Issues in Information Systems
Volume 24, Issue 2, pp. 320-333, 2023

DOI: https://doi.org/10.48009/2_iis_2023_128

Comparing cybersecurity skills and cybersecurity curricula: a pre and post COVID analysis

Queen E. Booker, *Metro State University, queen.booker@metrostate.edu*
Mousumi Munmun, *Metro State University, mousumi.munmun@metrostate.edu*

Abstract

COVID brought many changes to the workplace. Now that most COVID restrictions have been removed, organizations are faced with a diminished workforce, with a national unemployment rate of 3.4%. As with other occupations, cybersecurity professionals are in demand. Low unemployment often means changing educational requirements and/or years of experience to attract a wider range of candidates and potential employees. This paper examines and compares pre-COVID (2019) and post-COVID (2022) position descriptions and current cybersecurity curricula to how well the curricula is preparing new graduates for employment in the workplace. This study is limited to US based organizations. Results indicate that the position description changes in required skills have mostly resulted in an increase in soft skills, and that most curricula remain strong on the technical skills but few are explicit regarding building the soft skills.

Keywords: Cybersecurity, position analysis, curriculum analysis, education

Introduction

Businesses have become dependent on information technology for day-to-day operations. With that dependency comes a dependency on security measures to protect the computer, data and internet connections that links the business to their customers, suppliers and other stakeholders. According to Gartner (2022), worldwide spending on security and risk management is forecast to grow 11.3% in 2023 due to increased remote or hybrid work, zero-trust network access, and cloud delivery. In addition, there are increasing and sophisticated threats to organizations across the globe. For example, in 2021, cloud exploitation increased by 95%, and dark web traffic increased by 112% (CrowdStrike, 2022). These increasing trends in cybersecurity threats highlight the need to close the gap between supply and demand for cybersecurity professionals with the right skills and experiences.

The novel Corona virus disease (COVID) pandemic caused many US businesses to shutter their doors and request most professionals to work remotely. The pandemic also saw a migration from the workforce, resulting in a US unemployment rate is 3.4% in 2023, which is almost equivalent to full employment. Both the outmigration and full employment conditions are exacerbating the supply of cybersecurity professinals. According to the U.S. Bureau of Labor Statistics ([BLS] 2022), the overall employment rate is expected to be robust, especially in computer and information technology with an expected growth of 15% between 2021 to 2031.

Over the decade, this growth will create about 682,800 new jobs. Additionally, there will be even more openings due to retirement or change of profession, around 418,500 on average. Comparatively, the BLS projects that the number of cybersecurity jobs will grow by 35% between 2021 and 2031. Worldwide, there

are currently about 3.5 million open cybersecurity jobs, according to Cybersecurity Ventures (Sausalito, 2021). The number of openings reported by Cybersecurity Ventures confirms the Wall Street Journal (2018) article that discusses the gap between supply and demand for cybersecurity professionals. However, despite the demand and the limited supply of cybersecurity professionals, new graduates still need to be "prepared" to enter the workforce, which requires higher education to be diligent in preparing students with the right knowledge, skills and abilities (KSA) to be successful, especially since cybersecurity professionals require a set of specialized technical skills.

This study examines the skills required for new undergraduate graduates with a year or less of work experience for 2019 and 2022, comparing the skills for both years and identifying the changes. Those skills are then compared to a random selection of academic programs to ascertain how well the programs are designed to meet the changing needs of businesses. The paper is organized as follows. Next is the literature review which is followed by the research methodology, results, discussion, and conclusions, limitations and next steps.

Literature Review

According to Joint Task Force on Cybersecurity Education (2017), cybersecurity skills "range from the areas like cryptography and network defense to planning, policy development, and regulatory compliance" (p. 78). Hall & Rao's (2020) study also confirmed the need for specialized technical skills but found a growing need for non-technical skills for cybersecurity graduates because technical skills alone are inadequate to handle security threat incidents. Harris & Patten (2015), however, stated that postsecondary institutions are challenged to provide graduates for the emergent cybersecurity sector with sufficient skill and knowledge. To better understand this gap, it is necessary to perform both position analysis and curricula analysis, and determine how well curricula is meeting industry expectations. Comparison of historical position descriptions can also indicate changes that are needed to determine needed changes to the curricula.

Higher education plays a critical role in protecting the world's cyber infrastructure as it is the only industry that provides degreed cyber professionals. However, the ability to supply enough people to meet the current and growing demand means information system security (ISS) programs plays a key role in keeping IT infrastructure safe (Hwang & Soe, 2010; Mills et al., 2016; Sauls & Gudigantala, 2013).

Hunter (2022) mentioned that not only threats are increasing they are also changing in nature. Mills et al. (2016) point out that these circumstances complicate the post-secondary cyber security curricula development. To prepare students for the job market, faculty need to understand and adjust their curriculum according to the most current industry needs which can be ascertained from position descriptions as well as discussion with industry professionals (Gudigantala, 2013; Triche et al., 2016).

The methodologies for designing and delivering post-secondary programs for the growing cybersecurity industry have been much examined in current literature. There is agreement that the best practice is to design a curriculum based on employers' expectations such as job postings and direct conversations with industry professional. Post-secondary professional programs analyze employment advertisements to understand specific skill requirements (Brooks et al., 2018; Hirudayaraj & Baker, 2018; Stanton, 2017).

Job postings play a crucial role in curriculum development to accurately reflect the industry standards in an academic program (Carnevale et al., 2014; Diamond et al., 2014). The reasons for this core role are that it delivers real-time hiring trends, employment demand statistics, and degree and skill requirements (Ahsan et al., 2013; Carnevale et al., 2014; Rosén, 2014). A study by McArthur et al. (2017) found that the best method for examining the emergent industry's skill and employment environment demand is the recruitment

ads analysis method. Downey et al. (2008) and Harper (2012) also support this method. Information Systems is a constantly changing discipline and industry. Thus, the literature reflects this with multiple empirical studies based on job postings as datasets in order to capture current requirements for skills and degrees (Booker & Munmun, 2022; Brooks et al., 2018; Debuse & Lawley, 2009; Harris et al., 2012).

Brooks et al. (2018) state that to develop a successful cybersecurity curriculum, post-secondary educators must evaluate the range of employer expectations. The authors analyzed 798 job postings to capture all skill requirements from employers. They argue that findings from the job posting need critical analysis before being added to the curriculum because not all employers' expectations can be covered in a two to four years degree cycle. Therefore, a curriculum developer must focus on the major and timely ones. Peslak & Hunsinger (2019) analyzed 487 cybersecurity analyst positions and found employers asked for industry certificates and job experience along with a post-secondary degree. Parker & Brown (2019) analyzed 196 cybersecurity job advertisements from five websites in South Africa. The authors found that employers were looking for both soft and technical skills. They also found that employers preferred an undergraduate Information Systems degree with industry certificates.

Paulsen et al. (2012) proposed a community effort strategy for cybersecurity education and cyber workforce development. The community here is government, academia, and industry. Connections between these three sectors are significant. For example, the government develops policies that the industry follows, academia develops degree programs based on industry needs, and the industry hires students from academia. To train the tomorrow's workforce, academia needs to know the industry's needs; similarly, the industry needs to know about the policy they can work within. Furthermore, in cybersecurity, skill sets are driven by the industry, which makes collaboration especially needed for program development in academia.

Liu & Murphy (2012) developed a "when" and "how" holistic framework for Information Systems courses in order to balance between a sustainable curriculum and adding emergent topics. The authors argue that while academia needs to prepare students for current competitive job market conditions, it must also teach critical thinking skills and adaptive strategies for future technology innovations and industry environments. Bicak et al. (2015) adapted Liu & Murphy's (2012) holistic framework to develop a graduate-level cybersecurity curriculum. They suggest developing a cybersecurity curriculum strategically to serve the industry. In addition, they developed specialties strategically based on the holistic framework. For the graduate level, they recommended three specialties: cybersecurity data analysis, cyber intelligence, and health care security and privacy.

Research Study/Methodology

This study compares job posting data for 2019 and 2022 from indeed.com is an online job posting site that describes itself as “the #1 job site in the world with over 300M unique visitors every month” (indeed.com accessed 5/24/2023). The use of indeed.com for position analysis has been used in prior research including Ramezan (2023), Ho et al. (2019), and Verma et al. (2019). The study also examines curricula for 30 randomly selected cybersecurity bachelor degree programs. The programs were selected from the list of degree programs provided by the website cybersecurity guide (2023)

Data Collection-Position Descriptions

The job posting data was collected daily from January 1, 2019 through December 31, 2022 using the terms cybersecurity, information security and information assurance with the filter of posted within the last twenty-four hours. The data was collected using a Python script. Data collected included the position title, position description, required qualifications, preferred qualifications, and position location. The total

number of positions for 2019 was 224536, of which 149793 were duplicate, reposts, or multiple postings for the same position, leaving 114743 for analysis. The total number of positions for 2022 was 373030 of which 223828 were duplicate, reposts, or multiple postings for the same position, leaving 149212 for analysis. Next, the remaining position titles were examined to eliminate positions that were not specific for cybersecurity professionals such as sales and marketing, user design, or product development.

The elimination of those positions reduced the number of usable positions to 100723 for 2019 and 102651 for 2022. Of the positions analyzed for 2019, 95237 of the positions required a bachelor's degree, 19001 required a Master's degree, and 45897 required one year or less of prior experience. In 2022, 125338 required a bachelor's degree, 22012 a Masters, and 51261 required one year or less of prior work experience. This list was further refined to only include positions requiring a year or less of work experience and a Bachelor's degree which would be the closest to the majority of new cybersecurity graduates. This resulted in 40,601 positions to analyze for 2019 and 46,183 for 2022. A random selection of 100 positions for each year was selected to verify the remaining positions were designed to recruit cyber security professionals.

Data Collection-Curricula

The curricula data was collected on May 1, 2023 from 30 randomly selected programs from the list of bachelor degree programs posted on cyber…com. The data was manually collected by visiting the website for the program and listing the courses offered and then viewing the course catalog for course descriptions. Only courses specific to the program were viewed. According to cyber…com, there are 226 cybersecurity or information security programs currently available across the US. Figure 1 shows the number of programs available in each state. A search of key terms from position descriptions lead to the identification of an additional 120 related degrees such as Computer Science, Management Information Systems, Information Assurance, Software Engineering and Systems Engineering.

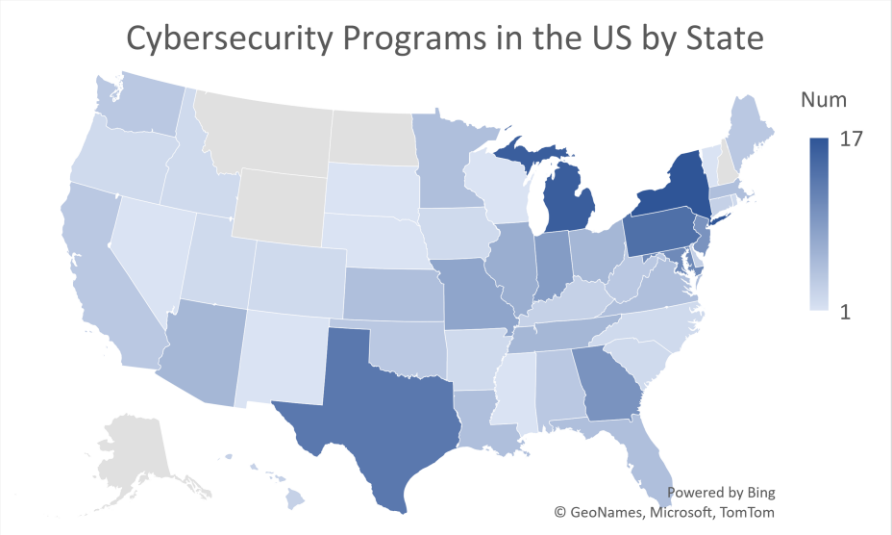

Figure 1: Cybersecurity Programs in the US by State

Both lists were combined to randomly select 30 undergraduate programs for review. The programs were selected by generating a random number for each program and sorting by the randomly generated number. The programs were randomly sorted three times to ensure the randomness of the selection. Although not

all states were represented by the 30 selected programs, all regions of the country were as shown in Figure 2.

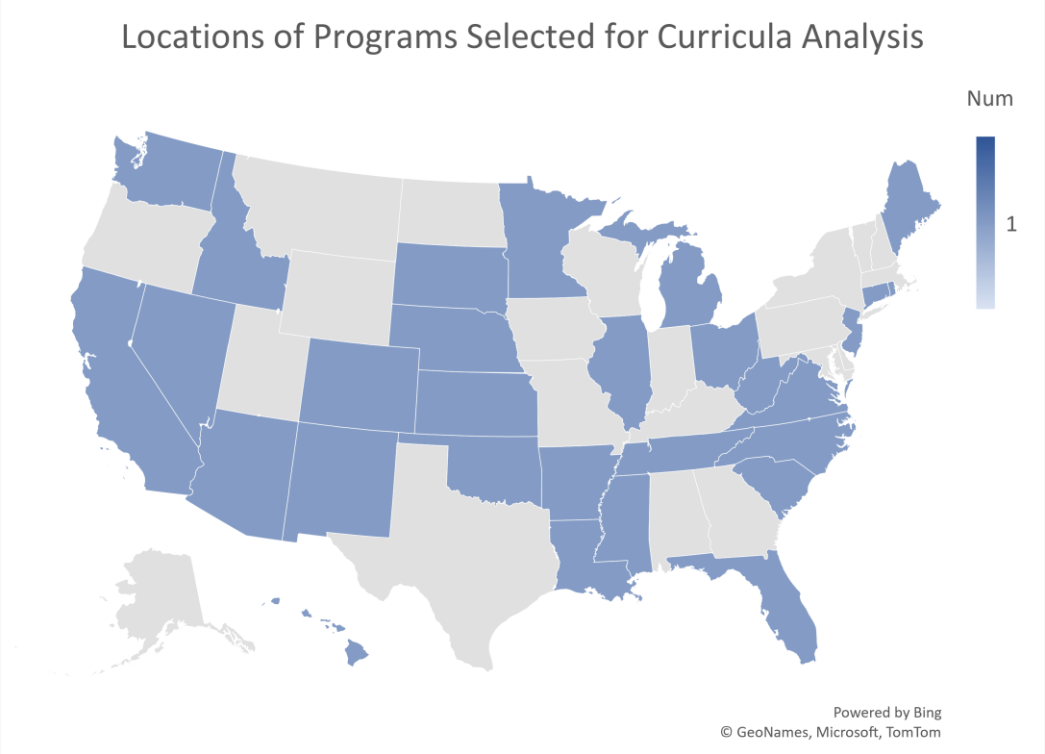

Figure 2: Locations of Programs

The courses specific to degree not including the General Education courses were copied and pasted into a Microsoft Word file without reference to the University or College or the location. Any mention that may have informed the readers of the program's location or site was removed from the course descriptions to prevent bias on the part of the evaluators.

Position Classification and Category Descriptions

Cybersecurity is a diverse, wide-ranging discipline, which can be divided into a variety of sub-fields of specialty areas without a widely adopted formal categorization and definition of sub-fields in the discipline. The identification and delineation of sub-fields in cybersecurity continue to be an active area of research and development (Petersen et al., 2020) Ramezan (2023) created a listing and description of the classification categories used in this analysis for their analysis.

To maintain some consistency in study, this same table is repeated in Table 1 and is used for this study. Ramezan (2023) assigned job postings to a specific category based upon the responsibilities outlined within the job description. In cases where a job description contained responsibilities that would fall under multiple categories, the category which best described a majority of the position's duties was assigned. This study used the same process.

Table 1: Sub-Field Categories and Description (repeated from Ramezan (2023))

Job Classification Category	Description
Architecture	Design, development, and implementation of information security systems, security architectures, network configuration, firewalls, access control lists, network management, system security engineering, system administration, management of identity and access management systems.
Auditing	Specifically relating to either internal or external information technology (IT), information security (IS) or organizational cybersecurity auditing.
Education	Formal cybersecurity educator positions at either private sector training organizations, secondary education, or higher education. Higher education cybersecurity research, service, or teaching faculty.
Governance, Risk, Compliance (GRC)	Risk management, risk assessment, IT governance, compliance, and privacy. Policy development, controls assessment, security awareness training development and implementation, disaster recovery and business continuity planning.
Management	C-Suite, Director of Information Security, senior managers, cybersecurity project managers, positions where primary responsibility entails supervision of personnel and cybersecurity teams.
Operations	Security operations, security analytics, log analysis, digital forensics, blue team, vulnerability and incident management, network, systems, and application scanning.
Penetration Testing	Penetration testing, ethical hacking, red team, vulnerability assessment, web application testing.
Software Security	DevSecOps, software development, software testing, application design, software development life cycle, security tool development. Positions which have a heavy emphasis on application development, coding, programming, incorporating secure by design principles, code reviews, software security assessment.
Threat Intelligence / Research	Collection, analysis, and reporting of cybersecurity threats, vulnerabilities, intelligence, and technologies. Tracking adversary

Position Description-Data Analysis

All job postings were inspected by a text processing algorithm written in R, extracting the position title, location, required qualifications, preferred qualifications, and experience required. One hundred randomly selected positions from each year were examined manually by three separate people to validate the algorithm's performance and reliability as manual analysis is suitable method to validate machine learning and text analysis algorithms. (Ramezan, 2023)

The study also used the data extraction process described by Ramezan (2023) to establish the criteria. For example, the minimum experience required for the position was recorded for the lowest educational attainment required. For example, if a position required 1-2 years of professional experience at the bachelor degree level, then one year of required professional experience was recorded for that position.

Curricula Analysis

In order to develop a thriving workforce based on education requirements from the industry, degree program analyses are essential. Carnevale et al. (2010) mentioned that examining current postsecondary offerings shows whether existing degree programs meet the growing industry demand. The authors emphasize the fact of the dynamic relationship between academia and industry; postsecondary education demands derive from professional growth in an industry. This approach was supported in Fletcher et al. (2015), Fletcher et al. (2017), and Assael (2017). For this study, 30 program were examined. Their courses were evaluated and checked for evidence for both technical and non-technical skills identified from the position analysis. While it would be ideal to measure the strength of the curricula, the purpose of this study

is simply to determine how many of the tops skills were addressed as part of the academic program. Course descriptions including learning objectives were read and evaluated by two separate faculty members. Evaluators were provided the list of top technical and non-technical skills along with the type of terms to search for in the descriptions. While some terms are fairly straightforward, particularly for the technical skills, soft skills development and identification were more difficult. For example, for communication they were asked to look for evidence of group activity in the course learning objectives as well as the course description. If there was confusion or disagreement that a skill was covered, a third faculty member evaluated the course or courses. The third evaluation became the final decision.

Results

Position Analysis

Of the positions analyzed for 2019, 95237 of the positions required a bachelor's degree, 19001 required a Master's degree, and 45897 required one year or less of prior experience. In 2022, 125338 required a bachelor's degree, 22012 a Masters, and 51261 required one year or less of prior work experience. Those positions requiring a bachelor's degree and one year or less were examined further for comparison of skills as they are the closest to the type of positions most recent graduates would be qualified for.

Table 2: Positions Based on Educational Requirements

Minimum Education/Year	2019		2022	
	Number	Percent	Number	Percent
High School	17	0.01%	13	0.01%
Associate/Technical	303	0.26%	398	0.27%
Bachelors	95237	83.00%	125338	84.00%
Masters	19001	16.56%	23312	15.62%
Doctorate	185	0.16%	151	0.10%

Table 3: Positions Based on Educational Requirements and one year or less of related work experience

Minimum Education/Year	2019		2022	
	Number	Percent	Number	Percent
High School	0	0.00%	0	0.00%
Associate/Technical	0	0.00%	0	0.00%
Bachelors	57142	90.4%	75203	91.1%
Masters	5890	9.3%	7227	8.7%
Doctorate	168	0.03%	137	0.2%

Of those positions requiring one year or less of work experience, the most frequent desired degrees were Computer Science, Management Information Systems, Computer Engineering, Cybersecurity, and Information Security as shown in Table 4. The degree frequency did not change much percentage wise between years. Computer Science remains the top required degree followed by Cyber Security and Information Security. Management Information Systems and Computer Engineering complete the top five but both are mentioned less than 50%.

Table 4. Degree Frequency*

Degree	2019		2022	
	Number	% of Total	Number	% of Total
Computer Science	39959	69.93%	49111	65.30%
Cyber Security	38262	66.96%	46019	61.19%
Information Security	37523	65.67%	46361	61.65%
Management Information Systems	27068	47.37%	35645	47.40%
Computer Engineering	19013	33.27%	24809	32.99%
Information Assurance	18674	22447	32.68%	29.85%
Information Technology	2804	3148	4.91%	4.19%
Computer Forensics	1812	1785	3.17%	2.37%
Systems Engineering	1084	1162	1.90%	1.55%
Electrical Engineering	784	841	1.37%	1.12%
General Engineering	398	784	0.70%	1.04%
Mathematics	192	702	0.34%	0.93%

** Totals do not match degree total as many positions listed more than one degree they would accept.The top five degrees constituted more than 80% of the required degrees for both years, indicating no change between 2019 and 2022.*

The most frequently required skills found in both 2019 and 2022 are listed in Table 5. Top Ranked Skills for 2019 and 2022. Communication skills ranked high for both 2019 and 2022 as did knowledge of programming languages, hands-on experience with incident response and vulnerability management, and knowledge of cyber threats. In 2022, relationship building, teams, analytical skills, organizational skills and the ability to work independently appeared more often in position descriptions than in 2019 indicating a stronger emphasis on "soft skills" in 2022. Also, while they were not skills appearing in 2019 position descriptions, knowledge of robotics process automation (RPA) and artificial intelligence (AI) techniques appeared in approximately 15% of the position descriptions in 2022, primarily as preferred skills. Although 2020 and 2021 are not part of this analysis, both RPA and AI appeared in 2020 and 2021 at 5% and 7% respectively as preferred skills, indicating companies are beginning to consider both tools as necessary for cybersecurity professionals.

Table 5. Top Ranked Skills for 2019 and 2022

Skill/Year	2019		2022	
	Number	Percent	Number	Percent
Strong communication skills	32481	80%	43412	94%
Knowledge of programming languages	30451	75%	38332	83%
Hands-on experience in incident response, vulnerability management, or related areas.	30451	75%	40179	87%
Knowledge of cyber threats, attack vectors, and TTPs used by threat actors.	28421	70%	41565	90%
Proficiency in using threat intelligence platforms, tools, and technologies.	23143	57%	38332	83%
Knowledge in IT, network and infrastructure, cloud hosting, development frameworks and devops environments	22737	56%	25862	56%

Skill/Year	2019		2022	
	Number	Percent	Number	Percent
Analytical skills with the ability to identify patterns, trends, and anomalies in threat intelligence data	21519	53%	42950	93%
Ability to work independently	20301	50%	40179	87%
Ability to work as part of a team	12180	30%	34637	75%
Organizational skills	12180	30%	25862	56%
Ability to work in a diverse team environment	10150	25%	27710	60%
Able to forge strong, trusting collaborative relationships	4060	10%	24939	54%

Curricula Analysis

As stated earlier, to develop a thriving workforce based on education requirements from the industry, degree program analyses are essential. Carnevale et al. (2010) mentioned that examining current postsecondary offerings shows whether existing degree programs meet the industry demand. The authors emphasize the fact of the dynamic relationship between academia and industry; postsecondary education demands derive from professional growth in an industry. This approach was supported in Fletcher et al. (2015), Fletcher et al. (2017), and Assael (2017).

For this study, 30 program were examined. Their course descriptions and course learning objectives were evaluated and checked for evidence for both technical and non-technical skills identified from the position analysis for 2022. If a skill wasn't found in the course description, program description and program level learning objectives were evaluated to see if such skills were part of the overall curriculum. The 2022 year was used as it is closest to the current employment year. To begin the analysis, the 2022 skills were separated from the comparison list with 2019 and then sorted in ascending order, adding the RPA and AI to the list as they are a growing preferred skills. The results from the analysis are shown in Table 6.

Table 6. Number of Programs Addressing Top and Emerging Skills

Skill	Number	Percent
Analytical skills with the ability to identify patterns, trends, and anomalies in threat intelligence data	30	100%
Artificial intelligence tools for cybersecurity	2	7%
Build strong, trusting relationships	0	0%
Communication skills	30	100%
Diverse teams	5	17%
Experience in incident response, vulnerability management, or related areas.	30	100%
Knowledge in IT, network and infrastructure, cloud hosting, development frameworks and devops environments	30	100%
Knowledge of cyber threats, attack vectors, and TTPs used by threat actors.	30	100%
Knowledge of programming languages	30	100%
Organizational skills	0	0%
Robotic process automation	1	3%
Team/group work	30	100%
Threat intelligence platforms, tools, and technologies training	30	100%
Work independently	15	50%

All programs evaluated covered all the technical skills. The programming language requirement ranged from "low-code" options to required programming courses in Python, Javascript or similar languages. Evidence of communication skills were found in learning objectives such as "Communicate results to diverse audiences". Evidence of diverse teams were found in program descriptions that included program learning objectives such as "respect for diverse perspectives". Evidence of trusting relationships and organizational skills were not explicitly found in any program description, learning objective, program outcome or course description. Two programs have an elective that includes RPA and one program has a required course in Applied AI.

The major recommendation emerging from this analysis would be for academic program managers be explicit in their course learning objectives or program descriptions about developing the students' soft skills while measuring the "strength" of the curriculum in meeting the technical skills. For example, a program may provide training in network and infrastructure but not cloud hosting. Likewise, some programs provide a course in applications development methodologies whereas some programs only cover applications development as a topic in a course. Some programs offer multiple courses on threat intelligence platforms and tools and some only offer only one.

What programs are able to offer appear to depend heavily on the General Education program for the college or university. Some programs had as many as 45 general education requirements while some had as few as 30. Some programs were explicit in the general education requirements that specifically minimized the number of General Education courses needed by (1) specifying specific General Education courses students needed to take and combining courses that would count for more than one General Education area, allowing for additional courses to be completed for the program without exceeding the 120 credit limit.

Discussion

The purpose of this study was to determine how cybersecurity positions for entry level positions have changed after the COVID pandemic, and how well cybersecurity academic programs are meeting the current entry level position expectations. This analysis was conducted because of the change in the workplace from primarily onsite to a higher number of remote workers which makes the security role more challenging to manage.

The analysis showed that the bachelor degree is the main degree that allows new graduates to enter the cybersecurity field without or with minimum experience. Despite low unemployment, organizations have not begun to rely on associate degrees or lower with no experience like some areas in IT such as RPA, software development and network management. However, the entry level positions also do not require industry certifications yet. This may change now that ISC^2 is now offering an entry level certification for people without experience in the field. Faculty and academic program managers will need to examine position descriptions regularly or speak with industry professionals to determine if the new offering will become a required or preferred qualification and to determine where and when to enter the certification option into the curriculum.

The position description changes show an increase in emphasis on soft skills as well as stronger emphasis on technical skills. Emerging skills include AI tools and RPA skills. Cybersecurity training programs are meeting the expectations well but varying degrees of strength. Low-code is an emerging skills with the programming expectation, as is specific development methodologies such as scrum and agile. Secure development methodologies knowledge also increased between 2019 and 2022. These nuances indicate that

while this analysis showed a national view, it is important that institutions analyze the position descriptions for their region and compare their industry skill needs with their respective curriculum.

Limitations, Conclusions and Next Steps

This study examined cybersecurity positions in 2019 and 2022 for entry level positions from a national view and found that the top skills between the years did not change much but the emphasis on the skills did for both technical and non-technical qualifications. However, this study provided a national view rather than a regional view which is a major limitation as most cybersecurity bachelor programs are offered by regional comprehensive institutions of higher education. Further, the position descriptions are from one source: indeed.com. It would have been helpful to have multiple sources of position descriptions as indeed.com is owned by a Japanese company and some companies may not post on it because of its international ownership. Also, most of the companies that do advertise on indeed.com tend to be larger companies which means this analysis is missing smaller companies that might advertise locally through social media, local newspapers and other job boards. Therefore, the voices of smaller firms may be missing from the analysis which is needed to ensure the program is meeting the needs of all firms, not just large ones.

The next steps in this research are to add the industry professional voice to the study as well as conduct analysis at regional levels, comparing position descriptions for two or more regions to determine how different programs are meeting their local needs. Future studies might also examine faculty skills to match for industry demands for teaching a higher ed cyber security program. Such studies are needed because many programs follow a national accreditation model such as ABET which may not necessarily meet the needs of local businesses as well as a more customized program might.

References

2023 global threat report. Crowdstrike. (2022). https://go.crowdstrike.com/2023-global-threat-report.html

Ahsan, K., Ho, M., & Khan, S. (2013). Recruiting project managers: A comparative analysis of competencies and recruitment signals from job advertisements. Project Management Journal, 44(5), 36-54.

Assael, L. (2017). Current status of postdoctoral and graduate programs in dentistry. Journal of dental education, 81(8), eS41-eS49.

Association for Computing Machinery. (2017). Cybersecurity curricula 2017 - Association for Computing Machinery. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Bicak, A., Liu, X. M., & Murphy, D. (2015). Cybersecurity curriculum development: introducing specialties in a graduate program. Information Systems Education Journal, 13(3), 99.

Booker, Q., & Munmun, M. (2022). Industry RPA Demands and Potential Impacts for MIS and Related Higher Education Programs.

Brooks, Greer, T. H., & Morris, S. A. (2018). Information systems security job advertisement analysis: Skills review and implications for information systems curriculum. Journal of Education for Business, 93(5), 213–221. https://doi.org/10.1080/08832323.2018.1446893

Carnevale, A. P., Smith, N., & Strohl, J. (2010). Help wanted: Projections of job and education requirements through 2018. Lumina Foundation.

Carnevale, A. P., Smith, N., & Strohl, J. (2013). Recovery: Job growth and education requirements through 2020.

Carnevale, A. P., Jayasundera, T., & Repnikov, D. (2014). Understanding online job ads data. A technical report. MS o. PP Center on Education and the Workforce. https://cew.georgetown.edu/wp-content/uploads/2014/11/OCLM.Tech_.Web_.pdf

Criteria for accrediting computing programs - abet.org. (2021). https://www.abet.org/wp-content/uploads/2022/03/2022-23-CAC-Criteria.pdf

Cybersecurity.com (2023) https://cybersecurityguide.org/programs/cybersecurity-bachelors-degree/#Schools Accessed 30 May 2023.

Debuse, J., & Lawley, M. (2009). Desirable ICT graduate attributes: Theory vs. practice. Journal of Information Systems Education, 20(3), 313.

Diamond, K., Pierce, D., Johnson, J., & Ridley, M. (2014). Content analysis of sponsorship sales job postings in the United States. Graduate Journal of Sport, Exercise, & Physical Education Research, 2, 19-36.

Downey, J. P., McMurtrey, M. E., & Zeltmann, S. M. (2008). Mapping the MIS curriculum based on critical skills of new graduates: An empirical examination of IT professionals. Journal of Information Systems Education, 19(3), 351.

Fletcher Jr, E. C., Gordon, H. R., Asunda, P., & Zirkle, C. (2015). A 2015 status study of career and technical education programs in the United States. Career and Technical Education Research, 40(3), 191-211.

Fletcher Jr, E. C., & Gordon, H. R. (2017). The status of career and technical education undergraduate and graduate programs in the United States. Peabody Journal of Education, 92(2), 236-253.

Gartner identifies three factors influencing growth in security spending. Gartner. (2022). https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i

Gudigantala, N. (2013). An active learning approach to teaching undergraduate introduction to MIS Course.

Hall, J. L., & Rao, A. (2020, April). Non-Technical skills needed by cyber security graduates. In 2020 IEEE Global Engineering Education Conference (EDUCON) (pp. 354-358). IEEE.

Harper, R. (2012). The collection and analysis of job advertisements: A review of research methodology. Library and information research, 36(112), 29-54.

Harris, Greer, T. H., Morris, S. A., & Clark, W. J. (2012). Information Systems Job Market Late 1970'S-Early 2010'S. The Journal of Computer Information Systems, 53(1), 72–79. https://doi.org/10.1080/08874417.2012.11645599

Harris, M. A., & Patten, K. P. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computic Curriculum. Journal of Information Systems Education, 26(3), 219-234.

Hirudayaraj, M., & Baker, R. (2018). HRD competencies: analysis of employer expectations from online job postings. European Journal of Training and Development
.

Ho, A., Nguyen, A., Pafford, J. L., & Slater, R. (2019). A data science approach to defining a data scientist. SMU Data Science Review, 2(3), 4.

Hunter, G. (2022). How tech hiring is changing. Computer Fraud & Security, 2022(3).

Hwang, D., & Soe, L. L. (2010). An Analysis of Career Tracks in the Design of IS Curricula in the US. Information Systems Education Journal, 8(13), n13.

Liu, X. M., & Murphy, D. (2012). Tackling an IS educator's dilemma: a holistic model for "when" and "how" to incorporate new technology courses into the IS/IT curriculum.

McArthur, E., Kubacki, K., Pang, B., & Alcaraz, C. (2017). The employers' view of "work-ready" graduates: A study of advertisements for marketing jobs in Australia. Journal of Marketing Education, 39(2), 82-93.

Mills, R. J., Chudoba, K. M., & Olsen, D. H. (2016). IS programs responding to industry demands for data scientists: A comparison between 2011 – 2016. Journal of Information Systems Education, 27, 131–141.

Parker, A., & Brown, I. (2019). Skills requirements for cyber security professionals: a content analysis of job descriptions in South Africa. In Information Security: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, Revised Selected Papers 17 (pp. 176-192). Springer International Publishing.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a cybersecurity workforce and aware public. IEEE Security & Privacy, 10(3), 76-79.

Peslak, A., & Hunsinger, D. S. (2019). What is cybersecurity and what cybersecurity skills are employers seeking?. Issues in Information Systems, 20(2).

Ramezan, C. A. (2023). Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field. Journal of Information Systems Education, 34(1), 94-105.

Rosén, E. M. (2014). From ad-man to digital manager: Professionalization through Swedish job advertisements 1960-2010. Journal of Communication Management, 18(1), 16-39.

Stanton, R. (2017). Do technical/professional writing (TPW) programs offer what students need for their start in the workplace? A comparison of requirements in program curricula and job ads in industry. Technical Communication, 64(3), 223-236.

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

Sausalito, C. (2021, November 9). Cybersecurity Talent Crunch to create 3.5 million unfilled jobs globally by 2021. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-jobs-report-2019/

Simons, J. (2018, May 30). It's a good time to find a cybersecurity job. The Wall Street Journal. https://www.wsj.com/articles/its-a-good-time-to-find-a-cybersecurity-job-1527646081

Triche, J. H., Firth, D., & Harrington, M. (2016). A comprehensive framework to enhance the effectiveness of the recruiting experience for data science graduates. Communications of the Association for Information Systems, 39(1), 1.

U.S. Bureau of Labor Statistics. (2022, September 8). Computer and Information Technology Occupations: Occupational Outlook Handbook. U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/home.htm

Verma, A., Yurov, K. M., Lane, P. L., & Yurova, Y. V. (2019). An investigation of skill requirements for business and data analytics positions: A content analysis of job advertisements. Journal of Education for Business, 94(4), 243-250.