ISSN: 2473-4901
v12 n6816

Understanding Cybersecurity Workforce Demand: A Topic Modeling Analysis of 11,562 Job Advertisements

Stephanie Totty
stephanie.totty@mtsu.edu

Christopher Conner McAnally
conner.mcanally@mtsu.edu

Soham Sengupta
soham.sengupta@mtsu.edu

Nita Brooks
nita.brooks@mtsu.edu

Middle Tennessee State University
Murfreesboro, TN, 37132, USA

Abstract

Cybersecurity has become a strategic organizational priority, increasing demand for professionals with specialized security knowledge and skills. At the same time, employers continue to report challenges in recruiting qualified cybersecurity talent, creating a need to understand better the competencies sought in the labor market. This study examines 11,562 cybersecurity job advertisements to identify the skill clusters that characterize contemporary demand in the cybersecurity workforce. Using skills extracted from the job advertisements and topic modeling based on Non-negative Matrix Factorization, we identify nine skill clusters of cybersecurity work: Government, Risk, and Compliance; Software Development; Information Assurance and Risk Management Frameworks; Cyber Threat Intelligence and Incident Response; Professionalism and Leadership; Endpoint Management; Network and Infrastructure Security; Identity and Access Management; and Cloud Security. We further examine the cybersecurity job titles most closely associated with each skill cluster and compare these clusters with an established cybersecurity workforce framework. The findings suggest that cybersecurity labor market demand is organized around distinct combinations of technical and professional skills rather than around job titles alone, with many common job titles spanning multiple skill clusters. The results contribute to understanding the structure of cybersecurity workforce demand and provide insights for higher education institutions, employers, and workforce development organizations seeking to align better curriculum design, recruitment practices, and training initiatives with evolving labor market needs.

Keywords: Cybersecurity, Job Advertisements, Skill Cluster, Topic Modeling

Understanding Cybersecurity Workforce Demand: A Topic Modeling Analysis of 11,562 Job Advertisements

Stephanie Totty, Christopher Conner McAnally, Soham Sengupta, and Nita Brooks

1. INTRODUCTION

Industry 4.0 has expanded the cyber threat landscape by increasing organizational attack surfaces and introducing new vulnerabilities. Emerging technologies, including generative AI, have intensified cybersecurity risks and made cybersecurity a strategic organizational capability. Reflecting this strategic importance, cybersecurity has consistently been ranked among the top two most important IT management issues for organizations over the last decade (Johnson et al., 2025). IBM's Cost of a Data Breach Report 2025 (IBM, 2025) states that the average cost of a data breach in the US increased by 9% to $10.22 million. Additionally, AI-driven cyber threats have led to a 13% increase in attacks. Of these, 60% resulted in data compromises, while 31% caused severe operational disruptions. Literature suggests that an increasing number of companies are adopting a proactive stance towards cybersecurity (Islam et al., 2024; Kuraku et al., 2023). Simultaneously, regulatory bodies such as the SEC require public companies to disclose their cybersecurity governance in their annual shareholders' reports. As organizations strengthen their cybersecurity posture, the demand for qualified cybersecurity professionals has increased, making cybersecurity talent a sought-after resource.

Despite this unprecedented demand, organizations continue to struggle to recruit and retain qualified cybersecurity professionals. According to the U.S. Bureau of Labor Statistics, employment for Information Security Analysts is projected to grow at 29% between 2024 and 2034, substantially faster than the average for all other occupations (U.S. Bureau of Labor Statistics, 2025). At the same time, CyberSeek, an interactive tool and initiative that provides data on cybersecurity jobs in its 2025 report (Cyber Seek, n.d.), and ISC2 in its 2024 report (ISC2, 2024) estimate that the United States currently faces a cybersecurity workforce shortage between 480,000 and 570,000, while the global number exceeds three million professionals (Goupil et al., 2022). The persistence of these vacancies, despite strong employment prospects, suggests that the challenge extends beyond workforce size and reflects a growing disconnect between the capabilities employers seek and available candidates possess. This disconnect has increasingly been characterized as a cybersecurity skills gap.

Understanding this skills gap has become particularly challenging because cybersecurity itself is evolving rapidly. Cloud-native architectures (Theodoropoulos et al., 2023), zero-trust security models (Joshi, 2025), AI-enabled defensive capabilities (Kabir et al., 2026), DevSecOps practices (Abiona et al., 2024), identity-centric security (Ghadge, 2024; Sheik et al., 2021), and increasingly sophisticated threat environments (CrowdStrike, n.d.) continually redefine the competencies expected of cybersecurity professionals. This motivates us to explore evolving cybersecurity job opportunities in the US to understand the skill requirements of respective roles better and mitigate the skills gap.

This study addresses this gap by conducting an exploratory analysis of contemporary cybersecurity job advertisements in the United States using topic modeling techniques. Rather than beginning with predefined occupational categories, we analyzed 11,562 cybersecurity job advertisements to identify the latent structure of cybersecurity employment as expressed directly by employers. By examining the skills in job advertisements, we identify naturally occurring cybersecurity skill clusters, the job titles associated with those clusters, and the combinations of skills that distinguish them. This bottom-up approach allows the cybersecurity labor market to define itself through employer demand rather than through existing occupational classifications or theoretical frameworks.

Accordingly, this study seeks to answer the following research questions:

- **RQ1:** What are the overarching cybersecurity skill clusters in the United States cybersecurity labor market?
- **RQ2:** What are the most sought-after skills associated with cybersecurity positions?
- **RQ3:** What are the most common cybersecurity job titles advertised by employers?

RQ4: How do cybersecurity job titles align with the overarching cybersecurity skill clusters identified through topic modeling?

RQ5: How do the empirically derived cybersecurity skill clusters align with established cybersecurity workforce frameworks?

This research makes important contributions. First, it provides one of the most comprehensive and up-to-date empirical examinations of the U.S. cybersecurity job market by analyzing a large corpus of recent cybersecurity job advertisements across multiple cybersecurity occupations. Second, unlike prior studies that primarily examine certifications, educational qualifications, or years of experience, this research identifies the skill combinations that characterize distinct cybersecurity skill clusters, thereby providing a substantially more granular understanding of employer expectations. This study offers insights for higher education institutions, curriculum designers, and employers.

2. LITERATURE REVIEW

Existing research consistently demonstrates that cybersecurity competence extends beyond technical expertise alone. Successful cybersecurity professionals require an integrated combination of technical capabilities, professional skills, domain-specific knowledge, and interpersonal competencies to operate effectively within increasingly complex organizational environments (Benson et al., 2025; Dawson & Thomson, 2018; Graham & Lu, 2023). For example, while educational approaches such as Capture-the-Flag competitions effectively develop technical skills in areas including cryptography and network security (Švábenský et al., 2021), they often provide comparatively limited exposure to human-centered aspects of cybersecurity, such as social engineering and cybersecurity awareness. At the same time, emerging technologies continue to reshape employer expectations, with increasing demand for competencies related to analytics and artificial intelligence alongside traditional cybersecurity knowledge (Graham, 2025; Graham & Lu, 2023). These findings suggest that cybersecurity education must evolve continuously to balance technical expertise with broader organizational and professional competencies.

Cybersecurity workforce requirements are also influenced by regulatory environments, organizational priorities, workforce maturity, and national contexts (Graham, 2025). Studies conducted across South Africa, South Korea, the United Kingdom, and Morocco demonstrate that although cybersecurity occupations share common technical foundations, employers emphasize different combinations of skills, qualifications, and competencies depending on regional and organizational needs (Brink et al., 2022; Furnell, 2021; Jun et al., 2023; Parker & Brown, 2019; Rahhal et al., 2019). Collectively, these findings suggest that cybersecurity education and competency models must evolve continuously to reflect changing labor market requirements rather than relying on static descriptions of cybersecurity work.

Understanding these evolving workforce requirements requires empirical evidence that reflects current employer demand. Job advertisements have become an increasingly valuable source of workforce intelligence because they directly communicate the qualifications, technologies, certifications, and competencies organizations seek in prospective employees (Brooks et al., 2018; Peslak & Hunsinger, 2019; Ramezan, 2023). Unlike occupational classifications or competency frameworks, which are periodically revised through expert consensus or government initiatives, job advertisements provide a near-real-time representation of labor market demand and changing organizational priorities. This advantage has made them an important data source for workforce research across the information systems discipline (Harris et al., 2012; Maier et al., 2002). Furthermore, advances in computational text analytics have transformed how researchers analyze job advertisements. Rather than relying solely on manual review, recent studies increasingly employ text mining, natural language processing, and machine learning techniques to analyze large collections of job advertisements and uncover latent relationships among occupations and skills (Fortino & You, 2022; Pejic-Bach et al., 2020; Roeksiri & Amphawan, 2023). These methodological advances provide an increasingly robust foundation for examining employer demand within rapidly evolving technical domains such as cybersecurity and have stimulated a growing body of research that specifically analyzes cybersecurity job advertisements to understand the contemporary cybersecurity labor market.

Beyond describing employer requirements through job advertisements, there is a body of research examining the alignment between cybersecurity education, competency frameworks, and workforce needs. Studies have developed and evaluated competency frameworks to support workforce development while assessing how well they reflect employer expectations (Almeida, 2025; Bendler &

Felderer, 2023; Nautiyal & Rashid, 2024). Comparative analyses further reveal discrepancies between university curricula, competency frameworks, and industry requirements, with employer demand emphasizing implementation, deployment, operational, and legal competencies more strongly than academic programs (Budde et al., 2023; Goupil et al., 2022). Collectively, this stream of research suggests that although competency frameworks provide valuable guidance for cybersecurity workforce development, they remain normative representations of professional competencies and do not always capture the rapidly evolving demands of the cybersecurity labor market.

Existing literature, summarized in Appendix A, has either provided descriptive statistics, analyzed individual job titles, or compared job advertisements with existing frameworks. However, there is a lack of studies that identify recurring combinations of skills across cybersecurity job titles to inform academia and practice in identifying and cultivating them to build the most effective cybersecurity workforce. For comparison, although Ozyurt & Ayaz (2024) examined 9407 job advertisements from 2021 to 2022 to identify job titles and skills required by companies, our study is more recent and examines skills across job titles/advertisements, informed by the O*NET Code, which is more methodical in defining cybersecurity-related jobs.

3. METHODOLOGY

To answer our research questions, we collected the job advertisements for cybersecurity jobs in the United States that were newly listed in February 2025. As noted previously, prior literature has mined job advertisement text and used the skills listed in those advertisements as indicators of the skills desired or required of individuals in the workforce. We collected the job advertisements data from Lightcast (Lightcast, 2025). We included the O*NET codes in Table 1 to capture most cybersecurity job advertisements without incurring a significant number of false positives in the search results (see Appendix B for additional information about the O*NET Code decision process). Our search resulted in 11,562 job advertisements across the 5 O*NET codes. In total, 1287 unique job titles are represented by these advertisements. Virginia (1291 job advertisements), Texas (1045 job advertisements), and California (894 job advertisements) are the three states with the most job advertisements in our sample.

O*NET Code	Occupation	Number of Job Advertisements
13-1199.07	Security Management Specialists	359
15-1212.00	Information Security Analysts	2516
15-1299.04	Penetration Testers	1336
15-1299.05	Information Security Engineers	7087
15-1299.06	Digital Forensics Analysts	264

Table 1. O*NET Codes included in the job advertisements search and the resulting number of job advertisements returned

The job titles appearing most frequently in our data are shown in Table 2.

Job Title	Number of Job Advertisements
Cybersecurity Engineers	620
Security Engineers	490
Cybersecurity Analysts	440
Information Systems Security Officers	382
Cybersecurity Specialists	359
Unclassified	310
Information Security Analysts	269
Application Security Engineers	266
Cloud Security Engineers	182
Information Security Engineers	175

Table 2. Top 10 most common job titles

Lightcast deduplicates the data in its database by identifying "job postings with the same values for the company name, location, job title, and similarity of job posting text" (Harris & Clark, 2024, p. 281). Lightcast uses a proprietary approach that uses shingling to assess the similarity of the job posting text (Harris & Clark, 2024). Lightcast programmatically derives the skills included in each job advertisement (Lightcast, n.d.). Because each job advertisement often includes many other common sections (e.g., a description of the company and legally required hiring language), we used the derived skills to exclude these known sources of noise from the data. Lightcast derives skills based on the Lightcast Skills Taxonomy, which accounts for "aliases, acronyms, abbreviations, and historic names" (Lightcast, n.d., "Skills"). Additionally, Lightcast scans the remaining text for word sequences to ensure the skills are identified in the proper context (e.g., homonyms).

4. ANALYSIS

We used Python 3.12.7 with several common data libraries (pandas v1.5.2, NumPy v1.23.5, scikit-learn v1.2.0, NLTK v3.9.1, gensim v4.4.0, pyLDAvis v3.4.1, Matplotlib v3.7.1, Seaborn v0.13.2, ipywidgets v7.7.1, and Transformers v4.57.1) to process, visualize, and analyze the data. To prepare the data for analysis, we standardized the skills field prior to modeling to ensure consistent term usage. We lowercased all text so that variations of the same term (like "AWS" vs. "aws") would not be treated differently; for reporting and figures, we re-capitalized familiar acronyms and proper nouns for readability. We then removed any text in parentheses (e.g., "Certified Information System Auditor (CISA)" to "Certified Information System Auditor") to prevent duplicate forms during tokenization, merged multi-word skills into single tokens (e.g., "identity_and_access_management") so phrases would stay intact, and split comma-separated entries into individual tokens so each skill is counted only once. The skills most listed in a job advertisement are noted in Table 3.

Skill	Number of Job Advertisements	Percent
computer_science	4440	38
certified_information_systems_security_professional	3984	34
leadership	3428	30
operation	3341	29
auditing	3289	28
incident_response	2993	26
problem_solving	2679	23
vulnerability_management	2648	23
security_controls	2442	21
amazon_web_services	2379	21

Table 3. Number and percent of job advertisements that include the 10 most occurring skills

After preprocessing, each job advertisement was represented as a TF-IDF-weighted skill vector, allowing skills to be weighted according to both their frequency within advertisements and their distinctiveness across the corpus. Skills were filtered to a maximum document frequency of 50% to exclude overly common, low-signal terms. A custom tokenization pattern was used in place of the vectorizer's default tokenizer so that multi-part skill terms containing punctuation (e.g., "ci/cd", "asp.net") were preserved as single features rather than split apart. We then applied Non-negative Matrix Factorization (NMF) to identify latent skill clusters within the resulting skill matrix. NMF was selected because it performs well on short, structured inputs and produces interpretable additive skill-cluster representations. NMF was fit using scikit-learn's default coordinate-descent solver, NNDSVDA initialization, Frobenius-norm lsos, a convergence tolerance of 1×10^{-4}, and a maximum of 200 iterations, with a fixed random seed (random_state=42) for reproducibility.

To ensure we modeled the appropriate number of skill clusters (K), we first swept $K \in [5,20]$ using U_{Mass} coherence, which indicated a high-coherence band around 5 to 12 skill clusters (see Figure 1). We then refined within that band using $C_v$coherence (often a better proxy for human interpretability; e.g., Morstatter & Liu, 2018). $C_v$coherence peaked at $K = 9$ and $K = 11$ (see Figure 2). We proceeded with 9 skill clusters for parsimony and stability.

ISSN: 2473-4901
v12 n6816

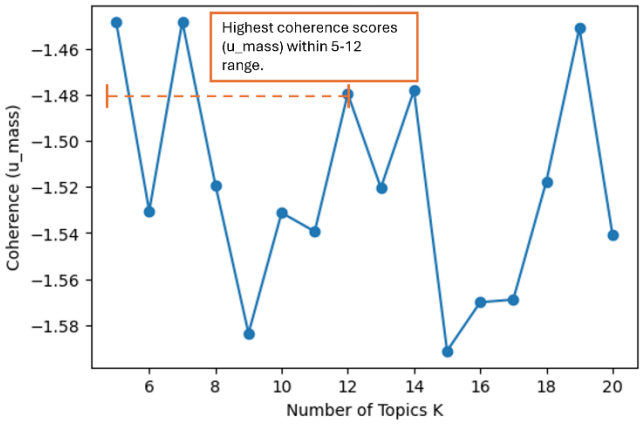

Figure 1. NMF coherence (u_mass) for 5 to 20 skill clusters

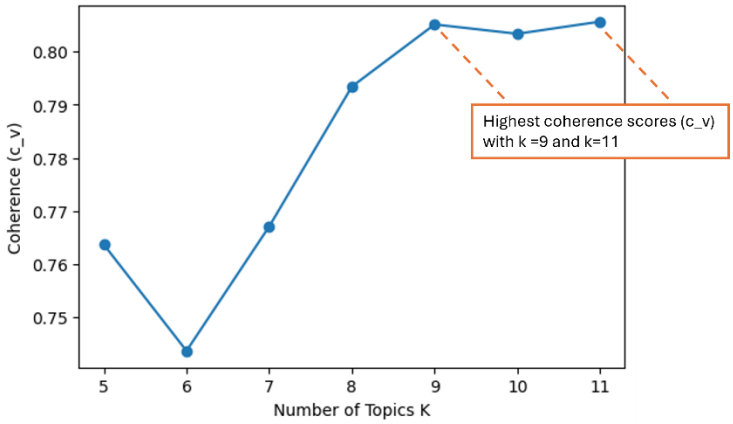

Figure 2. NMF coherence (c_v) for 5 to 11 skill clusters

To reduce vocabulary sparsity, skills were filtered using a minimum document frequency threshold of 0.5% (using an elbow heuristic), resulting in 834 skills that covered approximately 88% of all skill mentions. We then defined job advertisements as associated with skill clusters when their NMF loading exceeded 0.025. This threshold produced sparse and interpretable skill clusters assignments and yielded results similar to nearby thresholds (0.02 and 0.03) that were evaluated.

Upon reviewing the results, we identified 371 job advertisements (3.21% of all job advertisements in our dataset) with no skill cluster assignment at the association threshold (NMF loading ≥ 0.025). We reviewed the number of skills that were derived from the zero-skill cluster documents (see Table 4). In total, 136 zero-skill cluster documents (36.7%) had 3 or fewer skills. The remaining 235 zero-skill cluster postings had more than three derived skills; they did not reach the 0.025 loading threshold for any skill cluster, indicating that their skill content did not concentrate strongly in a single skill cluster. These were excluded from analysis, and we did not test whether retaining them under an alternative assignment rule would affect the reported distributions, which we note as a limitation.

Number of skills derived	Number of Job Advertisements	Percent of Total Zero-Skill Cluster Documents
0	40	10.78%
1	57	15.36%
2	17	4.58%
3	22	5.93%
Total	136	36.66%

Table 4. Number of job advertisements and percent of total zero-skill cluster documents with zero to 3 derived skills

Upon review by the authors, the final skill cluster model produced coherent, compact skill clusters. The authors reviewed the top 25 terms (skills) associated with each of the 9 skill clusters. We added human labels to the skill clusters (see Appendix C).

We allowed correlated skill clusters because we expect the resulting skill clusters to be related. Given the number of job advertisements associated with two or more skill clusters and the number of combinations of skill clusters that a job advertisement could be associated with, we also review the data using only the skill cluster with the highest association for parsimony and simplicity. Table 5 indicates the number of job advertisements associated with each skill cluster when only using the highest NMF loading.

Skill Cluster	**Number of Associated Job Advertisements**
Government, Risk, and Compliance	929
Software Development	1697
Information Assurance and Risk Management Frameworks	1712
Cyber Threat Intelligence and Incident Response	2232
Professionalism and Leadership	1910
Endpoint Management	394
Network and Infrastructure Security	717
Identity and Access Management	831
Cloud Security	771

Table 5. Number of associated job advertisements per skill cluster (highest NMF loading only)

5. SKILL CLUSTERS

Next, we provide a brief description of each resulting skill cluster. Appendix C lists job titles most frequently associated with each skill cluster.

5.1 Government, Risk, and Compliance

The Government, Risk, and Compliance skill cluster focuses on managing cybersecurity risk in organizations through auditing, regulatory compliance, and risk management frameworks. Individuals who work in these areas often hold certifications such as the Certified Information Systems Auditor, Certified Information Systems Manager, or Certified Information Systems Security Professional. Common tasks in Government, Risk, and Compliance often involve developing and implementing security policies, handling internal and external audits, and ensuring frameworks such as COBIT, NIST, and ISO 27001 are followed. Jobs related to GRC represent legal, operational, and technical aspects of the organization.

5.2 Software Development

Software development in the context of cybersecurity involves using tools such as C, Python, and Java, with security built in from the outset. Organizations must develop applications with security as a key component and not an afterthought. Secure coding and OWASP are common concepts/tools mentioned. OWASP represents best practices for web application development, and the OWASP Top 10 highlights the most common security issues. Being able to identify possible attack vectors during software design activities is a key competency; understanding secure design is critical in today’s environment.

5.3 Information Assurance and Risk Management Frameworks

The primary focus of this skill cluster is on federal frameworks and authorization processes. High-level security clearances are often required. Skills related to developing plans of action and milestones, managing information assurance activities, and assessments for government information systems are critical and geared towards federal and defense contractor roles. The focus on security clearance indicates the importance of access eligibility, regulatory knowledge, and technical skills.

5.4 Cyber Threat Intelligence and Incident Response

A fundamental area of cybersecurity that is growing is threat intelligence. Threat intelligence sources can be internal and/or external to the organization. Open-source threat intelligence is expanding. Professionals who work in this area gather, analyze, and use cyber threat intelligence (CTI) to secure systems. Security incident and event management systems are often used in these roles. They provide capabilities such as monitoring key performance indicators and providing visuals to alert incident response teams to issues as they occur. Individuals who work in this area must be familiar with the MITRE ATT&CK framework. Knowledge of endpoint detection and response systems, proactive threat hunting, and vulnerability management all help protect the organization. Commonly required certifications relate to CTI and incident management; jobs are often highly analytical and require specialization.

5.5 Professionalism and Leadership

In addition to the technical requirements found across cybersecurity jobs, professionalism and leadership skills are also expected. Individuals in these roles must be able to communicate, lead, and manage projects, and make thoughtful decisions. These expectations span different levels and are not solely limited to senior-level positions. The demand for skills in these areas underscores that cybersecurity is a people-focused profession, not solely about technology.

5.6 Endpoint Management

One of the most vulnerable aspects of our connected environments is the endpoint. Desktop devices running Microsoft Windows, Teams, and SharePoint, as well as mobile devices, require specific management approaches. Individuals supporting endpoints need to be proficient in PowerShell and Intune and are often expected to hold certifications specific to the operating system environment. Specific activities that must be managed include device enrollment, policy enforcement, patch management, and application deployment. Endpoint experts must be able to troubleshoot and support across a variety of applications. They are also responsible for understanding the attack vectors often exploited and for reducing the attack surface. Effective endpoint management is required to maintain secure environments, given that endpoints are often the path through which malicious traffic flows.

5.7 Network and Infrastructure Security

Cybersecurity is fundamentally important due to the interconnected nature of systems today. Professionals must exist who can design and implement a secure network infrastructure. Technologies and tools used in these roles include firewalls, virtual private networks, and intrusion detection and prevention systems. Organizational networks often are segmented to limit movement. Network-level threats must be addressed in real time, and unified threat management is critical. Network security architects are required to design defense-in-depth and zero-trust infrastructures. Security controls must be consistently enforced across cloud and on-premises networks. Employers require individuals who can operate under pressure to resolve network incidents as they occur.

5.8 Identity and Access Management

Professionals who understand the complexities of identity and access management (IAM) are necessary to securely manage any computing environment today. Knowledge of protocols such as SAML and OAuth, as well as understanding technologies such as Active Directory, is extremely important for roles in IAM. Reducing the attack surface through tools such as SSO is also part of creating a secure enterprise. Individuals working in this area focus on managing digital identities across platforms. They must also be able to balance security and usability, which has been a tension point in cybersecurity since it became a skill cluster of concern in organizations. Access management is strategically important for maintaining a secure environment, and demand for individuals with knowledge and skills in these tools and technologies will continue to grow.

5.9 Cloud Security

Cloud as a model for software development, application access, and infrastructure management continues to grow. As such, jobs often focus on cloud security specifically related to IaaS, PaaS, and SaaS. Amazon Web Services is a market leader in the area, as is Microsoft Azure. Organizations may require fluency in multiple platforms. It would be expected that security jobs require specific knowledge of these environments; individuals working in cloud security must be able to apply security principles and practices across architectures. Cloud certifications, such as the Certified Cloud Security Professional, are also becoming more popular. NIST provides guidance on cloud security and is a commonly associated expectation in cloud-related security roles.

6. DISCUSSION AND CONCLUSION

This study analyzed 11,562 cybersecurity job advertisements collected across the United States to identify the latent skill-based structure of contemporary demand in the cybersecurity workforce. Regarding RQ1, we used Non-negative Matrix Factorization topic modeling applied to employer-derived skill data and identified nine distinct cybersecurity skill clusters: Government, Risk, and Compliance; Software Development; Information Assurance and Risk Management Frameworks; Cyber Threat Intelligence and Incident Response; Professionalism and Leadership; Endpoint Management; Network and Infrastructure Security; Identity and Access Management; and Cloud Security. Particularly notable is the emergence of the Professionalism and Leadership skill cluster, which reinforces prior findings that cybersecurity requires more than technical expertise alone. With respect to RQ2, the most frequently demanded skills across the full corpus included computer science, the Certified Information Systems Security Professional credential, leadership, auditing, and incident response, highlighting the dual technical-professional nature of demand in the cybersecurity workforce.

Turning to RQ3 and RQ4, the most common job titles in our sample were Cybersecurity Engineers, Security Engineers, and Cybersecurity Analysts. However, these titles appeared prominently across multiple skill clusters rather than being concentrated in a single skill cluster. This finding suggests that employers often use common occupational labels to describe positions that require substantially different combinations of skill clusters. With respect to RQ5, comparison with the NICE framework further indicates that employer-defined skill groupings may not correspond directly with work-role categories (see Table 6). The initial mapping of this framework was completed by one of the authors, who is heavily engaged in the CAE-CD application. The other authors reviewed the mapping, and any disagreements were discussed and resolved.

Skill Cluster (This Study)	**NICE Work Role Categories**
Government, Risk, and Compliance	Oversight and Governance
Software Development	Design and Development
Information Assurance and Risk Management Frameworks	Oversight and Governance
Cyber Threat Intelligence and Incident Response	Protection and Defense
Professionalism and Leadership	-
Endpoint Management	Implementation and Operation
Network and Infrastructure Security	Implementation and Operation
Identity and Access Management	Implementation and Operation
Cloud Security	Implementation and Operation
Note: No skill cluster aligns with the NICE Work Role Category Investigation.	

Table 6. Skill cluster alignment with work role categories in the NICE Framework

6.1 Implications for Practice

The identified skill clusters have implications for both educators and employers. For higher education institutions, the findings support a curriculum structure that combines a common cybersecurity foundation with opportunities for specialization. For organizations, the results suggest that explicit skill profiles may better describe cybersecurity positions than broad titles such as cybersecurity analyst or

cybersecurity engineer.

The skill clusters identified in this study have important implications for higher education institutions, employers, and workforce development organizations seeking to align better cybersecurity education, recruitment, and training with evolving labor market demand. First, these findings have important implications for higher education institutions and curriculum designers. Rather than viewing cybersecurity as a single homogenous field, the results suggest that cybersecurity jobs are organized around skill clusters. Cybersecurity curricula may benefit from providing students with a common cybersecurity foundation while also offering opportunities to develop deeper expertise in specific skill clusters where demand is growing. Such an approach may better align academic preparation with combinations of skills employers seek. Furthermore, the presence of the Professionalism and Leadership skill cluster reinforces previous findings that cybersecurity professionals require more than technical expertise (Dawson & Thomson, 2018). Programs preparing students for cybersecurity careers should continue to integrate communication, teamwork, leadership, and problem-solving skills into their curricula.

Second, the results also have implications for organizations and hiring managers responsible for workforce planning and recruitment. The process that organizations currently use to hire could be improved (Cappelli, 2019). Many of the most common cybersecurity job titles appeared across multiple skill clusters, suggesting that job titles alone may provide an incomplete description of the skills required for a particular position. Employers may therefore benefit from defining positions using explicit skill profiles rather than relying primarily on broad occupational labels such as cybersecurity analyst, cybersecurity engineer, or security engineer. A skill-based approach to recruitment (Moritz & Zahidi, 2023) may improve candidate evaluation, hiring decisions, workforce planning, and professional development by providing greater clarity regarding the specific competencies required for success in a job.

6.2 Implications for Theory

This research also contributes to theory. Researchers have studied occupational categories, job types, and skill taxonomies to understand better the structure of professional work (e.g., Djumalieva & Sleeman, 2018; Eckhardt et al., 2016; Tornow & Pinto, 1976). Our findings contribute to this literature by demonstrating how contemporary cybersecurity work can be characterized using a bottom-up, data-driven approach derived directly from employer demand. Rather than relying on predefined classifications such as O*NET, NICE, and other expert-developed frameworks, the topic modeling approach identified nine skill clusters of cybersecurity skills that reflect how employers group competencies in practice. These findings suggest that cybersecurity work may be structured around empirically observable combinations of skills. As cybersecurity continues to mature as a distinct academic and professional discipline and as subdisciplines are identified (Chen & Yan, 2025; Ho et al., 2023), our results provide an empirical perspective on how those subdisciplines manifest in the labor market. More broadly, this study contributes to the growing body of literature that uses secondary data to develop and refine occupational taxonomies.

6.3 Limitations and Future Research Directions

The study is limited by both its geographic scope and occupation selection. The sample included only U.S. cybersecurity job advertisements posted in February 2025 and only the selected O*NET cybersecurity occupations. Because cybersecurity requirements vary across jurisdictions and because broader cybersecurity-related occupations were excluded, future research could examine whether similar skill clusters emerge in other countries and across alternative definitions of cybersecurity work.

Additionally, the analysis represents a single point in time and does not distinguish between entry-level and experienced positions. Cybersecurity workforce demand may vary across business cycles, government contracting activity, and technology trends. Future research could examine longitudinal changes in skill clusters and compare skill requirements across career stages.

From an analysis perspective, we did not formally test skill cluster stability across multiple random seeds. We also did not resample subsets of the data. These represent opportunities for future research.

This study also relies on job advertisements and Lightcast-derived skills as proxies for employer demand. While this approach provides a scalable and standardized representation of workforce requirements, job advertisements may not fully distinguish between preferred and required qualifications. Additionally, the job posting or derived skills data does not code the desired proficiency. Finally, while job advertisements have been used as proxies for employer demand in prior research, they may not accurately describe the positions. Future studies could compare these findings with models developed from full job-advertisement text, interviews, surveys, or Delphi-based approaches.

7. REFERENCES

Abiona, O. O., Oladapo, O. J., Modupe, O. T., Oyeniran, O. C., Adewusi, A. O., & Komolafe, A. M. (2024). The emergence and importance of DevSecOps: Integrating and reviewing security practices within the DevOps pipeline. *World Journal of Advanced Engineering Technology and Sciences*, *11*(2), 127–133. https://doi.org/10.30574/wjaets.2024.11.2.0093

Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security*, *151*, 104329. https://doi.org/10.1016/j.cose.2025.104329

Bendler, D., & Felderer, M. (2023). Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model. *ACM Transactions on Computing Education*, *23*(2), 1–33. https://doi.org/10.1145/3573205

Benson, V., Di Chiacchio, L., & Frączek, B. (2025). Why soft skills matter for women in cybersecurity. *Journal of Computer Information Systems*, 1–14. https://doi.org/10.1080/08874417.2025.2492883

Brink, R., Ophoff, J., & Ruhwanya, Z. (2022). Relevant cybersecurity: Curriculum guidance for the South African context. In R. J. Barnett, D. B. Le Roux, D. A. Parry, & B. W. Watson (Eds.), *ICT Education* (Vol. 1664, pp. 3–19). Springer International Publishing. https://doi.org/10.1007/978-3-031-21076-1_1

Brooks, N. G., 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

Budde, C. E., Karinsalo, A., Vidor, S., Salonen, J., & Massacci, F. (2023). Consolidating cybersecurity in Europe: A case study on job profiles assessment. *Computers & Security*, *127*, 103082. https://doi.org/10.1016/j.cose.2022.103082

Cappelli, P. (2019). Your approach to hiring is all wrong. *Harvard Business Review*, *97*(3), 47–57.

Chen, Y., & Yan, J. (2025). *Evolution of cybersecurity subdisciplines: A science of science study* (arXiv:2511.19331). arXiv. https://doi.org/10.48550/arXiv.2511.19331

CrowdStrike. (n.d.). *CrowdStrike 2026 Global Threat Report*. Retrieved July 14, 2026, from https://www.crowdstrike.com/explore/2026-global-threat-report

Cyber Seek. (n.d.). *Cybersecurity supply and demand heat map*. Retrieved July 14, 2026, from https://www.cyberseek.org/heatmap.html

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

Djumalieva, J., & Sleeman, C. (2018). *An open and data-driven taxonomy of skills extracted from online job adverts* (Working Paper ESCoE DP-2018-13; Economic Statistics Centre of Excellence (ESCoE) Discussion Papers). Economic Statistics Centre of Excellence (ESCoE). https://EconPapers.repec.org/RePEc:nsr:escoed:escoe-dp-2018-13

Eckhardt, A., Laumer, S., Maier, C., & Weitzel, T. (2016). The effect of personality on IT personnel's job-related attitudes: Establishing a dispositional model of turnover intention across IT job types. *Journal of Information Technology*, *31*(1), 48–66. https://doi.org/10.1057/jit.2014.27

Fortino, A., & You, Y. (2022). Tracking technology trends using text data mining. *2022 IEEE Integrated STEM Education Conference (ISEC)*, 415–421. https://doi.org/10.1109/ISEC54952.2022.10025069

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080. https://doi.org/10.1016/j.cose.2020.102080

Ghadge, M. N. (2024). Digital identity in the age of cybersecurity: Challenges and solutions. *London Journal of Research In Computer Science and Technology*, *24*(1), 1–10.

Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022). Towards understanding the skill gap in cybersecurity. *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 1*, 477–483. https://doi.org/10.1145/3502718.3524807

Graham, C. M. (2025). AI skills in cybersecurity: Global job trends analysis. *Information & Computer Security*, *33*(5), 673–689. https://doi.org/10.1108/ICS-09-2024-0235

Graham, C. M., & Lu, Y. (2023). Skills expectations in cybersecurity: Semantic network analysis of job advertisements. *Journal of Computer Information Systems*, *63*(4), 937–949. https://doi.org/10.1080/08874417.2022.2115954

Harris, A., & Clark, C. (2024). Understanding the diffusion of business analysis responsibilities. *Journal of Computer Information Systems,* *64*(2), 278-288. https://doi.org/10.1080/08874417.2023.2193964

Harris, A., Greer, T. H., Morris, S. A., & Clark, W. J. (2012). Information systems job market late 1970's-early 2010's. *Journal of Computer Information Systems*, *53*(1), 72–79. https://doi.org/10.1080/08874417.2012.11645599

Ho, L., Rabiei, S., & White, D. (2023). *A Comparative Study of Interdisciplinary Cybersecurity Education* [White Paper]. UC Berkeley Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/publication/interdisciplinary-cybersecurity-education/

IBM. (2025). *Cost of a Data Breach 2025*. Retrieved July 14, 2026, from https://www.ibm.com/reports/data-breach

ISC2. (2024, October 31). *Results of the 2024 ISC2 Cybersecurity Workforce Study*. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

Islam, S. M., Bari, M. S., Sarkar, A., Khan, A. J. M. O. R., & Paul, R. (2024). AI-driven threat intelligence: Transforming cybersecurity for proactive risk management in critical sectors. *International Journal of Computer Science and Information Technology*, *16*(5), 125–131. https://doi.org/10.5121/ijcsit.2024.16510

Johnson, V., Maurer, C., Torres, R., Guerra, K., Mohit, H., Srivastava, S., & Chatterjee, S. (2025). The 2024 SIM IT issues and trends study. *MIS Quarterly Executive*, *24*(1). https://aisel.aisnet.org/misqe/vol24/iss1/9

Joshi, H. (2025). Emerging technologies driving zero trust maturity across industries. *IEEE Open Journal of the Computer Society*, *6*, 25–36. https://doi.org/10.1109/OJCS.2024.3505056

Jun, H.-J., Park, B.-J., & Kim, T.-S. (2023). Information security job skills requirements: Text-mining to compare job posting and NCS ("Google Translate," Trans.). *Information Systems Review*

(경영정보학연구), *25*(3), 179–197.

Kabir, M. H., Razib, M., Jahin, Z., & Jesan, Z. (2026). Zero trust based critical infrastructure cybersecurity framework with AI-driven threat detection and secure network modernization. *Journal of Computer Science and Technology Studies*, *8*(5), 01–14. https://doi.org/10.32996/jcsts.2026.8.5.1

Kuraku, D. S., Kalla, D., Samaah, F., & Smith, N. (2023). Cultivating proactive cybersecurity culture among IT professional to combat evolving threats. *International Journal of Electrical, Electronics and Computers*, *8*(6), 01–07. https://doi.org/10.22161/eec.86.1

Lightcast. (n.d.). *Job Posting Analytics (JPA) Methodology | Lightcast Knowledge Base*. Retrieved July 14, 2026, from https://kb.lightcast.io/en/articles/6957446-job-posting-analytics-jpa-methodology

Lightcast. (2025, July 4). *Lightcast Data: Basic Overview | Lightcast Knowledge Base*. https://kb.lightcast.io/en/articles/6957498-lightcast-data-basic-overview

Maier, J. L., Greer, T., & Clark, W. J. (2002). The management information systems (MIS) job market late 1970s-late 1990s. *Journal of Computer Information Systems*, *42*(4), 44–49. https://doi.org/10.1080/08874417.2002.11647052

Moritz, R. E., & Zahidi, S. (2023). *Putting skills first: A framework for action*. World Economic Forum. https://www.weforum.org/publications/putting-skills-first-a-framework-for-action/

Nautiyal, L., & Rashid, A. (2024). A framework for mapping organisational workforce knowledge profile in cyber security. *Computers & Security*, *145*, 103925. https://doi.org/10.1016/j.cose.2024.103925

Ozyurt, O., & Ayaz, A. (2024). Identifying cyber security competencies and skills from online job advertisements through topic modeling. *Security Journal*, *37*(4), 1339–1359. https://doi.org/10.1057/s41284-024-00420-w

Parker, A., & Brown, I. (2019). Skills requirements for cyber security professionals: A content analysis of job descriptions in South Africa. In H. Venter, M. Loock, M. Coetzee, M. Eloff, & J. Eloff (Eds.), *Information Security* (Vol. 973, pp. 176–192). Springer International Publishing. https://doi.org/10.1007/978-3-030-11407-7_13

Pejic-Bach, M., Bertoncel, T., Meško, M., & Krstić, Ž. (2020). Text mining of industry 4.0 job advertisements. *International Journal of Information Management*, *50*, 416–431. https://doi.org/10.1016/j.ijinfomgt.2019.07.014

Peslak, A., & Hunsinger, D. S. (2019). What is cybersecurity and what cybersecurity skills are employers seeking? *Issues In Information Systems*. https://doi.org/10.48009/2_iis_2019_62-72

Rahhal, I., Makdoun, I., Mezzour, G., Khaouja, I., Carley, K., & Kassou, I. (2019). Analyzing cybersecurity job market needs in Morocco by mining job ads. *2019 IEEE Global Engineering Education Conference (EDUCON)*, 535–543. https://doi.org/10.1109/EDUCON.2019.8725033

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.

Roeksiri, N., & Amphawan, K. (2023). CID-CJA: Co-occurrence information discovery in computer-related job advertisements. *2023 27th International Computer Science and Engineering Conference (ICSEC)*, 247–252. https://doi.org/10.1109/ICSEC59635.2023.10329668

Sheik, A. T., Maple, C., Epiphaniou, G., & Atmaca, U. I. (2021). A comparative study of cyber threats on evolving digital identity systems. *IET Conference Proceedings*, *2021*(4), 62–69. https://doi.org/10.1049/icp.2021.2428

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, *102*, 102154. https://doi.org/10.1016/j.cose.2020.102154

Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., Girolamo, M. D., Barone, P., Taleb, T., & Tserpes, K. (2023). Security in cloud-native services: A survey. *Journal of Cybersecurity and Privacy*, *3*(4), 758–793. https://doi.org/10.3390/jcp3040034

Tornow, W. W., & Pinto, P. R. (1976). The development of a managerial job taxonomy: A system for describing, classifying, and evaluating executive positions. *Journal of Applied Psychology*, *61*(4), 410–418. https://doi.org/10.1037/0021-9010.61.4.410

U.S. Bureau of Labor Statistics. (2025, August 28). *Information Security Analysts*. Occupational Outlook Handbook. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

APPENDIX A

Literature Review of Previous Studies

Study	Dataset Size/Date	Occupational coverage	Analytical Output	Unit of Analysis
Benson et al., 2025	Interviewed 18 cybersecurity professionals having multiple years of experience across European organizations	Cybersecurity professionals across European organizations	Thematic Analysis was conducted to discover four main themes necessary to develop and leverage soft skills like, Confidence, Mentorship, Problem-solving, and inclusivity	Individuals/Women
Švábenský et al., 2021	More than 969 CTF events with a total of 12,952 challenges and 23,517 writeups posted on CTF time from 2012 to 2020	2 CTF formats namely the challenges and writeups	Mapped Knowledge areas and units in CTF writeups, jeopardy and attack-defense CTF formats	Capture-the-flag exercises.
Graham, 2025	Analyzed 8,262 job postings from nine countries, including the USA, UK, UAE, France, Germany, Canada, Belgium, Australia and Italy from March 1st, 2024 to May 31st, 2024.	Cybersecurity job roles globally.	Analysis shows AI skills such as machine learning (ML), natural language processing (NLP), predictive analytics and neural networks are in high demand globally tied to cybersecurity functions such as threat intelligence, anomaly detection and automated incident response.	Job Advertisements level.
Pejic-Bach et al., 2020	Analyzed 2566 job advertisements on LinkedIn from April 1st to July 1st of 2018.	Job advertisements in English that contained one of the two phrases, "Industry 4.0" OR "Smart factory"	Text mining analysis to cluster job roles by job profiles, phrases associated with them, and distribution of seniority level.	Job Advertisements level.
Roeksiri & Amphawan, 2023	Analyzed 4280 job advertisements in IT from three job search websites from Aug 2020 to April 2023	Job advertisements in "computer related" field.	Introduced a novel approach called CID-CJA (Co-occurrence Information Discovery in Computer-related Job Advertisements) for uncovering valuable co-occurrence information within computer-related job advertisements	Job Advertisement level.

Study	Dataset Size/Date	Occupational coverage	Analytical Output	Unit of Analysis
Fortino & You, 2022	Built a technology trend analyzer, a tool on R with a shiny interface.	Searched for most frequently occurring technology job titles from the U.S. Bureau of Labor Statistics O*NET occupation database filtered for STEM IT occupations.	Built a tool that searches job descriptions on job websites for O*NET occupation titles as job titles.	
Ozyurt and Ayaz (2024)	Analyzed 9407 CS job advertisements from Indeed published between 9/15/2021 and 6/15/2022	Keywords "cyber security" or "cybersecurity"	Manually grouped job titles, LDA of job ads naming topics, showed how the topics varied across job title groups. Employed Latent Dirichlet Allocation (LDA) topic modeling to identify dominant themes within cybersecurity job advertisements and examined how these themes varied across manually defined cybersecurity job title groups.	Job Advertisement level.
Brooks et al. (2018)	The different types of job postings queried over a 30-day time-period in 2018. 798 security-specific job ads were obtained where each listing included job requirements, job title, and location.	Keywords "information security", "cybersecurity", "cyber security", and "IT security"	Frequency distributions of titles, skills, etc. Examined cybersecurity job titles and associated skills to better understand the distribution of cybersecurity occupations and inform Information Systems curriculum development. Domain related skills, education, certifications, and soft skills were identified from the job advertisements.	Job Advertisement level.
Harris et al. (2012)	10,487 IT-Job advertisements posted on www.carrerbuilding.com from 2010 - 2011	70 key words were added to the query used to search the job skills database.	Job postings were manually analyzed for words, phrases, and abbreviations describing desirable job qualifications/ certifications for IS professionals. Count of IT job advertisements and skills were identified by city, and time periods.	Job Advertisement level.

Study	Dataset Size/Date	Occupational coverage	Analytical Output	Unit of Analysis
Maier et al. (2002)	Job ads in the classified sections for five major metropolitan newspapers, The Atlanta Journal Constitution, Chicago Tribune, LA Times, The Tennessean, and The New York Times.	The advertisements were found under MIS-related section headings such as "Computers," "Programmers," "Data Processing," "Systems Analysts," and "Information Systems."	Content analysis of the classified advertisements resulted in four broad Groupings/categories for the job skills: networking and operating systems, programming and software, Internet, and personal characteristics	Job Advertisement level.
Ramezan (2023)	A total of 935 unique Job postings were acquired from Indeed.com on June 18th 2021.	Keywords: "Cybersecurity", "Information Security"	Search Date: June 18, 2021 Manually extracted information from cybersecurity job advertisements, including educational qualifications, professional experience, certifications, security clearances, programming languages, organizational characteristics, and salary information.	Job Advertisement level.

Study	Dataset Size/Date	Occupational coverage	Analytical Output	Unit of Analysis
Jun et al. (2023)	Korean job advertising sites from June 1 – June 19 in each year from: 2014, 2019, 2022, & September 2022	Compared to keywords in national competence standards ("technical skills such as technology development, network, and operating systems are preferred in the actual workplace. In contrast, managerial skills such as the legal system and certification systems are prioritized in vocational training.	Examined South Korean cybersecurity job advertisements collected across multiple time periods to investigate changes in educational requirements, professional experience, company characteristics, and employer expectations.	Job Advertisement level.
Graham & Lu (2023)	Retrieved detailed job descriptions of 17,929 cybersecurity job positions in all 50 states of the United States from Indeed.com. Dates not published	keywords of every job position contain the terms 'cyber' and 'security'.	Applied semantic network analysis to cybersecurity job advertisements and demonstrated that employer expectations extend beyond technical competencies to include broader organizational and professional capabilities.	Job Description level.
Peslak & Hunslinger (2019)	Obtained 487 non-duplicate returned job Descriptions for cybersecurity analyst. On www.postjobfree.com in April 2019.	"Cybersecurity Analyst"	Analyzed cybersecurity job advertisements using word frequencies, collocation analyses, and word clouds to identify the technical skills, certifications, and general competencies most frequently sought by employers.	Job Description level.

Study	Dataset Size/Date	Occupational coverage	Analytical Output	Unit of Analysis
Goupil et al. (2022)	Compared cybersecurity skills identified in job advertisements with university curricula across Switzerland, Austria, and Germany.	"cyber-security" and "it-sicherheit" (cyber-security in German) & the keyword "security" (German: "Sicherheit") should either occur in the job title or at least three times in the job description	3 months of data Extracted skills using keywords from ACM CCS and EU Cybersecurity Taxonomy. Manual comparison of frequencies for skills comparison and an automatic comparison of skills reported substantial differences between employer demand and academic preparation.	
Rahhal et al. (2019)	409 job ads collected from 9 Moroccan job portals from Feb 2017 to Jun 2018.	terms such as "cybersecurity" and the combination of Security and IT.	Examined Moroccan cybersecurity job advertisements and identified discrepancies between employer expectations and university curricula, particularly regarding risk analysis, industry certifications, and English-language proficiency.	Job Advertisement level.
Parker & Brown (2019)	196 Adverts were collected from 5 job portal websites on a weekly basis over a two-month period.	"Cyber Security" and "IT Security"	South Africa Using Content analysis manually analyzed cybersecurity job advertisements in South Africa to examine industries, educational qualifications, years of experience, job levels, and required interpersonal and technical skills	Job Advertisement level.
Budde et al. (2023)	Surveyed both academic and industry experts to identify cybersecurity job profiles and the competencies associated with each of the six roles across Europe		Industry participants emphasized implementation, deployment, and legal competencies, whereas academic participants prioritized conceptual and network-oriented cybersecurity knowledge.	individual

Study	Dataset Size/Date	Occupational coverage	Analytical Output	Unit of Analysis
Brink et al. (2022)	Job Advertisements in South Africa were manually collected and weekly reviewed for possible omission due to position being filled from five online job portals: Careers 24, Indeed, LinkedIn, PNet, and SimplyHired	Keywords used were, "cyber security", "cybersecurity", "IT security, "security"	Classified South African cybersecurity positions according to the CSEC 2017 knowledge framework. The three most occurring roles were IT security specialist, Security/Cyber Analyst, and Cyber Security Officer. 5+ years of experience were most prevalent. Technology-related bachelor's degree and certifications like CISSP, CISM, and CISA was most required. Job advertisements were classified under knowledge areas and knowledge units.	Job Advertisement level.
Furnell (2021)	Dataset not disclosed		Analyzed cybersecurity job advertisements in the United Kingdom using the Chartered Institute of Information Security (CIISec) Skills Framework to better understand cybersecurity workforce shortages via. Role, Salary, and certifications.	Job Advertisement level.
Nautiyal and Rashid (2024)			Proposed a cybersecurity skills profile derived from the cybersecurity body of knowledge to support workforce development, recruitment, and employee evaluation.	
Almeida (2025)	Collected 10 EU-based cybersecurity skills frameworks.		Using qualitative content analysis approach compared cybersecurity competency frameworks across the European Union and argued for more adaptive frameworks capable of incorporating emerging areas such as artificial intelligence security.	Framework level.
Bendler and Felderer (2023)	Analyzed 27 competency models and two additional sources that constituted supplementary material.		Using qualitative content analysis Found substantial alignment among existing cybersecurity competency models despite differences in their organization and intended audiences.	Competency model level.

Table A-1. Literature Review

APPENDIX B

Process of Selecting which O*NET Codes to Include

Two of the authors used keywords to search Lightcast for the appropriate data filtering method when pulling the data. The two authors iterated through different searches using different keywords and O*NET codes reviewing the resulting data. Initially, the authors used O*NET codes 15-1212 (Information Security Analysts) and 15-1299.05 (Information Security Engineers) based only on review of resulting data from Lightcast; however, after additional review of the O*NET taxonomy, the authors added 15-1299.04 (Penetration Testers), 15-1299.06 (Digital Forensics Analysts), and 13-1199.07 (Security Management Specialists). We excluded other O*NET codes such as 11-3013.01 (Security Managers) because while this describes security jobs, rarely do security professionals begin as management. We also excluded jobs that were peripherally cybersecurity such as cybersecurity sales with this filtering. While the authors intentionally chose these O*NET codes, other selections may have resulted in different findings.

APPENDIX C

Description of Skill Cluster Labeling Process and Skill Cluster Definitions

All authors and an additional faculty member reviewed and discussed the results in a room. Several in this group had taught cybersecurity classes, conducted cybersecurity research, and/or maintained industry connections through program advisory boards, professional organizations, or individual professional connections. The group discussed and resolved any disagreements.

Skill Cluster	Top 10 Terms (by Weight)
Government, Risk, and Compliance	auditing; certified information system auditor; certified information security manager; risk analysis; risk management; governance; certified information systems security professional; management; governance risk management and compliance; certified in risk and information systems control
Software Development	C; Python; Java; threat modeling; software development; application security; automation; secure coding; Open Web Application Security Project; CI/CD
Information Assurance and Risk Management Frameworks	risk management framework; Top Secret Sensitive Compartmented Information; information systems security; plan of action and milestones; information assurance; authorization; Top Secret clearance; security clearance; assessment and authorization; risk analysis
Cyber Threat Intelligence and Incident Response	cyber threat intelligence; incident response; security information and event management; MITRE ATT&CK framework; vulnerability management; GIAC certifications; endpoint detection and response; cyber threat hunting; cyber operations; operating systems
Professionalism and Leadership	communication; leadership; detail oriented; Microsoft Office; interpersonal communications; problem solving; project management; writing; customer service; decision making
Endpoint Management	Microsoft; Microsoft Intune; Microsoft Certified Professional; Windows PowerShell; Microsoft Teams; Microsoft SharePoint; troubleshooting; scripting; Office Exchange Online; OneDrive for Business
Network and Infrastructure Security	firewall; virtual private networks; infrastructure security; network security; IT security architecture; Fortinet; security solutions; network troubleshooting; intrusion detection systems; Microsoft Azure
Identity and Access Management	identity and access management; authentication; Active Directory; single sign on; Security Assertion Markup Language; OAuth; Lightweight Directory Access Protocols; IdentityIQ; Okta; privileged access management
Cloud Security	NIST; software as a service; infrastructure as a service; platform as a service; Amazon Web Services; cybersecurity compliance; Certified Cloud Security Professional; cloud security; Microsoft Azure; cloud services

Table C-1. Skill clusters derived from topic modeling

APPENDIX D

Top 10 Job Titles by Frequency Associated with Each Skill Cluster

Job Title	Number of Job Advertisements
Cybersecurity Specialists	156
Cybersecurity Analysts	114
Information Security Analysts	85
Client Management Interns	60
Cybersecurity Engineers	55
Tier 3 Support Engineers	51
IT Auditors	48
Cybersecurity Managers	48
Security Governance Managers	46
Directors of Cyber Security	45

Table D-1. Top 10 job titles associated with the Government, Risk, and Compliance skill cluster

Job Title	Number of Job Advertisements
Application Security Engineers	254
Security Engineers	163
Cybersecurity Engineers	111
Cloud Security Engineers	89
DevSecOps Engineers	69
Product Security Engineers	53
Site Reliability Engineers	48
Infrastructure Security Engineers	42
Unclassified	33
Offensive Security Engineers	27

Table D-2. Top 10 job titles associated with the Software Development skill cluster

Job Title	Number of Job Advertisements
Information Systems Security Officers	343
Cybersecurity Engineers	165
Cybersecurity Specialists	157
Cybersecurity Analysts	81
Information Assurance Engineers	60
Unclassified	54
Tier 3 Support Engineers	51
Information Systems Security Managers	48
Information Systems Security Engineers	46
Information Security Analysts	45

Table D-3. Top 10 job titles associated with the Information Assurance and Risk Management Frameworks skill cluster

Job Title	Number of Job Advertisements
Cybersecurity Analysts	179
Cybersecurity Engineers	130
Security Engineers	92
Information Security Analysts	84
Information Security Engineers	79
Vulnerability Management Analysts	73
Unclassified	63
Lead Cybersecurity Engineers	56
Cyber Defense Incident Responders	55
Cyber Threat Analysts	49

Table D-4. Top 10 job titles associated with the Cyber Threat Intelligence and Incident

Response skill cluster

Job Title	Number of Job Advertisements
Electronics Technicians	55
Cybersecurity Engineers	54
Security Engineers	53
Unclassified	46
Information Assurance Security Analysts	45
Information Security Analysts	40
Directors of Cyber Security	38
Cybersecurity Managers	38
Cybersecurity Project Managers	36
Cybersecurity Analysts	32

Table D-5. Top 10 job titles associated with the Professionalism and Leadership skill cluster

Job Title	Number of Job Advertisements
Policy Administrators	52
Microsoft Consultants	36
Security Engineers	22
Cybersecurity Analysts	13
Windows Engineers	12
Security Operations Engineers	11
Cyber Consultants	9
Unclassified	9
Cybersecurity Engineers	9
Endpoint Engineers	8

Table D-6. Top 10 job titles associated with the Endpoint Management skill cluster

Job Title	Number of Job Advertisements
Network Security Engineers	86
Security Architects	51
Data Protection Specialists	48
Network Infrastructure Consultants	47
Network Infrastructure Managers	45
Cybersecurity Engineers	43
Industrial Control Systems Cybersecurity Consultants	28
Security Engineers	24
Cybersecurity Analysts	19
Information Security Advisors	18

Table D-7. Top 10 job titles associated with the Network and Infrastructure Security skill cluster

Job Title	Number of Job Advertisements
Security Engineers	81
Identity and Access Management Managers	58
Cybersecurity Engineers	47
IAM Engineers	40
Unclassified	37
Identity and Access Management Engineers	28
IAM Security Engineers	25
Information Security Analysts	19
Information Security Engineers	18
Sailpoint Engineers	16

Table D-8. Top 10 job titles associated with the Identity and Access Management skill cluster

Job Title	Number of Job Advertisements
Cybersecurity Specialists	62
Cybersecurity Software Engineers	53
Information Systems Security Engineers	51
Information Security Program Managers	51
GPS Technicians	50
Cloud Security Engineers	41
Recovery Managers	27
Cybersecurity Engineers	27
Security Governance Managers	20
Security Engineers	18

Table D-9. Top 10 job titles associated with the Cloud Security skill cluster