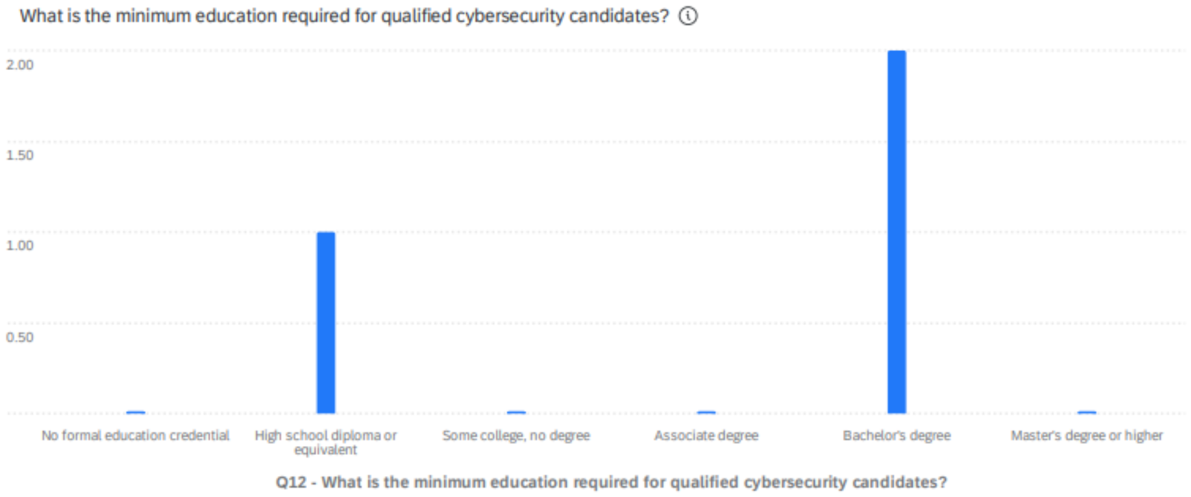

Figure 8: Q12 What is the minimum education required for qualified cybersecurity candidates?

Companies also have minimum prior work experience in addition to minimum education requirements. Question thirteen results are shown in *Figure 9* for what the minimum prior work experience for qualified cybersecurity candidates is. The respondents had the option of choosing none, less than one year, one to two years, three to five years, and six or more years. Two responses were recorded for not requiring any prior experience in order to be considered a qualified cybersecurity candidate. One response was recorded for requiring less than one year of prior work experience. While this question does explore what the minimum requirement for work experience is, it does not say how this work experience can be obtained or if the experience needs to be relevant to what an entry-level cybersecurity job may require.

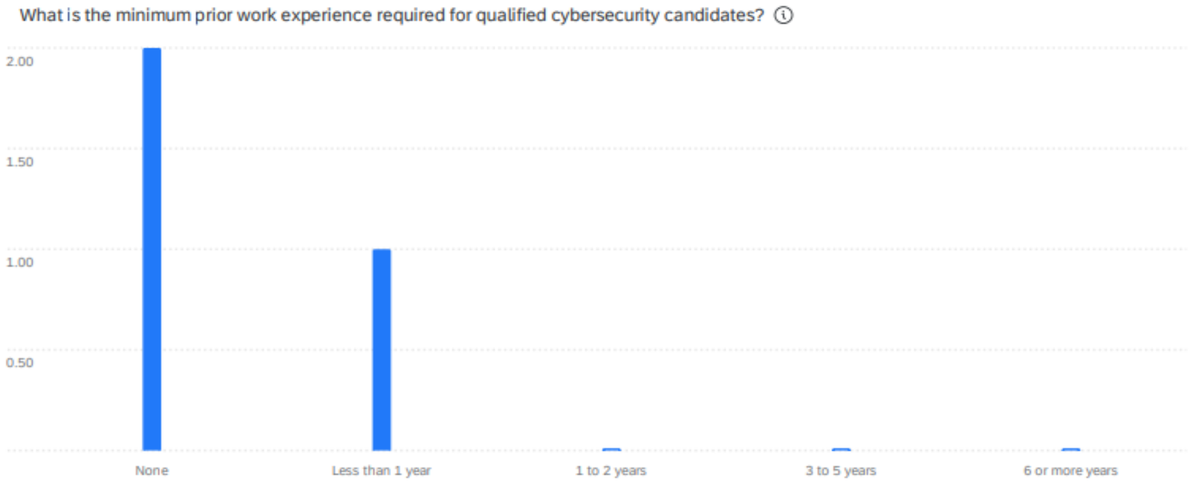

Figure 9: Q13 What is the minimum prior work experience required for qualified cybersecurity candidates?

4.2.8 Soft Skills for Cybersecurity New Hires

Soft skills are something that is equally as important but not as heavily focused on in an academic setting. Question fourteen shown in *Figure 10* asked the respondents to identify what they believed to be the top three soft skills that are most important for cybersecurity new hires. Respondents could choose from the following options: communication, writing, troubleshooting, teamwork/collaboration, ethics, planning, problem solving, building effective relationships, quality assurance and control, self-starter, enthusiasm, quick learner, bilingual, or other with the option to fill in something that was not already listed. The top soft skill that was most important was communication which was selected three times. Ethics and problem solving were selected twice by two respondents. With one response each was quick learner and troubleshooting.

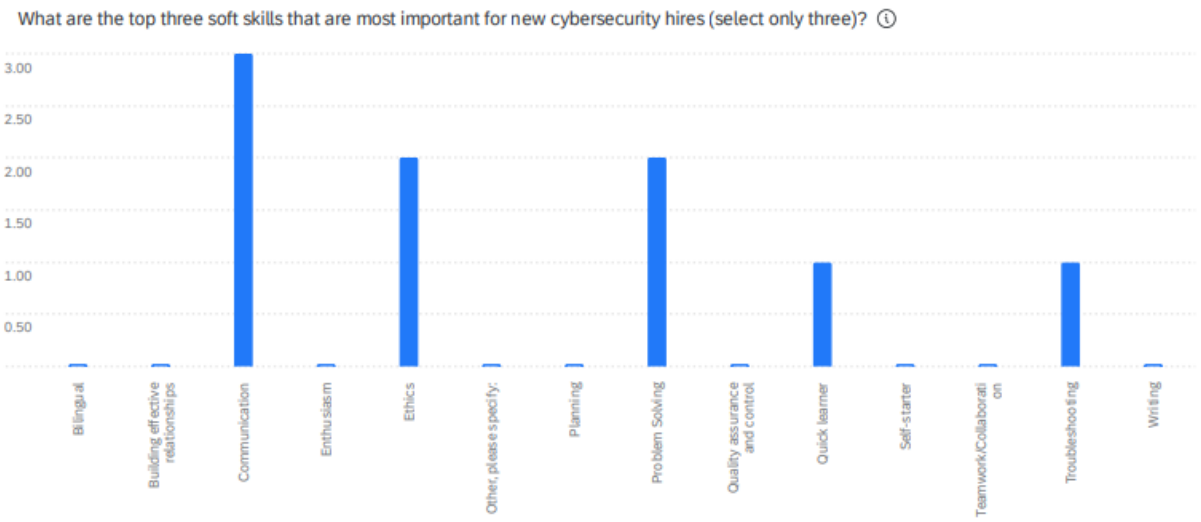

Figure 10: Q14 What are the top three soft skills that are most important for new cybersecurity hires (select only three)?

4.3 Comparison Between Gap Analysis and Survey

Table 6: Comparison of Results

Gap Analysis	Thought to be Missing	Industry Survey Results	What is the Same?	What is Different?
Asset/Inventory Management	Computer Forensics	Client Relationship Management	Computer Forensics	Client Relationship Management
Computers and Electronics	Incident Management	Computer Forensics	Oral Communication	Computer Network Defense
Conflict Management	Knowledge Management	Computer Network Defense	Problem Solving	Critical Thinking
Contracting/Procurement	Operating Systems	Critical Thinking	Risk Management	Data Analysis
Intelligence Analysis	Oral Communication	Data Analysis	Written Communication	Data Privacy and Protection
Knowledge Management	Problem Solving	Data Privacy and Protection		Database Administration
Modeling and Simulation	Risk Management	Database Administration		Identity Management
Operating Systems	Written Communication	Identity Management		Information Systems/Network Security

Table 6: Comparison of Results Continued

Process control		Information Systems/Network Security		Information Technology Assessment
Requirements Analysis		Information Technology Assessment		Interpersonal Skills
Software Development		Interpersonal Skills		Project Management
Software Testing and Evaluation		Oral Communication		Strategic Planning
Systems Integration		Problem Solving		Threat Analysis
Workforce Management		Project Management		Vulnerabilities Analysis
		Risk Management		
		Strategic Planning		
		Threat Analysis		
		Vulnerabilities Assessment		
		Written Communication		

After the completion of the gap analysis and the survey results a comparison can be made between the two. With fourteen NICE competencies not being taught or covered in some capacity; it is probable that there will in fact be a gap. The gap analysis predicted that risk management, incident management, operating systems, knowledge management, and computer forensics were shortcomings in the current cybersecurity curriculum for Purdue University's four-year ABET-accredited undergraduate cybersecurity program. These competencies were either not covered at all or not covered sufficiently enough for a student to be considered proficient in said competency. Risk management is not covered in near enough depth and is merely glossed over briefly in certain courses. Incident management focuses more on writing an incident response plan rather than how to tailor an approach depending on the type of incident. Operating systems are used but not covered and are limited to mostly just Windows and some Linux. Knowledge management is expected that students have a prior understanding, but students are not taught best practices for how to maintain, find, contribute, or document knowledge whether it be for making a decision or sharing findings. Computer forensics is also only covered in one undergraduate course making it difficult to cover all that this particular competency might entail to demonstrate proficiency or adequate knowledge.

The survey results came to the consensus that the most critical issues respondents had with hiring new cybersecurity talent was a lack of work experience, lack of adequate technical skills, and a lack of qualified candidates in general. These respondents also only felt that new hires for industry cybersecurity positions were only somewhat adequately prepared for the demands of the position upon arrival, which is understandable when these companies do not require prior work experience and the minimum education requirements are a high school diploma or bachelor's degree. Now, while these issues are important the respondents were also asked to give university programs, such as this one, suggestions or advice to improve their curricula to better align with workforce requirements. Responses such as networking as much as possible, working on “passion projects,” and working with major companies for a curriculum evaluation were recommended. The survey also noted recruiters hiring for entry level cybersecurity positions prefer industry certifications, something the current undergraduate cybersecurity curriculum at Purdue University does not currently require. The preferred industry certifications can be from CompTIA, CISCO, Ec-Council, or ISC2.

The most important soft skills a new graduate from a four-year cybersecurity program like Purdue’s are communication, ethics, problem solving, and troubleshooting. These soft skills are required and practiced as routine in each undergraduate course regardless of the topic, how to perform each soft skill effectively is not taught. There is an unspoken expectation that each student understands how to communicate effectively and efficiently regardless of the delivery method, especially regarding the cybersecurity industry. However, the most preferred NICE competency the survey results showed in terms of proficiency noted by the respondents was risk management. The next preferred competencies were computer network defense, data privacy and protection, information systems/network security, oral communication, problem solving, threat analysis, and vulnerabilities assessment. Finally, the respondents listed client relationship management, computer forensics, critical thinking, data analysis, database administration, identity management, information technology assessment, interpersonal skills, project management, strategic planning, and written communication.

Based on these findings from both the gap analysis and the survey shown in Table 6, it has been determined that a gap does exist between workforce development for cybersecurity knowledge, skills, and tasks (aka competencies) that graduates from ABET-accredited four-year bachelor's cybersecurity-IT programs (degrees and majors). This comparison shows that as suspected in the original gap analysis and confirmed by the results of the survey, both soft and technical skills along with competencies like risk management and computer forensics are lacking in the current curriculum. It should also be noted that while industry certifications are not required to secure entry level positions at the companies who responded to the survey, they certainly are preferred. This would also be considered a gap as outside industry certifications are not a requirement for the undergraduate four-year cybersecurity program at Purdue University.

5. DISCUSSION AND CONCLUSION

The findings indicated that there is a gap in terms of workforce development for cybersecurity competencies that graduates from ABET-accredited four-year bachelor's cybersecurity-IT programs (degrees and majors) have. Upon discovery that a gap does in fact exists, H_0 is supported, which stated that a gap exists between the industry level expectations for recent graduates from ABET-accredited four-year cybersecurity programs and what is being taught in the curriculum for these same ABET-accredited four-year cybersecurity programs.

This study explored three aspects to determine whether the hypothesis would be supported or not: a gap analysis, a survey, and a comparison between the findings of the two first sections. The gap analysis was the result of breaking down each course taught in the Purdue University ABET-accredited four-year cybersecurity undergraduate program and mapping the competencies taught in these courses to the NICE framework competencies. The NICE framework was chosen because it is the adopted federal standard framework for the cybersecurity industry in the United States. Since it is just a framework, it is more of a suggested outline to follow showing what cybersecurity industry professionals should be able to show proficiency in prior to entering the workforce. The more of these competencies that can be taught in the classroom, the less a prospective student will have to make up proficiency in the missing competencies outside of the classroom through other channels. Essentially, the more competencies covered in the courses that are offered to the students for this degree, the more likely they are to be able to secure a position in the industry upon graduation. The NICE framework lists 60 competencies, 38 of which are currently covered in Purdue University's ABET-accredited four-year cybersecurity undergraduate program, and 14 are not being covered. As mentioned, these remaining competencies that are not currently taught could be covered in elective courses or other courses in different departments in order to fulfill the bachelor's degree requirements for the university.

The survey was the second part of this study. A 25-question survey was created via Qualtrics and distributed through email. The participants were recruited through a list provided by Purdue University's Computer and Information Technology department which consisted of companies who had attended the departmental career fair in previous years. Another distribution was sent out by Purdue University's Center for Career Opportunities (CCO) of companies that have hired students from the Computer and Information Technology department in the past. It is estimated the survey was sent out to about 150 companies. The purpose of this aspect of the study was to connect directly with industry companies that previously hired students from Purdue University ABET-accredited four-year cybersecurity undergraduate program in order to see what they felt were missing or lacking aspects of the current curriculum. The survey consisted of six sections: industry hiring questions, workforce gap, work role related questions, industry demographics, demographics, and closing questions. Each section provided more overview into how the company is involved with cybersecurity, aspects of the hiring process for new cybersecurity professionals such as challenges, what makes a qualified candidate, and preferences for cybersecurity positions at that company.

This survey's results concluded that the most common issues with hiring new cybersecurity talent are lack of qualified candidates in general, lack of work experience, and lack of adequate technical skills. Overall, the respondents noted that they only felt their new cybersecurity hires were somewhat prepared for the demands of the job. When hiring for these new cybersecurity entry level positions, the companies who responded claimed they do not require any industry certifications nor do all of them require a bachelor's degree from a cybersecurity specific program. They do, however, prefer cybersecurity candidates to have industry certifications from CompTIA, ISC2, CISCO, or Ec-Council. The survey also encouraged the respondents to give advice or suggestions related to how they could improve their curriculum and make their students better candidates for entry-level cybersecurity positions. These suggestions noted working on outside “passion projects,” networking as much as possible, and working with industry companies to evaluate their curriculum to better align with workforce requirements. The survey saw that “soft skills” such as communication, ethics, problem solving, and troubleshooting are just as important as the technical skills. Respondents also noted the most preferred NICE competency is risk management, something the current cybersecurity curriculum at Purdue University does not currently cover enough. Competencies such as computer network defense, data privacy and protection, information systems/network security, oral communication, problem solving, threat analysis, and vulnerabilities assessment were also ranked quite high. Many of these would also be categorized as “soft skills” meaning they need to be covered in more depth to ensure a student can demonstrate proficiency. The final competencies still noted, despite not being chosen by every respondent were client relationship management, computer forensics, critical thinking, data analysis, database administration, identity management, information technology assessment, interpersonal skills, project management, strategic planning, and written communication

After performing the gap analysis and completion of the survey's data collection, it can be determined that a gap exists between workforce development for cybersecurity knowledge, skills, and tasks (aka competencies) that graduates from ABET-accredited four-year bachelor's cybersecurity-IT programs (degrees and majors). A comparison between the results of the two parts of this study shows that cybersecurity industry companies value the proficiency of "soft skills" just as much as highly technical skills. NICE competencies such as computer forensics and risk management are shown from the survey to be important to show proficiency in but are also areas the curriculum is lacking in as shown by the original gap analysis. In addition to this comparison showing a gap, it should also be recognized that industry certifications are not a requirement for most cybersecurity industry companies but they are still preferred for many entry-level cybersecurity positions.

It is suspected that we found these results because these are areas that are not covered thoroughly enough in Purdue University's ABET accredited four-year undergraduate cybersecurity program. From the initial gap analysis fourteen competencies were shown to be not covered in any of the cybersecurity specific courses. Thirty-eight competencies were also found to have been covered. However, just because these thirty-eight competencies are covered within a certain course, that does not mean they are covered in any kind of depth or that a student needs to show proficiency. Many of the competencies would be considered "soft skills" such as presenting effectively, oral communication, written communication, (etc...). Now while these soft skills are helpful and might be utilized in each course in terms of an end of course project, these students are not being taught how to communicate their findings effectively regardless of the delivery method. These need to be taught in a consistent way across cybersecurity specific courses that way the skills can be worked on and graded upon the same scale each time. This ensures the student can learn from their mistakes and work on improving them even if the topic of the assignment or project changes depending on the class.

The number one competency that was concurrent with what was previously thought to be missing in the current curriculum that was confirmed by the survey was risk management. Some of the biggest challenges faced were the lack of experience, lack of technical skills, and lack of qualified candidates in general. Only sixty-six percent of respondents felt their new cybersecurity hires had somewhat adequate knowledge to be prepared for the position they were hired for.

It is important that the companies hiring these cybersecurity professionals feel comfortable with the skillset and knowledge of their employees. With entry-level employees already having the skills and knowledge necessary to perform the basic functions of a position, they can be given a broader range of tasks and responsibilities. They might be ahead of their peers and be given more opportunities or progress faster through a promotion track.

Students need to have a realistic understanding of the expectations for minimum knowledge and education requirements. By having data collected directly from the companies that are trying to hire graduates from Purdue’s undergraduate cybersecurity program, it can help better prepare the students as well as show them the benefits of completing the program. While there is no best pathway that is specifically suited to obtaining an entry-level cybersecurity professional position, it can only benefit a prospective student or application by completing a bachelor's degree in cybersecurity. Also, not requiring students to obtain an industry certification for the current curriculum would contribute to the gap as industry certifications can serve as a catch all for specific aspects of the cybersecurity industry instead of being tested within a course on a particular topic. Fifty percent of respondents preferred their entry level cybersecurity hires to have an industry certification whether its CISSP, CEH, CCNS, CCNP, Sec+, or Pentest+. By not requiring this in some capacity, students might struggle to set themselves apart from other applicants for the same entry-level cybersecurity positions.

Soft skills are important to note because they are not directly taught in a technical academic setting. They are usually just practiced repetitively in the form of group projects, lab reports, and presentations. But these skills are not taught how to be done most effectively, especially in a technical setting. It is important to have these skills but even more so to have them and be able to adapt them based on the needs of the audience. Communication is one of the biggest soft skills that companies need an employee to be competent in because they need to be able to communicate their findings or issues in a concise understandable manner to peers, supervisors, clients, stakeholders, etc. Ethics is huge in cybersecurity and needs to be understood on all fronts with all employees to ensure there are no violations of any laws or policies being that of the company or on a state or federal level. Problem solving and troubleshooting go hand in hand. A prospective hire needs to be able to solve simple problems and not be handheld on how to do so after a certain point. This can come in the form of asking the right questions or following the correct procedures in case of an incident.

While the respondents concurred that anywhere from no prior work experience to less than a year of work experience is required, this is not the case for all companies hiring entry-level cybersecurity professionals. It is the experience of the author that this is not the case for most companies hiring right out of a four-year cybersecurity program. More often than not companies want to see several years, or summers worth of internship experience taken concurrently with completing a four-year university undergraduate cybersecurity program. The difficulty with this is that companies are typically hiring those with more experience, which is understandable in an entry-level position right after graduation. However, when this experience needs to start within the first few years via an internship acquired by the student's own accord or through a university sponsored career fair, it can leave many students behind who are not seen as "desirable" due to lack of outside projects. Building up students with more experience, who more often than not, are the top academic performers can also tend to leave a gap between those students and those who may not be top performers. This leaves those students who are still trying to secure the necessary experience from an internship or job that will make them equally as competitive upon graduation behind from the start. Based on personal experience, some of the recommendations I would make for any four-year undergraduate cybersecurity curriculum would be to encourage attendance at conferences of any kind whether they be academic or more informal, including a requirement for at least one industry level certification, and aid for students directly from the department/program/faculty on preparing for career fairs and potential job prospects in the cybersecurity industry. This could be accomplished by obtaining and working with a student success advisor specific to the department this program resides in. By having a specific person dedicated to understanding what options there are for students to learn outside of academia, we could work on creating a graduated approach for benchmarking options available to students depending on what year they are into the program. This might provide more realistic and doable options for students as they progress throughout their career. Of course, these options would be self-paced for the students, but will give them a good idea of where they can start if they are looking for opportunities for learning outside of the classroom.

While conducting this study there were some limitations throughout the process. These limitations could be a means for future research both in this area and as a continuation of this study specifically. If the study were to be redone, it would be better if there was a larger sample size for the industry survey. The biggest limitation this study saw was how many people the survey was able to reach. It is possible the with the lists given the survey did not reach a physical person whether that be the email was stuck in a spam filter due to being sent from an outside sender from the company's organization, the email was invalid or not current, or the contact was no longer with that company. The survey would have had a higher response rate if there were better contacts, this could have potentially been done by expanding the scope to include those who have been hired from the computer science and computer engineering departments at Purdue University. More responses could have shown different results in what was most likely lacking or missing in terms of a knowledge gap for competencies being taught in cybersecurity courses. Another limitation to consider is why there was not a better list of contacts to send the survey too, this could mean that the department is not as connected to the industry as they think or claim to be.

If the study were to be continued, it might be beneficial to expand the survey to more companies that hire students from other ABET accredited four-year cybersecurity institutions. This could also be expanded by companies that hire students with any form of cybersecurity specific college degree or certification. By expanding the list of companies there is a possibility for a higher response rate for the survey which could give more insight into what the specific gaps in knowledge are. By having the specific gaps narrowed down it would be easier to see where to bridge that gap. Another path for future research would be to compare the results of this survey to other ABET accredited four-year cybersecurity programs. While these other programs might have the same requirements to keep their accreditation, they might have different courses, learning objectives, and competencies being covered within that program. It is believed that part of the reason we found these differences is that industry focuses more on training and workforce development needs, whereas universities have an education and understanding focus. While education might include training, it is not solely focused on it.

REFERENCES

2022 best undergraduate cybersecurity programs - US news ... Best Undergraduate Cybersecurity Programs Computer Science/Cybersecurity. (n.d.). Retrieved January 4, 2022, from https://www.usnews.com/best-colleges/rankings/computer-science/cybersecurity

ABET approves accreditation criteria for Undergraduate Cybersecurity programs. ABET. (2018, November 30). Retrieved January 4, 2022, from https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/

ABET seeks feedback on proposed accreditation criteria for Cybersecurity Engineering Academic programs. ABET. (2017). Retrieved January 4, 2022, from https://www.abet.org/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-engineering-academic-programs/

Aufman, Sherri, and Ping Wang. 2019. "Discovering Student Interest and Talent in Graduate Cybersecurity Education." In 16th International Conference on Information Technology-New Generations (ITNG 2019), 77–83. Springer International Publishing.

Bicak, Ali, Xiang Michelle Liu, and Diane Murphy. 2015a. "Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program." Information Systems Education Journal 13 (3): 99.

Bicak, Ali, Xiang Michelle Liu, and Diane Murphy. 2015b. "Cybersecurity Curriculum Development: Introducing Specialties in a Graduate Program." Information Systems Education Journal 13 (3): 99.

Burley, Diana L., and Alfred H. Lewis. 2019. "Cybersecurity Curricula 2017 and Boeing: Linking Curricular Guidance to Professional Practice." Computer. https://doi.org/10.1109/mc.2018.2883567.

California, S. (2018). Cybersecurity: Labor Market Analysis and Statewide Survey Results from California Employers and Postsecondary Institutions. Retrieved October 14, 2020, from https://militarycouncil.ca.gov/2018/08/22/cybersecurity-labor-market-analysis-and-statewide-survey-results-from-california-employers-and-postsecondary-institutions/

Chang, Hsia-Ching, Cary Jim, and Suliman Hawamdeh. 2020. "Bridging the Cybersecurity Talent Gap: Cybersecurity Education in iSchools." Cybersecurity for Information Professionals. https://doi.org/10.1201/9781003042235-4.

CompTIA Career Pathway. Which certification is right for me: CompTIA it certifications. Cybersecurity Pathway. (n.d.). Retrieved January 3, 2022, from https://www.comptia.org/certifications/which-certification

Conklin, Wm Arthur, Raymond E. Cline, and Tiffany Roosa. 2014a. "Re-Engineering Cybersecurity Education in the US: An Analysis of the Critical Factors." In 2014 47th Hawaii International Conference on System Sciences, 2006–14. IEEE.

Conklin, Wm Arthur, Raymond E. Cline, and Tiffany Roosa. 2014b. "Re-Engineering Cybersecurity Education in the US: An Analysis of the Critical Factors." In 2014 47th Hawaii International Conference on System Sciences, 2006–14. IEEE.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014. "Defining Cybersecurity." Technology Innovation Management Review 4 (10). https://timreview.ca/article/835.

Criteria for Accrediting Computing Programs, 2020 – 2021. ABET. (n.d.). Retrieved January 4, 2022, from https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2020-2021/

Crumpler, W., & Lewis, J. A. (2020, May 22). The Cybersecurity Workforce Gap. Retrieved October 14, 2020, from https://www.csis.org/analysis/cybersecurity-workforce-gap

Cybersecurity Certifications: Information Security Certifications: (ISC)². Cybersecurity Certifications | Information Security Certifications | (ISC)². (n.d.). Retrieved December 27, 2021, from https://www.isc2.org/Certifications

Cybersecurity Courses & Certifications. Cyber Security Courses | SANS Institute. (n.d.). Retrieved December 27, 2021, from https://www.sans.org/cyber-security-courses/?msc=home-header

Cybersecurity curricula 2017 - Association for Computing ... (2017, December 31). Retrieved from https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Dearing, J. (2009, September 1). Applying Diffusion of Innovation Theory to Intervention Development. Retrieved December 02, 2020, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2957672/

Faily, S. (n.d.). Ethical Hacking Assessment as a Vehicle for Undergraduate Cyber-Security Education. core.ac.uk. Retrieved January 4, 2022, from https://core.ac.uk/download/pdf/42142144.pdf

Hoag, Jim. 2013. "Evolution of a Cybersecurity Curriculum." Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13. https://doi.org/10.1145/2528908.2528925.

HR perceptions of it training and certification - CompTIA. (n.d.). Retrieved January 13, 2022, from https://certification.comptia.org/docs/default-source/downloadablefiles/hr-perceptions-of-it-training-and-certification.pdf

It certification roadmap - CompTIA. IT Certification Roadmap. (n.d.). Retrieved December 27, 2021, from https://certification.comptia.org/docs/default-source/downloadablefiles/it-certification-roadmap

Jeffery, L., & Ramachandran, V. (2021, July 8). *Why ransomware attacks are on the rise - and what can be done to stop them*. PBS. Retrieved January 13, 2022, from https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them

Karampidis, K., S. Panagiotakis, M. Vasilakis, E. K. Markakis, and G. Papadourakis. 2019. “Industrial CyberSecurity 4.0: Preparing the Operational Technicians for Industry 4.0.” In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 1–6.

Knapp, Kenneth J., Christopher Maurer, and Miloslava Plachkinova. 2017. “Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance.” Journal of Information Systems Education 28 (2): 101.

Knutson, T. (2020, February 11). *Cybersecurity jobs going begging as college computer science grads lack skills/experience says House leader*. Forbes. Retrieved January 13, 2022, from https://www.forbes.com/sites/tedknutson/2020/02/11/cybersecurity-jobs-going-begging-as-college-computer-science-grads-lack-skillsexperience-says-house-leader/

Leaser, D. (2019, July 24). *The demand for cybersecurity professionals is outstripping the supply of skilled workers*. IBM Training and Skills Blog. Retrieved January 3, 2022, from https://www.ibm.com/blogs/ibm-training/new-cybersecurity-threat-not-enough-talent-to-fill-open-security-jobs/

Lewis, J. A. (2019, January 29). The Cybersecurity Workforce Gap. Center for Strategic and International Studies (CSIS). Retrieved from https://www.csis.org/analysis/cybersecurity-workforce-gap

Libicki, Martin C., David Senty, and Julia Pollak. 2014. Hackers Wanted: An Examination of the Cybersecurity Labor Market. Rand Corporation.

Macnish, K., & Ham, J. van der. (2020, September 9). *Ethics in Cybersecurity Research and Practice*. Technology in Society. Retrieved January 13, 2022, from https://www.sciencedirect.com/science/article/pii/S0160791X19306840

McGill, T. & Dixon, M. (2005). Information Technology Certification: A Student Perspective. Information International Journal of Information and Communication Technology Education, 1(1), 19-30.

Morgan State University. (2021, August 31). *Nice Framework Success Story: Cybersecurity curricula*. NIST. Retrieved January 5, 2022, from https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-success-story-1

Mouheb, Djedjiga, Sohail Abbas, and Madjid Merabti. 2019. "Cybersecurity Curriculum Design: A Survey." In Transactions on Edutainment XV, edited by Zhigeng Pan, Adrian David Cheok, Wolfgang Müller, Mingmin Zhang, Abdennour El Rhalibi, and Kashif Kifayat, 93–107. Berlin, Heidelberg: Springer Berlin Heidelberg.

NICE Cybersecurity Workforce Framework. (n.d.). Retrieved October 14, 2020, from https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

The National Cybersecurity Workforce Framework. National Initiative for Cybersecurity Education (NICE). (n.d.). Retrieved January 4, 2022, from https://www.nist.gov/system/files/documents/2017/04/04/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (n.d.). *Workforce Framework for cybersecurity (NICE framework) - NIST*. NIST Special Publication 800-181 Revision 1. Retrieved January 4, 2022, from https://doi.org/10.6028/NIST.SP.800-181r1

Patterson, Wayne, Cynthia Winston, and Lorraine Fleming. 2016. "Behavioral Cybersecurity: Human Factors in the Cybersecurity Curriculum." Advances in Intelligent Systems and Computing. https://doi.org/10.1007/978-3-319-41932-9_21.

Programs. EC. (2021, April 16). Retrieved December 27, 2021, from https://www.eccouncil.org/programs/

Rainie, L., & Anderson, J. (2020, August 6). *Experts on the future of work, jobs training and skills*. Pew Research Center: Internet, Science & Tech. Retrieved January 13, 2022, from https://www.pewresearch.org/internet/2017/05/03/the-future-of-jobs-and-jobs-training/

Rashotte, R. (2020, December 30). Closing the cyber skills gap requires a culture of continuous learning. Security Magazine RSS. Retrieved January 3, 2022, from https://www.securitymagazine.com/articles/94254-closing-the-cyber-skills-gap-requires-a-culture-of-continuous-learning

Rayome, A. D. N. (2017, March 29). *5 reasons your company can't hire a cybersecurity professional, and what you can do to fix it*. TechRepublic. Retrieved January 13, 2022, from https://www.techrepublic.com/article/5-reasons-your-company-cant-hire-a-cybersecurity-professional-and-what-you-can-do-to-fix-it/

Rob, M. A. (2014). IT Certification: Demand, Characteristics, and Integration into Traditional University MIS Curriculum. Communications of the IIMA, 14(1), 20-44.

SAHIN, I. (2006, April). DETAILED REVIEW OF ROGERS' DIFFUSION OF INNOVATIONS THEORY ... Retrieved December 2, 2020, from https://files.eric.ed.gov/fulltext/ED501453.pdf

Shoemaker, Daniel, Anne Kohnke, and Ken Sigler. 2020. "The Cybersecurity Body of Knowledge." https://doi.org/10.1201/9781003022596.

State of cybersecurity 2021. ISACA. (n.d.). Retrieved January 4, 2022, from https://www.isaca.org/go/state-of-cybersecurity-2021?utm_source=isaca&utm_medium=other&utm_campaign=research&utm_content=pr_research_state-of-cybersecurity-2021-part-1-press-release&cid=pr_2006993&Appeal=pr

Thames, Lane, and Dirk Schaefer, eds. 2017. Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing. Springer, Cham.

Western Governors University. (2021, November 10). *A guide to common entry-level cyber security jobs*. Western Governors University. Retrieved January 4, 2022, from https://www.wgu.edu/blog/guide-entry-level-cyber-security-jobs2102.html#close

Wireschen, D. & Zhang, G. (2010). Information Technology Certification Value: An Initial Response from Employers. Journal of International Technology and Information Management, 19(4), 89-109.

Wright, M. A. (2015). Improving Cybersecurity Workforce Capacity and Capability. ISSA

Journal, 14-20.

Zurier, S. (2021, June 25). 56% of security professionals say today's cyber workforce lacks Soft Skills. SC Media. Retrieved January 4, 2022, from https://www.scmagazine.com/news/training/56-of-security-managers-say-todays-cyber-workforce-lacks-soft-skills

APPENDIX

Cyber Industry Needs Survey Thesis Version Final

Start of Block: Industry Hiring Questions

Consent Cyber Industry Needs Survey Thank you for your interest in our study of cyber industry industry needs. The purpose of this study is to assess current industry and workforce needs in cybersecurity. Completing this survey will take approximately fifteen (15) minutes of your time. Participation in this survey is completely voluntary. You are free to stop answering questions at any time. Any data that you provide will be strictly confidential and will be stored securely. If you have any questions about this study, please contact Sienna Bates at the following email address: bates46@purdue.edu This research project has been approved by the Purdue University Institutional Review Board. If you have read and understand the above statements, please click 'I consent' button below to indicate your consent to participate in this study.

○ I consent (1)

○ I do not consent (2)

Skip To: End of Survey If Cyber Industry Needs Survey Thank you for your interest in our study of cyber industry industry n... = I do not consent

Q1

Do you employ Cybersecurity and/or Information Technology(IT)/Information Systems(IS) workers who require some level of cybersecurity skills?

○ Yes (1)

○ No (2)

Skip To: End of Survey If Do you employ Cybersecurity and/or Information Technology(IT)/Information Systems(IS) workers who... = No

Q2 Does your company hire graduates from university cybersecurity programs?

○ Yes (1)

○ No (2)

Skip To: End of Survey If Does your company hire graduates from university cybersecurity programs? = No

Q3 If you answered yes to above, how many do you hire per year?

____

Q4 Do you plan to hire any Cybersecurity and/or IT/IS workers who require some level of cybersecurity skills in the next 12-24 months?

○ Yes (1)

○ No (2)

Q5

Are you familiar with current employment numbers, work roles and hiring criteria for cybersecurity and or IT/IS workers who require some level of cybersecurity skills at your organization?

○ Yes (1)

○ No (2)

Skip To: End of Survey If Are you familiar with current employment numbers, work roles and hiring criteria for cybersecurity... = No

Q6 Do you prefer any cybersecurity industry certifications for new hires?

○ Yes (1)

○ No (2)

Skip To: End of Block If Do you prefer any cybersecurity industry certifications for new hires? = No

Q7 If yes, which ones?

□ Certified Information Systems Security Professional (CISSP) (1)

□ CISCO Certified Network Associate (CCNA) (2)

□ CISCO Certified Network Professional (CCNP) (3)

□ CompTIA PenTest + (4)

□ CompTIA Security + (5)

□ Ethical Hacker (6)

□ SANS/GIAC Certification (7)

□ Certified Information Systems Auditor (CISA) (8)

□ Certified Information Security Manager (CISM) (9)

□ Other, please specify: (10)

____

End of Block: Industry Hiring Questions

Start of Block: Workforce Gap

Q8 Do you feel your new hires coming from university cybersecurity programs have adequate cybersecurity related knowledge and skills?

○ Yes (1)

○ Somewhat (2)

○ No (3)

Q9 What are the top 10 competencies do you most prefer an entry level cybersecurity professional have? (repeat from earlier)(add 38 competencies add other and fill response)

□ Business Continuity (1)

□ Client Relationship Management (2)

□ Collection Operations (3)

□ Computer Forensics (4)

□ Computer Network Defense (5)

□ Critical Thinking (6)

□ Data Analysis (7)

□ Data Management (8)

□ Data Privacy and Protection (9)

□ Database Administration (10)

□ Database Management Systems (11)

□ External Awareness (12)

□ Identity Management (13)

□ Information Assurance (14)

□ Information Management (15)

□ Information Systems/Network Security (16)

□ Information Technology Assessment (17)

□ Interpersonal Skills (18)

□ Legal, Government, and Jurisprudence (19)

□ Mathematical Reasoning (20)

□ Operations Support (21)

□ Oral Communication (22)

□ Organizational Awareness (23)

□ Policy Management (24)

□ Presenting Effectively (25)

□ Problem Solving (26)

□ Project Management (27)

□ Risk Management (28)

□ Strategic Planning (29)

□ Systems Testing and Evaluation (30)

□ Target Development (31)

□ Teaching Others (32)

□ Technology Awareness (33)

□ Third Party Oversight/Acquisition Management (34)

□ Threat Analysis (35)

□ Vulnerabilities Assessment (36)

□ Web Technology (37)

□ Written Communication (38)

Q10 What, if any, advice would you give to the university programs to better align their graduates with workforce requirements?

____

End of Block: Workforce Gap

Start of Block: Work Role Related Questions

Block Introduction For the following set of questions, we would like for you to try to equate your business/organization's specific position titles with the more general work roles. The titles used in the survey may differ from the specific titles used in your organization.

Q11 What issues or challenges does your business/organization face in hiring cybersecurity professionals? (select all that apply)

□ Lack of qualified candidates with necessary security clearance (1)

□ Candidates lack required education (2)

□ Candidates lack relevant work experience (3)

□ Candidates lack required technology skills (4)

□ Lack of qualified candidates in general (5)

□ Other, please specify: (6)
____

□ N/A (7)

Q12 What is the minimum education required for qualified cybersecurity candidates?

○ No formal education credential (1)

○ High school diploma or equivalent (2)

○ Some college, no degree (3)

○ Associate degree (4)

○ Bachelor's degree (5)

○ Master's degree or higher (6)

○ N/A (7)

Q13 What is the minimum prior work experience required for qualified cybersecurity candidates?

○ None (1)

○ Less than 1 year (2)

○ 1 to 2 years (3)

○ 3 to 5 years (4)

○ 6 or more years (5)

Q14 What are the top three soft skills that are most important for new cybersecurity hires (select only three)?

□ Communication (1)

□ Writing (2)

□ Troubleshooting (3)

□ Teamwork/Collaboration (4)

□ Ethics (5)

□ Planning (6)

□ Problem Solving (7)

□ Building effective relationships (8)

□ Quality assurance and control (9)

□ Self-starter (10)

□ Enthusiasm (11)

□ Quick learner (12)

□ Bilingual (13)

□ Other, please specify: (14)

____

Q15 On average, has the percentage of time spent on security/cybersecurity issues increased, compared to the percentage of time spent 12 months ago?

○ Yes (1)

○ No (2)

○ Unsure (3)

Skip To: End of Block If On average, has the percentage of time spent on security/cybersecurity issues increased, compared... != Yes

End of Block: Work Role Related Questions

Start of Block: Industry Demographics

Q16 What industry is your firm most closely associated with? (Select only one)

○ Mining (1)

○ Construction (2)

○ Manufacturing (3)

○ Agriculture (4)

○ Wholesale Trade (5)

○ Retail Trade (6)

○ Transportation, Warehouse, and Utilities (7)

○ Information (including information technology, information systems, ISP providers, etc.) (8)

○ Finance and Insurance (9)

○ Real Estate, Rental, and Leasing (10)

○ Professional, Scientific, and Technical Services (11)

○ Administrative, Support, and Waste Services (12)

○ Educational Services (13)

○ Health Care and Social Assistance (14)

○ Arts, Entertainment, and Recreation (15)

○ Accommodation and Food Services (16)

○ Federal Government (17)

○ State Government (18)

○ Local Government (19)

○ Other, please specify: (20) ____

Q17 How is your business/organization involved with cybersecurity? (Select all that apply)

- □ Creator/Producer of Cyber Security Products (1)
- □ Provider of Cyber Security products and/or services (2)
- □ User of Cyber Security products or services (3)
- □ Other involvement with Cyber Security (4)
- □ Regulated industry (5)

Q18 How many permanent employees work at your location, including full-time, part-time, and remote employees?

____

Q19

How many employees do you expect to have at your location 12 months from now, including part-time and full-time employees?

- ○ More (1)
- ○ Less (2)
- ○ The same number of permanent employees (3)

End of Block: Industry Demographics

Start of Block: Demographic Questions

Q20 In which state is your business or company located at?

____

Q21 Which of the following most accurately describes your primary functional work area?

○ CEO (1)

○ CIO (4)

○ CTO (5)

○ CFO (6)

○ CISO (7)

○ Senior Manager (8)

○ Manager (9)

○ HR (12)

○ Other, please specify: (11) ____

Q22 How many employees are there in your company?

○ Under 10 (1)

○ 10-50 (2)

○ 51-100 (3)

○ 100-1,000 (4)

○ 1,000-5,000 (5)

○ 5,000-10,000 (7)

○ more than 10,000 (8)

Q23 What is the annual revenue of your company?

○ Under $10,000 (1)

○ $10,001 to $50,000 (2)

○ $50,001 to $100,000 (3)

○ $100,001 to $500,000 (4)

○ $500,001 to $1 Million (5)

○ $1 Million to $10 Million (6)

○ $10 Million to $50 Million (7)

○ $50 Million to $100 Million (8)

○ Over $100 Million (9)

○ Unsure (13)

○ Prefer not to say (11)

Q24 What percentage of your organization's operating budget is spent on cybersecurity?

○ Less than 10% (1)

○ 10 to 25% (2)

○ 26 to 50% (3)

○ 51 to 75% (4)

○ 76 to 99% (5)

○ 100% (6)

○ Unsure (7)

End of Block: Demographic Questions

Start of Block: Closing Questions

Q25 Do you have any comments or feedback?

____

____

____

____

____

End of Block: Closing Questions