Journal of
Information
Systems
Education

Volume 34
Issue 1
Winter 2023

Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field

Christopher A. Ramezan

Recommended Citation: 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.

Article Link: https://jise.org/Volume34/n1/JISE2023v34n1pp94-105.html

Received:	January 25, 2022
Revised:	May 2, 2022
Accepted:	June 6, 2022
Published:	March 15, 2023

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

Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field

Christopher A. Ramezan
Department of Management Information Systems
West Virginia University
Morgantown, WV 26508, USA
cramezan@mail.wvu.edu

ABSTRACT

While demand for cybersecurity professionals is high, the field is currently facing a workforce shortage and a skills gap. Thus, an examination of current cybersecurity position hiring requirements may be advantageous for helping to close the skills gap. This work examines the education, professional experience, industry certification, security clearance, and programming skill requirements of 935 cybersecurity positions categorized by sub-field. The nine sub-fields are: architecture, auditing, education, GRC (governance, risk, and compliance), management, operations, penetration testing, software security, and threat intelligence / research. Prior work experience and higher education degrees in technical fields were found to be frequently required across all sub-fields. Over 48% of positions listed an industry cybersecurity certification, while 19% of positions required a security clearance. In addition, 25% of positions listed knowledge of a programming language as a requirement for employment. There were notable differences in certain position requirements between sub-fields. On average, management positions required three years of additional work experience than positions in the auditing, operations, and penetration testing sub-fields. Security clearance requirements were relatively similar across all other sub-fields, with the GRC sub-field having the highest percentage of positions requiring a security clearance. Programming skills were desired most prevalently in positions within the architecture, software security, and penetration testing sub-fields. Demand for industry certifications varied by sub-field, although the Certified Information Systems Security Professional (CISSP) certification was the most frequently desired certification. Cybersecurity education programs should consider the diverse nature of the cybersecurity field and develop pathways to prepare future cybersecurity professionals for success in any sub-field.

Keywords: Employment skills, Job skills, Cybersecurity, IT professional

1. INTRODUCTION

As of 2021, cybersecurity is one of the fastest growing occupational fields in the United States. According to the U.S. Bureau of Labor Statistics, the projected job growth outlook for information security analysts is 31% between 2019-2029, the highest growth percentage of all occupation subcategories in the Computer and Information Technology occupations category, and seven times faster than the average U.S. job growth rate in 2021 of 4% (U.S. Bureau of Labor Statistics, 2021). Another report by Cybersecurity Ventures anticipates that in 2025, there will be a predicted 3.5 million unfilled cybersecurity positions worldwide (Morgan, 2021). Given the recent widespread attention to cybersecurity issues through massive ransomware attacks such as the Colonial Pipeline incident and the JBS ransomware attack (Erickson, 2021), the demand for qualified cybersecurity professionals is expected to continue to increase.

Although the demand for cybersecurity professionals is high, the cybersecurity field is currently facing a labor shortage and a skills gap (Caldwell, 2013; Cobb, 2018; Crumpler & Lewis, 2019; Vogel, 2016). According to ISACA's State of Cybersecurity 2021 research, which surveyed cybersecurity professionals across the globe in a wide variety of industries, 61% of survey respondents indicated that their cybersecurity teams are understaffed, while 44% of respondents said that it takes their organization between 3-6 months to acquire talent for unfilled cybersecurity positions (ISACA, 2021). While there are a variety of factors that may be contributing to a clogged cybersecurity talent pipeline, one of the most frequently mentioned challenges to cybersecurity job recruitment are position qualification requirements such as education, professional experience, technical skills, and industry certifications (Markow et al., 2019).

In addition to professional, skills, and academic requirements, many United States government and federal contractor cybersecurity positions often require prospective applicants to possess and maintain an active U.S. security clearance. Previous research (e.g., Wilson & Wilson, 2011) has shown that security clearance requirements may exclude qualified and talented cybersecurity professional applicants who have not had the opportunity to obtain a clearance, creating a hiring barrier for clearance-required positions.

Given the current skills gap and demand for the cybersecurity domain, an in-depth analysis of the requirements of current cybersecurity job postings would be beneficial for informing higher education and training programs on preparing the cybersecurity workforce to best meet the qualification demands of the industry as part of an effort to reduce the current cybersecurity skills gap. In addition, this analysis would also be useful for cybersecurity job seekers by providing insights on education, experience, programming skills, and clearance requirements for a variety of positions in the cybersecurity field.

2. LITERATURE REVIEW AND AIMS

Previous studies that have examined cybersecurity job descriptions suggest that cybersecurity positions list various pre-requisite qualifications, such as formal education, technical skills, professional experience, and industry certifications. For example, a study by Peslak and Hunsinger (2019) which analyzed 487 cybersecurity analyst positions, found that professional experience and a higher education degree were commonly required in the information security field. In addition to formal education requirements, industry certifications were also found to be a common listing on Cybersecurity Analyst job descriptions. A similar study by Marquardson and Elnoshokaty (2020) also found that industry certifications, experience, and higher education degrees were typical for a variety of entry-level cybersecurity positions. Parker and Brown (2019)'s analysis of cybersecurity job descriptions in South Africa found similar requirements as well.

While many of these studies are useful for gaining insights into the cybersecurity job market, previous investigations have either focused on analyzing job requirements of a single cybersecurity position type, such as Cybersecurity Analyst or Cybersecurity Architect (Marquardson & Elnoshokaty, 2020; Peslak & Hunsinger, 2019), or a generalized search of cybersecurity positions (Brooks et al., 2018). Although investigations on a single or few cybersecurity job titles can be useful, they may limit insights into the cybersecurity job market. Cybersecurity is a broad field with a wide variety of positions that may require expertise, experience, or knowledge within in a specific sub-field or domain of the cybersecurity field. For example, positions with job titles similar to "Information Security and Compliance Manager" and "Information Security Analyst" would both be considered cybersecurity positions, but require vastly different skillsets, with the former position likely requiring in-depth knowledge of risk management and regulatory compliance frameworks, project management, and organizational management, while the latter position would likely require deep technical expertise and familiarity with security operations, tools, and practices. Thus, analyses that focus on analyzing the position requirements of a singular job role or title may be providing insights on a single type of position, rather than the cybersecurity field in general, which constitutes an assortment of positions with a wide variety of roles and responsibilities.

An additional concern in conducting analyses of cybersecurity job descriptions based on position title is the non-standardized usage of position titles within the industry. For example, the generalized title of "Information Security Officer (ISO)" in one organization may be a management-focused position, where the position calls for the leadership of organizational cybersecurity operations and leading cybersecurity personnel. In another organization, the ISO position could be more of an applied role, where the ISO works within an information security team or department as part of a security operations center (SOC), or part of an engineering or systems administration team responsible for designing and managing secure network architectures. While the position title may be identical, the job responsibilities, area of expertise, and qualifications of ISOs in different organizations are likely vastly different. This phenomenon could lead to complications in analyses that attempt to provide insights on a single type of cybersecurity position based on position title.

In contrast, using generalized search terms which can capture a wide variety of cybersecurity positions would be advantageous for examining position requirements across the cybersecurity field. This method was used in an analysis by Brooks et al. (2018), who analyzed 30 discrete cybersecurity job titles acquired through a generalized search query. However, when conducting a broader analysis of cybersecurity positions using generalized search parameters, careful attention should be given to the diverse breadth of positions that exist in the cybersecurity field. For example, while a systems security architect and an application penetration tester would both be considered cybersecurity positions and may both be listed within a generalized search query of cybersecurity positions, in reality, these roles are very different, would likely have highly different job requirements and belong to different sub-fields within the cybersecurity discipline. Due to the complexity, diversity, and broad range of positions within the cybersecurity field, classifying positions based on their duties and responsibilities into defined and unique sub-field categories, instead of a single broad "cybersecurity" category may give additional insights into various types of cybersecurity positions, as well as better insights on the cybersecurity field in general, as these categories may capture additional insights on some of the nuances within the cybersecurity discipline.

Thus, this paper seeks to expand upon previous analyses of cybersecurity job requirements by categorizing cybersecurity positions into discrete subfield categories based on the job description and responsibilities listed rather than by the position title as part of a granular analysis of cybersecurity job requirements across the diverse breadth of the cybersecurity field.

This work aims to provide insights on the following prerequisite or desired requirements for professional positions within the cybersecurity field:

1. Education – (Secondary education, higher education degrees, vocational and skills training).
2. Experience – (Professional experience acquired through previous employment, projects, and internships).
3. Certifications – (Vendor-neutral and vendor-specific industry cybersecurity and information technology certifications such as the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), CompTIA Security+ (Sec+), Cisco Certified Network Associate (CCNA), Certified Ethical Hacker (CEH), Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified Public Accountant (CPA), Certified Information Privacy Technologist (CIPT), Certified in Risk and Information Systems Control (CRISC), Global Information Assurance Certification (GIAC), GIAC Security Leadership (GSLC), Offensive Security Certified Professional (OSCP), GIAC Penetration Tester (GPEN), Offensive Security Certified Expert (OSCE), Project Management Professional (PMP), CompTIA Advanced Security Practitioner (CASP+), GIAC Certified Incident Handler (GCIH), and others).

4. Clearance – (Possession of a United States (U.S.) government security clearance).
5. Programming skills – (Knowledge of specific programming languages).

3. DATA AND METHODOLOGY

Job posting data were acquired from Indeed.com. Job aggregator websites such as Indeed.com can be particularly useful for acquiring job description postings in a particular field of interest. Indeed.com was chosen as it is a highly popular job aggregator and was used by similar analyses of jobs postings in other fields, such as data scientists (Ho et al., 2019), data analytics (Verma et al., 2019), artificial intelligence and machine learning (Verma et al., 2022), human resource analytics (Kapoor & Kabra, 2014), and human resource management (Goldberg & Zaman, 2018). While Indeed.com's job postings are publicly accessible, permission was granted by Indeed.com to use their data in this analysis for academic research purposes. A workflow of the data acquisition, position classification, and information extraction methods can be seen in Figure 1. Further explanations of methods are provided in detail within the following sections.

3.1 Data Acquisition and Cleaning

A job search query was conducted on Indeed.com on June 18th, 2021, using two search parameters: "Cybersecurity" and "Information Security." No location information was specified in the location parameter within the search queries, however, it is possible that IP address localization was used by the search, as only job postings within the United States were returned.

In total – 19,109 jobs were listed between both queries. A random sample of 1,253 job postings was captured between both queries. The initial sample size of 1,253 was limited by the number of positions captured before the web query timed out. As Indeed.com generates unique static URL links to each job posting page, the URL link, position title, salary, and position summary were captured and saved in a database using a Python3 script. Each posting was then individually inspected. Out of 1,253 postings, 279 were found to be duplicate job postings and were removed. Through inspection of the remaining job descriptions, an additional 39 postings were removed. Also, 29 of these positions contained the keywords "Cybersecurity" or "Information Security" but were not cybersecurity positions. A select few examples of these positions were: Principle UX Designer marketing cybersecurity software, Sr. Geospatial Architect, Laboratory Information Specialist, Intellectual Property/Cybersecurity Lawyer, and Cybersecurity Journalist/Reporter. Two of the postings were cybersecurity higher education graduate school program advertisements, and the remaining eight postings were cybersecurity-related jobs, however, these postings did not contain any information and had corrupted or invalid external links. After removing these postings, a total of 935 unique postings remained for further analysis.

3.2 Position Classification and Category Descriptions

To provide a more granular analysis of position requirements for different types of jobs within the cybersecurity field, each job posting was individually inspected and assigned to one of nine discrete categories by the author. While cybersecurity is a diverse, wide-ranging discipline, which can be divided into a variety of sub-fields of specialty areas, it should be noted that as cybersecurity is a relatively young field of study, there has yet to be 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).

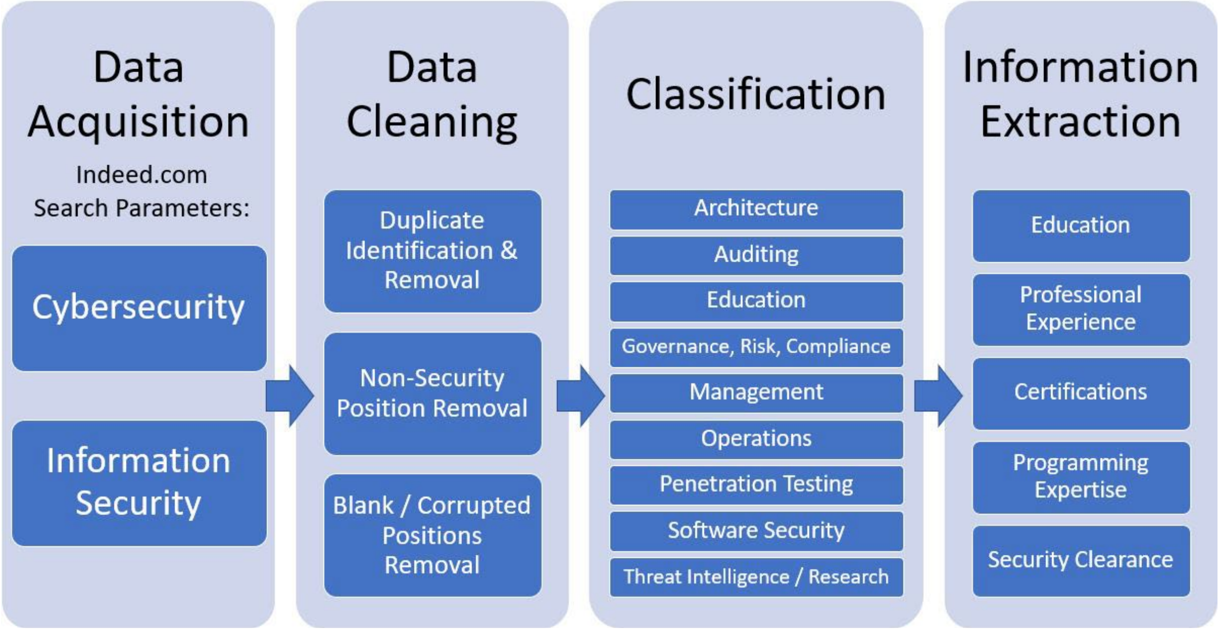

Figure 1. Methodology Workflow

While frameworks for the cybersecurity workforce and sub-fields such as the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework have been proposed to the cybersecurity community, these frameworks continue to be in development as the discipline matures (Newhouse et al., 2017; Petersen et al., 2020).

As there is a current lack of consensus on formally delineated sub-fields within the cybersecurity discipline, the sub-fields identified in this analysis were in-part designed to capture the breadth and diversity of common major domains within the cybersecurity discipline, into broad, discrete categories, some of which are seen in other proposed cybersecurity sub-field frameworks (Newhouse et al., 2017).

A listing and description of the classification categories used in this analysis can be found in Table 1. Job postings were assigned 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.

An example of this situation would be an Information Security Analyst position whose responsibilities include conducting vulnerability scans, conducting log analysis, monitoring the organization's network for malicious activity, and developing internal security policy to maintain compliance with external industry standards. Although one of the position's responsibilities falls under the "governance, risk, and compliance (GRC)" categories, a majority of the job responsibilities fall under the "operations" category. Thus, the position would be classified as an operations position as most of the responsibilities fall under that category. Each job posting was carefully inspected to ensure the best fit to the appropriate category.

3.3 Information Extraction

All 935 job postings were individually inspected by the author over the course of three weeks. To avoid potential issues with fatigue, information extraction and classification processes were limited to approximately 50–70 positions daily during the analysis period. Several information fields were extracted from each job description, including: Position title, company name, location, salary, security clearance requirement, education level, professional experience, certifications required, certifications preferred, programming languages, and a brief position summary. While automated text analysis and machine learning classification methods were considered for use, manual analysis was determined to be a feasible and suitable method, given the size of the dataset. Automated methods such as text analysis and machine learning classifiers may be more suitable in future analyses incorporating larger datasets.

As job description language and formats wildly varied, to ensure the standardization of the information extraction process, several rules were set up to guide the information extraction process. Regarding experience, the minimum experience required for the position was recorded. For example, if a position required 1-2 years of professional experience, one year of required professional experience was recorded for that position. If the professional experience requirement varied depending on educational level (high school, bachelor's, master's, doctoral), the required professional experience was recorded at the bachelor's degree level. In addition, as several positions listed multiple levels of security clearance, the minimum security clearance required to obtain the position was recorded as the security clearance level required for that position. For example, if a position required active "Secret" security clearance upon employment, but an active "Top Secret SCI" clearance was preferred, the clearance level for that position was recorded as "Secret."

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 groups, threat hunting. Non-academic applied or theoretical cybersecurity research positions.

Table 1. Sub-Field Categories and Descriptions

4. RESULTS

Of the 935 positions analyzed, 917 required at least one of the five prerequisites examined in this analysis (educational degree, prior professional experience, industry certification, security clearance, or expertise with a programming language). The remaining 18 postings provided a description of the position but did not include any specific pre-requisite requirements for employment. Only 22% of postings included a prospective salary or salary range. Due to the limited information on position salaries in this dataset, further analysis on position salaries was not explored in this study.

4.1 Position Type and Geographic Distribution

The largest three-position type categories were architecture, operations, and GRC, respectively. When combined, these three position categories comprised 79.5% of the dataset. Management was the next largest position category comprising 5.3% of the dataset. The remaining position categories comprised less than 5% of the dataset, with the smallest categories being auditing, with 9 positions making up roughly 1.0% of the dataset, and education, with 11 positions, comprising 1.2% of the dataset. Figure 2 shows the percentage of positions in the dataset belonging to each sub-field.

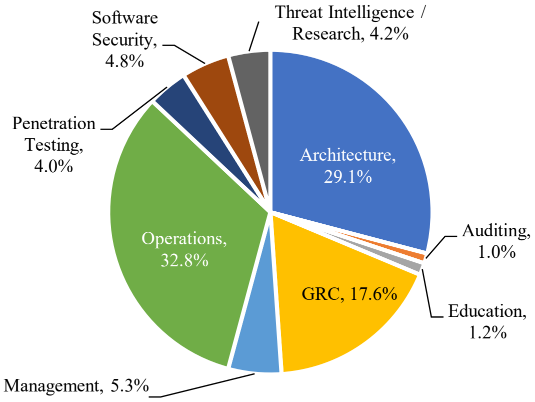

Figure 2. Percentage of Analyzed Positions by Sub-Field

Of the positions analyzed, 756 out of 935 (80.9%) included location information within the job posting. The geographic distribution of job postings in this analysis can be seen in Figure 3. The states with the highest concentrations of positions captured in this analysis were Virginia, California, Washington D.C., Maryland, Texas, and New York. Positions were located in every U.S. state, except for North Dakota, South Dakota, Louisiana, Mississippi, Kentucky, and Maine. Two positions were also located within the U.S. territory of Puerto Rico. Notably, 46 positions listed their location as "United States" or "USA" and did not list a specific location. Furthermore, 14.2% of all positions (133 positions) were listed as fully remote opportunities, with no specific work location assigned to the position. A possible explanation for a large number of remote positions in this dataset could be the ongoing COVID-19 pandemic (Watson et al., 2020).

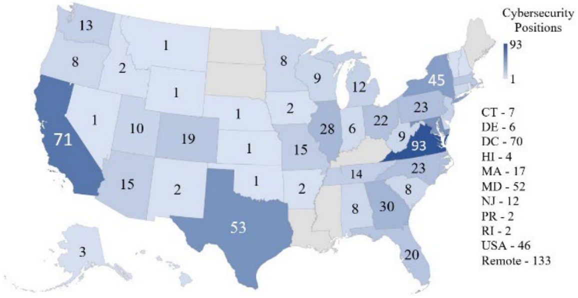

Figure 3. Geographic Distribution of Cybersecurity Positions

4.2 Education

Listed educational requirements by job category are shown in Table 2. Out of the 935 positions surveyed, 71% listed an education requirement, while 69% of jobs required a higher education degree (bachelor's, master's, or doctoral). Of the 663 positions that did list an education requirement, 93.8% listed a bachelor's degree, 17.8% listed a master's degree, and 4% listed a doctoral degree. High school diplomas were listed in 2.41% of positions which included an educational requirement.

Positions in auditing and education had the highest education requirements. However, the sample sizes of these categories were relatively small. Over 70% of positions in the architecture, GRC, operations, and penetration testing categories listed an educational requirement. The percentage of positions listing an educational requirement was slightly lower in the management, software security, and threat intelligence/research categories. Paradoxically, over 20% of all positions in the management, software security, and threat intelligence/research categories listed a master's degree, a higher percentage than the architecture, GRC, operations, and penetration testing sub-fields. Positions listing doctoral degrees were relatively rare, apart from the education category, where a doctorate was listed on 54.5% of positions, and in the threat intelligence/research category, which listed a doctoral degree on 10.3% of positions. Furthermore, 6.0% of management positions listed a doctoral degree as well. All other sub-fields only mentioned a doctoral degree in 3.0% or fewer positions.

By major, computer science was the most common degree, listed in 43.7% of positions requiring a degree. Notably, 38.9% of positions that listed a higher education degree requirement did not specify a specific major or field of study. Information systems or management information systems (MIS), and engineering were the second and third most popular degrees, listed on 25.2% and 25.0% of positions, respectively. Technology was listed as a desired or required major in 14.8% of positions, while a major in cybersecurity was listed in 10.3% of positions. Other prominent majors were computer engineering at 7.8%, information security at 6.5%, electrical engineering at 4.2%, business at 3.9%, and information assurance at 3.0%. Other fields such as mathematics, computer information systems (CIS), software engineering, systems engineering, accounting, data science, and statistics were also listed on less than 3.0% of positions.

	High school diploma	Associate's	Bachelor's	Master's	Doctoral	Positions listing education requirement	Total number of positions
Architecture	2.6%	2.9%	66.2%	14.7%	2.9%	71.7%	272
Auditing	0.0%	0.0%	88.9%	33.3%	0.0%	88.9%	9
Education	0.0%	0.0%	90.9%	72.7%	54.5%	90.9%	11
GRC	1.2%	2.4%	69.1%	9.7%	1.8%	72.7%	165
Management	0.0%	0.0%	66.0%	20.0%	6.0%	66.0%	50
Operations	2.0%	4.2%	66.4%	6.2%	0.3%	72.6%	307
Penetration Testing	2.7%	0.0%	64.9%	10.8%	2.7%	70.3%	37
Software Security	0.0%	0.0%	55.6%	22.2%	2.2%	55.6%	45
Threat Intelligence / Research	0.0%	0.0%	61.5%	20.5%	10.3%	61.5%	39

Table 2. Percentage of Cybersecurity Positions Listing a Degree by Sub-Field

Across all subfield categories, computer science, engineering, and information systems/MIS were the most frequently listed majors. Computer science was the most frequently listed major for all sub-fields except for the auditing and education sub-fields. Information systems/MIS was the second most frequently listed major for the architecture, GRC, management, and operations categories, and was the most frequently listed major for the auditing subfield. Information technology (IT), cybersecurity, and engineering were also among the top five listed majors for all subfields.

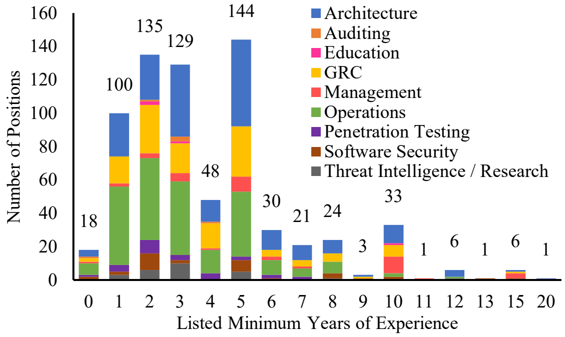

Figure 4. Distribution of Cybersecurity Positions by Listed Minimum Years of Required Experience

4.3 Experience

Of the analyzed 935 positions, 791 (84%) included a professional experience requirement. Also, 91 of the 791 positions listed an experience requirement but did not specify a numeric amount of required or desired experience. Experience requirements in years ranged from 0–20. Nearly 82% of positions that listed a numeric experience requirement required five years or less experience. In addition, 54% of positions required three years or less experience, while 36% of positions required two years or less. Also, 18 positions specifically listed 0 years of prior professional experience. On the higher end of professional experience requirements, 18% of positions listed six years or more professional experience, while 6% of positions required ten years or more. A majority of the positions that required ten years or more experience were generally within the architecture and management sub-fields. The highest recorded job experience requirement was a position in the architecture category, a Senior Information Systems Security Engineer, which required 20 years of prior professional experience. The number of positions listing various minimum years of experience as a requirement is in Figure 4.

Of the 700 positions that listed a numeric experience requirement, positions within the management, architecture, and software security categories had, on average, higher professional experience requirements, in terms of years required, than auditing, education, GRC, operations, penetration testing, and threat intelligence/research categories. While the management category did not contain the positions with the overall highest years of experience requirements, the category had the highest average required years of experience, at 6.5 years, nearly two years higher than the average years of experience for jobs in the software security category, the second highest category. The distribution of numeric professional experience requirements by subfield can be seen in Figure 5.

4.4 Certifications

Nearly half (48.3%) of surveyed positions included an industry certification within the job posting. Additionally, 21.1% of positions listed a certification as required for employment, while 30.7% of positions listed a certification as preferred. By category, 43.8% of architecture positions, 77.8% of auditing positions, 54.5% of education positions, 63.6% of GRC positions, 46.0% of management positions, 50.8% of operations positions, 59.5% of penetration testing positions, 11.1% of software security positions, and 23.1% of threat intelligence/research positions included an industry certification within the job posting. In total, 135 different certifications were listed across all 935 positions. Figure 6 visualizes all mentioned certifications in a word cloud scaled by frequency of listing.

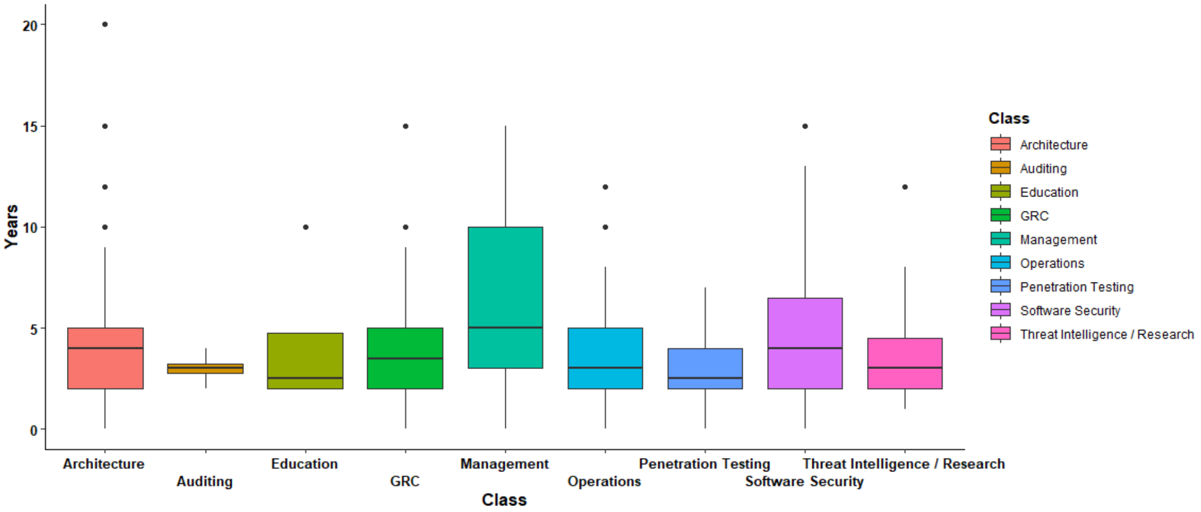

Figure 5. Distribution of Listed Required Years of Experience by Sub-Field

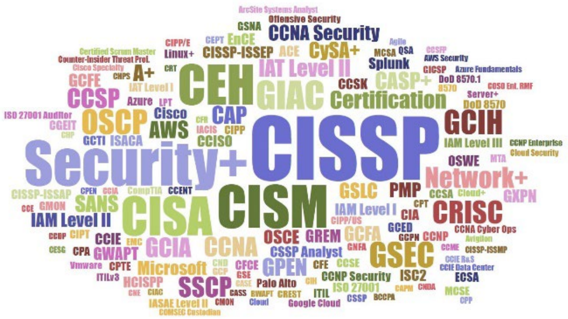

Figure 6. Word Cloud of Certification Listings

The most frequently mentioned certification was the Certified Information Systems Security Professional (CISSP), with 279 individual mentions. The Security+, CISM, CEH, and CISA were also frequently listed, with 133, 124, 108, and 99 mentions, respectively. The CISSP was the most frequently listed certification across all sub-fields, apart from the education and penetration testing sub-fields. The CompTIA Security+ and Cisco Certified Network Associate (CCNA) were the most frequently mentioned certifications in the education category, while the Offensive Security Certified Professional (OSCP) certification was the most frequently listed in the penetration testing category. Table 3 lists the top 5 listed certifications by category.

4.5 Clearance

U.S. security clearances were required for 177 out of 935 (19%) of the total analyzed positions. Notably, top secret sensitive compartmented information (TS/SCI) clearance, one of the highest levels of security clearance, was the most requested clearance, with 49 positions requiring a TS/SCI clearance for employment. Secret clearance was the second most common clearance requirement, listed in 45 positions. In addition, 20 positions required a security clearance but did not specify a specific level of clearance. A variety of clearances were requested across all 177 positions, including area-specific clearances such as Q clearance with the Department of Energy, and Department of Homeland Security (DHS) suitability clearance. By sub-field, clearance requirements were relatively similar, with the GRC sub-field having the highest percentage of positions requiring a security clearance, at 23.6%. The auditing and education sub-fields did not list any positions which required a security clearance. The percentage of positions requiring a security clearance by other sub-fields are

	Ranking by frequency of appearance				
	1st	2nd	3rd	4th	5th
Architecture	CISSP	CISM	Sec+	CEH	CCNA
Auditing	CISA	CISSP	CIA	CPA	CIPT
Education	Sec+	CCNA	CISSP	CEH	CISM
GRC	CISSP	CISM	CISA	Sec+	CRISC
Management	CISSP	CISM	CISA	Sec+	GSLC
Operations	CISSP	Sec+	CEH	GIAC	CISM
Penetration Testing	OSCP	CEH	GPEN	CISSP	OSCE
Software Security	CISSP	CISA	Sec+	PMP	CASP+
Threat Intelligence / Research	CISSP	GCIH	CEH	OSCP	GPEN

Table 3. Frequency of Certification Listing by Sub-Field

as follows: Architecture (18.8%), management (14.0%), operations (18.6%), penetration testing (18.9%), software security (17.8%), and threat intelligence/research (20.5%).

4.6 Programming

Of the 935 analyzed positions, 231 (24.7%) listed a programming language in the job posting. The software security and penetration testing sub-fields had the highest percentages of positions listing a programming language, at 71.1%, and 67.6%, respectively. Additionally, 51.3% of threat intelligence/research positions listed a programming language in the job posting. The other sub-fields mentioned programming languages less frequently. In particular, 32.0% of architecture positions, 11.1% of auditing positions, 6.1% of GRC positions, 2.0% of management positions, and 17.9% of operations positions listed a programming language. The education sub-field was the only category that did not have any positions which listed knowledge of a programming language as a desired or required skill. In total, 27 unique programming languages were listed across all 231 positions. Python was the most popularly listed language, followed by Java and C++. The most frequently mentioned languages listed on five or more positions are listed in Table 4.

Programming Language	Number of positions	% of positions listing a programming language (n=231)
Python	155	67.1%
Java	98	42.4%
C++	52	22.5%
C	48	20.8%
PowerShell	46	19.9%
SQL	45	19.5%
Bash	37	16.0%
Ruby	37	16.0%
Go	37	16.0%
C#	33	14.3%
Perl	30	12.9%
PHP	13	5.6%
HTML	7	3.0%
CSS	6	2.6%
Rust	5	2.2%
R	5	2.2%

Table 4. Frequently Listed Programming Languages

4.7 Education and Certification Position Requirements by Level of Required Experience

As seen in Figure 7, of the 700 positions that listed a numerical experience requirement, the percentage of positions listing an educational requirement generally did not decrease as the minimum experience requirement of positions increased. However, it should be mentioned that 89% of positions that listed 0 years of professional experience, listed an educational requirement, an exceptionally high percentage. The percentage of positions requiring certifications generally increased as the minimum required years of experience increased.

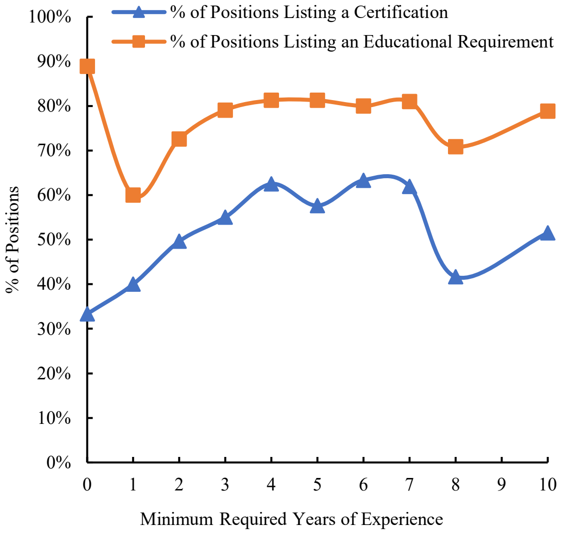

Figure 7. Percent of Positions Listing a Certification or Education Requirement as a Function of Minimum Required Years of Experience (Note these values are from the 700 positions which listed a numerical experience requirement.)

4.8 Requirements of Positions Specifically Listing MIS or Information Systems Degrees

Of the 935 positions analyzed, 167 positions listed a higher education degree in Management Information Systems (MIS) or Information Systems (IS) as a required or desired educational requirement. The sub-fields with the highest percentages of positions listing MIS or IS degrees were auditing at 62.5%, followed by penetration testing at 37.5%, threat intelligence/research at 33.3%, management at 30.8%, GRC at 28.4%, architecture at 25.5%, operations at 25.4%, and software security at 8.0%. No positions in the education category listed an MIS or IS degree as an educational requirement. Regarding certifications, 67.6% of positions listing MIS or IS degree requirements listed an industry certification.

Figure 8 shows the distribution of positions listing an MIS or IS degree with a numerical experience requirement. Notably, over a third of positions (33.5%) required 0-2 years' experience. However, the most frequently listed numerical experience requirement was five years. Only 13.8% of positions listed a clearance requirement, which was slightly lower than the population average of 18.9%. Programming expertise was listed on 13.7% of positions listing an MIS or IS degree. The architecture, penetration testing, and software security sub-fields had the highest percentages of positions listing a programming language. Python, Java, SQL, PowerShell, C, and C++, were the most frequently listed languages, respectively.

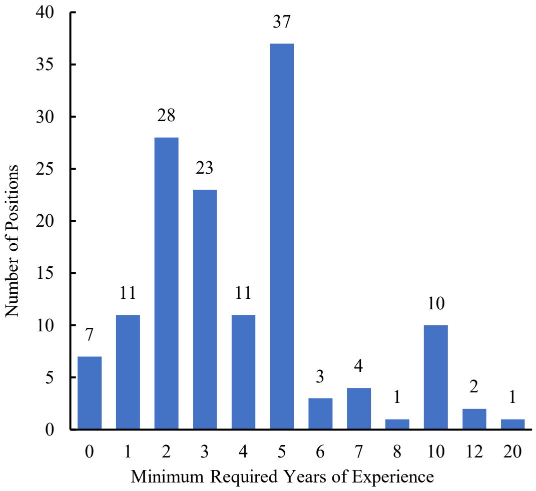

Figure 8. Distribution of Cybersecurity Positions Listing a MIS or IS Degree Requirement by Listed Minimum Years of Required Experience

5. DISCUSSION

Similar to the results found by Peslak and Hunsinger (2019), and Marquardson and Elnoshokaty (2020), I found that prior professional experience and possession of a higher education degree were the most frequently listed requirements for cybersecurity job postings based upon my analysis of 935 unique cybersecurity job postings. In addition to experience and education requirements, I also found that possession of an industry certification was also frequently required or desired for cybersecurity positions, as over half of all positions included an industry certification in the job posting. Similar insights on industry certifications were also found by Parker and Brown (2019). Regarding security clearances, based on the results of this analysis, I also found that security clearances were a common requirement listed on cybersecurity job postings, with nearly 1 out of 5 positions requiring an active security clearance, or the ability to obtain a clearance as a condition of employment. Knowledge of programming languages was also frequently listed on cybersecurity job postings, with nearly 1 out of 4 positions listing a programming language among desired or required skills.

While the general observations on cybersecurity job postings in this analysis are useful for providing insights on cybersecurity position requirements, I also observed that there were notable variations in requirements between cybersecurity positions in different sub-fields or categories that would not have been captured through a more generalized analysis. For example, regarding education, while only 2.9% of cybersecurity positions listed a doctoral degree as a requirement, 54.5% of education positions, 10.3% of threat intelligence/research positions, and 6.0% of management positions required a doctoral degree. If all cybersecurity positions were analyzed within the context of being within a single category, doctoral degrees would seem extremely rare. However, when cybersecurity position requirements are analyzed by sub-field, doctoral degrees are more frequently required in certain sub-fields. This phenomenon can also be seen in the varying experience requirements between positions in different sub-fields. While the average required experience of all cybersecurity positions in this analysis was 3.9 years, the average required experience of positions in the management, software security, architecture, and education categories were all higher than the overall average at, 6.5, 4.7, 4.3, and 4.2 years, respectively. Thus, an analysis of cybersecurity job postings that consider the varying nature and diversity of positions in the cybersecurity field can be advantageous for providing additional insights on industry hiring requirements.

Several summarized insights and recommendations can be made from the results presented in this analysis:

1. Most job postings in the cybersecurity field require either a higher education degree, prior professional experience, an industry certification, or any combination of the three. Specialized cybersecurity positions such as penetration testing, threat intelligence and research, and management-focused positions often have much higher education and experience requirements than other cybersecurity positions.
2. Regarding education, a high percentage of job positions require a bachelor’s degree. Technical majors such as computer science, information systems, engineering, information technology, and cybersecurity seem to be the most requested. While a much smaller percentage of positions require graduate degrees, master’s degrees are most requested for positions within the architecture, auditing, education, management, software security, and threat intelligence/research subfields. Doctoral degrees are most frequently requested for education, management, and threat intelligence/research positions. A bachelor’s degree, at a minimum, is highly recommended for cybersecurity job seekers.
3. Prior professional experience in a related role to the job posting is very common in cybersecurity job postings across all sub-fields. Most cybersecurity job postings require 0-5 years’ experience. Positions in the auditing and operations categories often require the least amount of prior work experience, while positions in the management category often require a higher number of previous years of experience than roles in other sub-fields.
4. Industry certifications continue to be prevalent in cybersecurity job postings and are often a prerequisite for employment. A wide variety of industry certifications may be listed on job postings. The CISSP is the most frequently mentioned certification, although other certifications such as the OSCP and CISA are the most popular certifications for specialty fields such as penetration testing and auditing, respectively.
5. Possession of a security clearance is also common on cybersecurity job postings in almost every sub-field, except for the auditing and education categories, which did not list any positions requiring a clearance. Nearly 1 out of 5 job postings require some level of security clearance as a pre-requisite for employment. Percentages of positions requiring a security clearance were relatively similar between subfields.
6. Programming languages were also commonly listed on cybersecurity positions, with nearly a quarter of positions listing knowledge and experience with a programming language as either a desired or required requirement for

employment. While various programming languages were listed, currently, Python and Java seem to be the most popularly requested languages. By subfield, the software security, penetration testing, and threat intelligence/research subfields had the highest prevalence of positions listing a programming language. Listing of programming languages was also common on positions within the architecture and operations categories. Programming language requirements were relatively uncommon for auditing, education, GRC, and management-focused positions.

As mentioned in the results section, MIS and IS degrees were the second most frequently listed major for positions containing an educational requirement. Except for the software security and education sub-fields, over a quarter of positions containing an educational requirement in all sub-fields, listed an MIS or IS degree as a desired or required pre-requisite for employment, suggesting that MIS degrees are sought after in almost every sub-field in cybersecurity. As experience was one of the most frequently listed requirements, MIS or IS students would greatly benefit from having 1-2 years of professional experience in cybersecurity, even from a professional internship. Industry cybersecurity certifications were also highly valued for positions listing MIS or IS degrees. Knowledge of a popular programming language such as Python, Java, or SQL would also be highly valuable for MIS or IS students seeking to enter the cybersecurity field, especially if they are interested in positions related to architecture, penetration testing, or software security sub-fields.

Based upon the results of this analysis, it would be advantageous for MIS and IS programs with a focus on preparing students for the cybersecurity profession to incorporate student training for industry certifications and programming into their curricula. In addition, encouraging students to pursue part-time work or professional internships to gain professional experience would be beneficial. Furthermore, as nearly a fifth of positions listing MIS and IS degrees required a security clearance, developing pathways for MIS and IS students to obtain a security clearance, or at a minimum, educating cybersecurity-focused MIS and IS students on the security clearance process may provide new professional opportunities for students entering the cybersecurity workforce.

In summary, while this analysis observed similar trends in cybersecurity position requirements to previous analyses (Peslak & Hunsinger, 2019, Marquardson & Elnoshokaty, 2020, Parker & Brown, 2019), the granular approach in this work provided additional new insights on various types of cybersecurity positions that could not be captured in a more generalized analysis of cybersecurity positions. There were notable differences in position requirements between positions in different sub-fields. This work highlights the complex, broad, and diverse nature of the cybersecurity field. Such complexity results in generating differing requirements and pre-qualifications depending on the nature of the position and job role. Thus, future analyses of cybersecurity job postings and requirements should consider this inherent complexity and diversity.

The observations made in this analysis could be highly beneficial for cybersecurity professional aspirants seeking to gain insights on what qualifications are required by various types of cybersecurity positions, but also for educational institutions seeking to train and prepare the cybersecurity workforce, as well as serve as a guide for developing pathways for student development and success in the cybersecurity career field. Due to the high demand for professional experience in cybersecurity job postings, the development or acquisition of professional internships and employment should be a priority for higher education programs. Furthermore, higher education programs should note the continued prevalence of industry certifications in the field and may consider aligning their curriculum, in part to prepare students for success in earning industry certifications. Courses that immerse students in one or more programming languages would also benefit student success. In addition, due to the demand for security clearances in cybersecurity positions, educational institutions should also consider working with the public sector to develop pathways for students to obtain a security clearance through activities such as government internship programs, or research opportunities.

It should be noted that this study had several limitations. The sample dataset of cybersecurity job postings was a snapshot in time. Given the dynamic nature of the cybersecurity field, it is highly likely that current observations on the popularity of programming languages and industry certifications will change over time as the field continues to develop and evolve. Also, the sample dataset consisted of cybersecurity positions within the United States only and may not reflect global cybersecurity job requirements. Furthermore, although the sample dataset was randomly selected, the dataset was a very small percentage of the currently available cybersecurity job market. In addition, partially due to the simple random sampling method employed in this analysis, the number of analyzed positions in the auditing and education sub-fields was very small. Further analyses which specifically analyze position requirements using specified search queries targeting positions in these two sub-fields or a disproportional stratified sampling method to increase class size would be useful for providing additional insights on auditing or education-focused cybersecurity positions. Future research incorporating a temporal analysis of cybersecurity job postings, with a broader, global scope, would be welcome. Furthermore, investigating an even larger sample of job postings using automated methods such as text mining and machine learning would also be welcome.

6. CONCLUSION

This analysis provided several insights into the education, experience, certification, clearance, and programming skill requirements of current cybersecurity positions. I also found that there were notable differences in requirements between positions in different specializations or sub-fields within the cybersecurity discipline. Generally, across all sub-fields, higher education degrees in majors such as computer science, information systems, and engineering, and prior professional experience are common requirements for cybersecurity positions. While cybersecurity positions on average, require 3-4 years of work experience, management-focused positions require, on average, over six years prior professional experience. Industry certifications were desired or required in over half of the cybersecurity positions we analyzed. While certifications such as the CISSP, Security+, and CISM were prevalent in positions in almost every sub-field, the demand and type of certification varied by sub-field, most notably in the penetration testing subfield, which frequently listed the OSCP and CEH certifications. Security clearances are also notably in demand for cybersecurity positions, as clearances were required or desired for approximately 20% of positions across all categories except for the education and auditing sub-fields. Finally, knowledge of programming languages such as Python, Java, and C++ was also frequently listed as a desired or required skill on cybersecurity job postings, most notably in positions in the architecture, penetration testing, and software security sub-fields.

Overall, a granular analysis of cybersecurity positions by sub-field was advantageous for emphasizing the diversity and complexity of the cybersecurity field. Although there are commonalities in cybersecurity position requirements across the entire discipline, there are also notable differences in the requirements of cybersecurity positions in different sub-fields. To further reduce the current skills and employment gaps in the cybersecurity field, higher education and cybersecurity training programs should take note of the current requirement trends of positions in the varying sub-fields within the cybersecurity discipline, to best prepare the next generation of cybersecurity professionals for success in any type of position. Based upon the insights provided by this analysis, it would be advantageous for educational programs to adapt their curricula and professional field experience programs to develop multiple training pathways that best prepare students and professionals for the varying position requirements within the sub-fields, and the cybersecurity discipline as a whole.

7. REFERENCES

Brooks, N. G., Greer, T. H., & Morris, S. A. (2018). Information Systems Security Job Advertisement Analysis: Skills Review and Implications for Information Systems. *Journal of Education for Business*, 93(5), 213-221.

Caldwell, T. (2013). Plugging the Cyber-Security Skills Gap. *Computer Fraud & Security*, 2013(7), 5-10.

Cobb, M. J. (2018). Plugging the Skills Gap: The Vital Role that Women Should Play in Cyber-Security. *Computer Fraud & Security*, 2018(1), 5-8.

Crumpler, W., & Lewis, J. A. (2019*). The Cybersecurity Workforce Gap*. Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-workforce-gap

Erickson, J. M. (2021). The Cyber Defense Review: Ransomware's Growing Impact. *The Cyber Defense Review*, 6(3), 9-12.

Goldberg, G., & Zaman, N. (2018). Text Analytics for Employee Dissatisfaction in Human Resources Management. *AMCIS 2018 Proceedings*.

Ho, A., Nguyen, A., Pafford, J. L., & Slater, R (2019). A Data Science Approach to Defining a Data Scientist. *Journal of Education for Business*, 93(5), 213-221.

ISACA. (2021). *State of Cybersecurity 2021 Global Update on Workforce Efforts and Resources*. Information Systems Audit and Control Association. https://www.isaca.org/go/state-of-cybersecurity-2021

Kapoor, B., & Kabra, Y. (2014). Current and Future Trends in Human Resources Analytics Adoption. *Journal of Cases on Information Technology*, 16(1), 50-59.

Markow, W., Bittle, S., & Liu, P. (2019). Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring. https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf

Marquardson, J., & Elnoshokaty, A. (2020). Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity jobs. *Information Systems Education Journal*, 18(1), 22-28.

Morgan, S. (2021). Cybersecurity Jobs Report: 3.5 Million Openings in 2025. *Cybercrime Magazine.* https://cybersecurityventures.com/jobs/

Newhouse, W., Keith, S., Scribner, B., & Witte. G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* NIST Special Publication 800-181, US Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181

Parker, A., & Brown, I. (2019). Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. In Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J. (Eds.), *Information Security* (pp. 176-192). ISSA 2018. Communications in Computer and Information Science, vol. 973. Springer, Cham. https://doi.org/10.1007/978-3-030-11407-7_13

Peslak, A., & Hunsinger, D. S. (2019). What Is Cybersecurity and What Cybersecurity Skills Are Employers Seeking? *Issues in Information Systems*, 20(2), 62-72.

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework)*. NIST Special Publication 800-181 Revision 1, US Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1

U.S. Bureau of Labor Statistics. (2021). *Information Security Analysts: Occupational Outlook Handbook.* U.S. Department 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), 243-50.

Verma, A., Lamsal, K., & Verma, P. (2022). An Investigation of Skill Requirements in Artificial Intelligence and Machine Learning Job Advertisements. *Industry and Higher Education*, 36(1), 63-73.

Vogel, R. (2016). Closing the Cybersecurity Skills Gap. *Salus Journal*, 4(2), 32-46.

Watson, R., Corbett, J., Galletta, D. F., Ives, B., Mandviwalla, M., & Tremblay, M. (2020). COVID-19 and IS: Challenges and Opportunities for People, Careers, and Institutions. *AMCIS 2020 Proceedings.* 5.

Wilson, A., & Wilson, C. (2011). The Effects of U.S. Government Security Regulations on the Cybersecurity Professional. *Proceedings of the Academy of Legal, Ethical and Regulatory Issues*, 15(2), 5-12.

AUTHOR BIOGRAPHY

Christopher A. Ramezan is an assistant professor of cybersecurity in the Department of Management Information Systems in the John Chambers College of Business and Economics at West Virginia University. He is also the Program Coordinator of the Master of Science in Business Cybersecurity Management. He currently teaches courses on Data Communications and Networks, Enterprise Security Architecture, Cybersecurity Analytics, Penetration Testing, Cybersecurity Operations, and Network Security. His research focuses on applied machine learning, enterprise security architecture, satellite and aerial remote sensing, and cybersecurity education. Ramezan also holds over 20 cybersecurity certifications including the CISSP, CISM, CASP+, and CDPSE, and has over 10 years prior professional experience in the IT / information security field.

Information Systems & Computing Academic Professionals

Education Special Interest Group

STATEMENT OF PEER REVIEW INTEGRITY

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

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