

Impacts of Artificial Intelligence (AI) on Cybersecurity Workforce

Ping Wang, *Robert Morris University*, wangp@rmu.edu

Noory Etezady, *Robert Morris University*, etezady@rmu.edu

Nader Kesserwan, *Robert Morris University*, kesserwan@rmu.edu

Abstract

The rapid technical developments in AI, and generative AI (GenAI) in particular, have brought about substantial opportunities for growth and challenges for workforce in many industries. This research reviews the general positive and negative impacts of AI on workforce and employment. The focus of this study is on the impacts of AI on the professional competencies or KSAs (knowledge, skills, and abilities) for the cybersecurity workforce in the United States. The research direction is based on an adapted Cybersecurity Competency Model including traditional tiers of cybersecurity KSAs with new qualifications for AI and strategic leadership. The research goal is to discover the effects of AI on specific qualifications or KSAs for major job titles in the U.S. cybersecurity workforce based on cybersecurity job posting data collected from both public and private sectors. The quantitative and longitudinal method for this study includes collecting and analyzing cybersecurity position postings in public and private sectors in the United States in the past five years (2022-2026). The findings of this study indicate a consistent emphasis on traditional professional KSAs along with an emerging but fast growing trend of AI-related skills for both public and private cybersecurity positions.

Keywords: Artificial intelligence (AI), cybersecurity, workforce, competency, KSAs

Introduction

The public release of ChatGPT by OpenAI in November 2022 has popularized artificial intelligence (AI), and generative AI (GenAI) in particular, for rapidly increasing efficiency and automation of work tasks in many fields. Meanwhile, the increasing adoption of AI and recent advances in GenAI have led to public concerns and anxiety that AI may cause job losses, diminish workforce demand, and may eventually replace human workers (Gimble et al., 2026; Hampole et al., 2025). The most comprehensive study on this issue so far is the joint research project titled “Artificial Intelligence and the Labor Market” done by researchers at MIT, Yale, and Northwestern universities (Hampole et al., 2025). Their research examines how AI adoption affects company dynamics and labor demand by measuring workers’ task-level exposure to AI and machine learning across various firms and occupations from 2010 through 2023. Their finding is that the overall effects of AI on labor demand is modest as the reduced demand in certain occupations with high AI exposures is offset by higher employment growth across firms with AI adoption leading to productivity growth and business scale expansion (Hampole et al., 2025; Murray, 2025). The latest study by Goldman Sachs Research indicates that potential impact of AI on labor, despite many uncertainties, is expected to grow in the next 10 years but AI may also help to create new jobs such as in industries supporting data centers to sustain the AI boom (Goldman Sachs, 2026). It is therefore important to find out what impacts does AI have actually on the workforce and labor demand.

Given wide variations of workforce dynamics across industries and countries with different economies, priorities, and policies, the focus of this research is on the impact of AI on cybersecurity workforce in the

United States. The projection for workforce demand for cybersecurity in the U.S. remains strong and steady. The market demand for information security analysts as a typical cybersecurity career is projected to grow at 29% during the 10-year period of 2024-2034, substantially higher than the 9% growth rate of all computer occupations and the 3% growth rate of all occupations (US BLS, 2026). GenAI is increasingly used in the cybersecurity industry. GenAI has the potential and capability to improve the efficiency, accuracy, and effectiveness of threat detection and analysis as well as pentesting process and vulnerability assessment; however, it is also a double-edged sword with risks of malicious misuse of AI tools for automated and powerful cyber attacks (Wang & D'Cruze, 2024; Wilson, 2023). For example, Anthropic limited its initial release of the Claude Mythos AI model to about 40 companies only for defensive security work due to its capability to identify software weaknesses and flaws that could be exploited by bad actors (Capoot, 2026). Given the increasing role of AI in cybersecurity tasks, it is a significant research problem to look into the impacts of AI on the cybersecurity workforce in the U.S.

The goal of this research is to discover the impacts of AI on the U.S. cybersecurity workforce competencies and demand. Specifically, this study will use cybersecurity jobs data collected from both public and private sectors in the past five years to address the following research questions:

1. What are the major competencies or KSAs identified from the cybersecurity jobs data?
2. What are the AI-related competencies or KSAs identified from the cybersecurity jobs data?
3. Is there any trend of the AI-related competencies or KSAs identified from the cybersecurity jobs data?

For this research, competencies and KSAs (knowledge, skills, and abilities) are synonymous and exchangeable with each other. This study will propose an adapted Cybersecurity Competency Model with comprehensive tiers of competencies or KSAs to guide the quantitative study and data analysis. The following sections will review relevant background literature, present the proposed Cybersecurity Competency Model, describe the methodology for data collection and analysis, and discuss the findings and conclusions.

Background

AI Impacts on General and IT Workforce

There have been divergent research findings on the impacts of AI on human workforce, including decreased need for human participation and involvement in workplace threatening employees' job security. On the other hand, AI has the potential to make employees more efficient and enhance the overall organizational performance. Nevertheless, certain perceived shortcomings of AI, such as the absence of emotional intelligence, deficiency of in-depth contextual knowledge, over-dependence on data quality, and deficiency in ethical and moral decisions, make it hard for AI to replace human intelligence (Akinwale, 2024). To better understand the impact of AI on the general and IT workforce, a review of recent literature is conducted using major databases including ACM, AIS eLibrary, EBSCO, IEEE eJournals, ProQuest Computing, Scopus, and Springer e-Journals during the past five years. Keywords used in the search include AI, artificial intelligence, impact, workforce, information technology, and IT. A total of 35 articles are identified from the search. Table 1 below summarizes the research publications deemed to be most relevant to this study and lists them in reverse chronological order starting with the most recent publication.

Table 1. Summary of Research on AI Impacts on General and IT Workforce

Year	Author	Methodology	Key Findings and Limitations
2026	Wang et al.	Quantitative survey	• Immediate AI knowledge significantly and negatively predicted adolescents' preferences for both low-and high-replaceable jobs. • Limited data collection from a middle school in southwest China.
2025	Akinwale et al.	Cross-section survey	• AI lacks emotional intelligence, in-depth contextual knowledge, and ethical and moral decision analysis with over-reliance on data quality. • The study is limited to customer services officers of banks, telecom customer agents, and retail organizations customer agents in Nigeria.
2025	Anto	Mixed-method	• AI chatbots can improve decision-making and productivity. • The Study is limited to customer service, human services, and administrative functions.
2025	Bonfiglioli et al.	Statistical modeling	• AI can automate jobs or complement workers. • Data is limited to 2000-2020 missing the AI growth in recent years.
2025	Dahiya	Systematic literature review	• AI is neither a purely destructive nor purely constructive but a transformational technology that reconfigures the nature, quality, and distribution of work. • The review is up to 2023 with English articles only and focusing only on the socio-economic implications.
2025	Smitha et al.	Mixed method	• A set of issues including data privacy, technical, and implementation must be resolved to harness AI effectively in learning. • The study is limited to IT professionals in Bengaluru and India.
2025	Wu et al.	Two-wave survey	• Increased AI usage can significantly heighten job insecurity among employees leading to their moonlighting for additional resources. • The study relies on self-reported data with potential bias.
2025	Xavier et al.	Mixed method	• There is a significant increase in job autonomy following AI integration across all participants. • The study is limited to small effect-sizes observed, which often fail to fully capture the complexities of real-world workplaces.
2024	Yu et al.	Quantitative quasi-experimental design	• Exposure to GenAI shows no significant negative impact on employment but a positive effect on labor productivity. • The data used for this study might be dated given the rapid AI development. A new study with more recent data will be beneficial.
2024	Kan et al.	Literature review	• Organizations need to strategically integrate specific AI technologies to meet their sectors' unique needs. • Literature is limited to 24 papers from only two sources.
2024	Santoni De Sio	Programmatic research	• Raises 7 ethical issues resulting from the introduction of AI. • The research is theoretical with no empirical validation.
2022	Perez et al.	Qualitative interviews	• Employees respond to AI by changing task and relationship boundaries and cognitively reframe their jobs. • The interviews are limited to 27 employees in a French bank.

The above literature review indicates that AI can be used to automate jobs or assist workers in performing their tasks, which may vary with industry sectors. The AI impact is more on service jobs than manufacturing and will negatively impact low-skill and production workers while it positively impacts high-wage earners

and workers in STEM careers and widens inequality by automating jobs (Bonfiglioli et al., 2025). There are ethical issues associated with the introduction of AI which need to be considered, including how to deal with the impact of AI on job losses and the social issues that emerge in the job market. AI may contribute to new forms of oppression and rights violation in the workforce, may create hidden labor or insufficient recognition of economically valuable tasks performed by humans, and increase of socio-economic power over people by technological companies (Santoni De Sio, 2024).

AI Impacts on Cybersecurity Industry

The recent AI evolution has significantly influenced the development of more sophisticated cyberattacks and countermeasures. AI-driven attacks have increased in frequency and impact, necessitating more advanced security measures to protect networks (Jada & Mayayise, 2024). GenAI can be used to support cybersecurity efforts through advanced detection, analysis, and response (Balasubramanian et al., 2025). However, the use of AI in cybersecurity presents notable challenges. Main concerns include data privacy and security, as GenAI can generate highly realistic content that may be exploited for identity theft, fraud, and reputational damage (Balasubramanian et al., 2025). Therefore, developing a comprehensive understanding of AI's impact on cybersecurity is essential for effectively identifying and mitigating AI-driven threats. Table 2 below lists in reverse chronological order and summarizes recent and most relevant research on AI impacts on cybersecurity up to March 2026 from these databases: ACM, AIS eLibrary, EBSCO, IEEE eJournals, ProQuest Computing, Scopus, and Springer e-Journals.

Table 2. Summary of Research on AI Impacts on Cybersecurity

Year	Author	Methodology	Key Findings and Limitations
2026	Mohammed et al.	Literature review	• Adopting an ethical and responsible approach is essential to equitable and effective implementation of AI-driven advancements. • Limited coverage of security in traditional symbolic AI technologies.
2025	Balasubramanian et al.	Literature review	• GenAI plays a vital role in improving threat detection, analysis, and response as cyber threats evolve in complexity. • GenAI serves as a powerful generator of deepfakes, creating realistic but malicious content. • Limitations – The study used secondary sources such as literature and case studies without real-world validation.
2025	Datta & Acton	Case study	• The escalating complexity and challenges of AI have an ever-growing impact on the cybersecurity landscape. • Limitations - The study is based on a fictional insurance company.
2025	Jones et al.	Experimental	• Specific LLMs demonstrate distinct strengths suitable for various stages of incident management. • Ethically, reliance on AI introduces risks, including the potential erosion of human expertise and critical thinking within security teams. • This experimental research was limited to OpenAI ChatGPT variants.
2025	Kavya et al.	Mixed method	• Deep learning models CNN and LSTMs provide high accuracy in the detection of phishing attacks, especially in the area of content and URL analysis of web content as well as phishing patterns in emails. • Limitations – Contextual awareness and behavioral analysis need to be studied.
2025	Lier et al.	Design Science Research	• Contributes a process model for successful implementation of AI for cybersecurity.

Year	Author	Methodology	Key Findings and Limitations
			• Limitations – The interviewed experts did not have direct experience with the applications and services or their implementation.
2025	Metin et al.	Explanatory-sequential mixed method	• Contributes an eight-stage operation framework that leverages AI for enhanced Business Logic Vulnerabilities detection and mitigation. • Limitations – The proposed framework has not been empirically tested and evaluated in real-world environments.
2025	Syllaidopoulos et al.	Illustrative case study	• AI-based security systems must include commitments to ethical principles, operational transparency, and international cooperation. • Limitations – The case studies do not support the main conclusion.
2024	Hasanov et al.	Literature review	• LLMs have remarkable efficacy in phishing attack simulations and in cybersecurity governance. • AI and LLMs substantially reduce the entry barriers for hackers and offer great benefits for penetration testers. • Limitations – The review is based on a limited number of AI models.
2024	Nowrozy	Secondary research based on the NICE framework	• Key findings include ChatGPT's ability to automate routine tasks, its limitations in critical thinking, and the necessity for a shift from memorization to critical thinking in education and certifications. • Limitations – Managerial aspects are omitted. It does not cover the full range of cybersecurity roles.
2024	Schmitt & Flechais	Mixed method	• The integration of Generative AI can profoundly amplify the effectiveness of social engineering attacks. • Limitation – The qualitative part, the literature search, was limited.

The literature review above shows that AI could strengthen cybersecurity by automating processes, predicting threats, enhancing infrastructure security, managing vulnerabilities, and supporting decision-making, thereby improving overall system resilience (Jada & Mayayise, 2024). At the same time, it introduces increased risks by enabling attackers to automate vulnerability discovery, attack coordination and exploitation. For instance, AI tools such as Anthropic's Mythos can detect complex software vulnerabilities, helping to improve security, but they may also be leveraged by adversaries to identify weaknesses and launch attacks (Subin & Son, 2026; Capoot, 2026). Thus, robust governance frameworks are necessary to ensure fairness, accountability, and trust in AI applications (Ibrar et al., 2025; Syllaidopoulos et al., 2025). Additionally, collaboration among academia, industry, policymakers, and regulatory bodies is essential for developing effective legal and ethical frameworks that maximize the benefits of AI while minimizing its risks in cybersecurity (Jabbarova, 2024).

Industry Expectations for Cybersecurity Workforce

It is necessary to include workforce expectations and guidance for the cybersecurity industry for measuring the AI impacts on cybersecurity workforce. This section reviews the major models and frameworks that provide expectations and guidance on the professional competencies or KSAs for the U.S. cybersecurity industry and workforce. These guidance models and frameworks include publications by the U.S. DoD (Department of Defense), the largest employer in the U.S., as well as NIST/NICE (National Initiative for Cybersecurity Education), and the U.S. Department of Labor. Table 3 below lists the models and frameworks in reverse chronological order and summarizes their main contributions and limitations.

Table 3. Summary of Industry Expectations for U.S. Cybersecurity Workforce

Year	Author	Publication Title	Key Contributions and Limitations
2025, Aug 4	U.S. DoD (Department of Defense)	DoD Cyber Workforce Framework Tool (DCWF) Tool Version 5.1	• Includes specific cyber workforce elements, work roles, job codes, work role definitions. • Includes data/AI work element and work roles such as AI/ML specialist, AI adoption specialist, and AI innovation leader. • Focus on technical KSAs with limited coverage on non-technical KSAs.
2025, Apr 28	NIST/NICE (National Initiative for Cybersecurity Education)	NICE Framework (workforce framework for cybersecurity) version 2.2.0	• Includes cybersecurity work role categories, work roles, competency areas, and task, knowledge, and skill statements. • Includes technical and some non-technical KSAs such as communication skills. • Includes a new competency area in AI but has limited details on KSAs.
2020	Wang et al.	The Role of Industry Partnerships and Collaborations in Information Technology Education	• Focuses on cybersecurity education and workforce in developing KSAs. • Emphasizes industry partnerships and collaboration in KSA development. • Highlights cybersecurity leadership as a key KSA for cyber workforce. • Does not address AI in KSA development.
2014	U.S. Department of Labor (DoL)	Cybersecurity Competency Model	• Includes five tiers of competencies for the cybersecurity workforce. • Contributes a systematic model addressing both technical and non-technical competencies for the entire cybersecurity workforce ecosystem. • Does not address AI in cybersecurity competency development.

The above summary of major expectations and guidance for the U.S. cybersecurity workforce shows the progressive development of industry expectations on the general competencies and KSAs for the cybersecurity workforce. These expectations address various aspects of the cybersecurity profession and workforce ecosystem, including both technical and non-technical qualifications, such as professional communication skills, leadership skills, and personal lifelong learning skills. Moreover, the review of the background literature shows the emerging and evolving development of AI in cybersecurity competencies.

Cybersecurity Competency Model

Figure 1 below presents a comprehensive Cybersecurity Competency Model with tiers of KSAs. The proposed model is adapted from the U.S. Department of Labor cybersecurity competency model (US DoL,

2014). The adapted model consists of five tiers of competencies based on the US DoL model while incorporating new competencies or KSAs related to AI for cybersecurity. Here are the proposed five tiers of competencies and their definitions:

- Tier 5 – Management/Leadership Competencies: KSAs for effectively managing and leading cybersecurity programs, projects, and businesses with a strategic vision and innovation, policy, and governance for using AI for cybersecurity.
- Tier 4 – Industry-wide Technical Competencies: KSAs applicable to cybersecurity and AI technology solutions, risk management, incident response.
- Tier 3 – Workplace Competencies: Professional KSAs including teamwork, organization, creative thinking, problem solving, decision making, and fundamental business skills.
- Tier 2 – Academic Competencies: KSAs for verbal and written communication, analytical thinking, and for screening and adopting effective IT and AI solutions.
- Tier 1 – Personal Effective Competencies: KSAs for interpersonal interaction, ethical judgement and integrity, professionalism, flexibility, adaptability, reliability, and lifelong learning for acquiring new KSAs.



Figure 1. Proposed Cybersecurity Competency Model

Methodology

This study adopts a quantitative longitudinal research design to investigate the impact of AI on cybersecurity workforce with a specific focus on the KSAs reflected in job postings in the U.S. The research leverages structured datasets derived from real-world job listings across both public and private sectors, which were collected using Python programs that interface with the APIs of each sector to automate data

extraction (Mishra, 2025). Job postings are treated as empirical proxies for labor market demand, enabling the identification of evolving skill requirements and the growing influence of AI-related competencies (Markel, Tale, & Belz, 2025). A longitudinal approach is used to capture temporal trends and compare workforce requirements across a five-year period (2022-2026), particularly distinguishing between pre-COVID and post-COVID labor market dynamics. This methodology is appropriate because job postings provide direct and observable evidence of employer expectations, and the integration of AI-related keywords allows for systematic measurement of AI's impact on cybersecurity roles.

Public and Private Sector Datasets

The public sector dataset consists of cybersecurity-related job postings in the U.S. collected from USAJobs. These datasets include major cybersecurity works roles, such as Information Security Specialist, IT Cybersecurity Specialist, Security Risk Analyst, and Senior Cyber Offense Specialist. This dataset captures structured attributes such as job title, agency, job description, required qualifications, and posting dates. The private sector dataset includes job postings aggregated from platforms such as LinkedIn, Indeed, and Adzuna. The dataset fields include company name, job title, job description, required skills, and location.

Data Collection Process (Pre-Collected Data)

The datasets were collected prior to analysis and stored in Excel files. The data collection process involved targeted keyword-based searches using terms, such as Cybersecurity Analyst, Information Security, Cybersecurity Specialist, AI, Machine Learning, and related terms. For private sector data, APIs (e.g., Adzuna API) and automated scraping tools were used to extract job postings. Public sector data was retrieved from USAJobs using structured queries. The following measures were taken to ensure data quality (Creswell & Creswell, 2017):

- Duplicates across platforms were identified using job title, organization, and textual similarity.
- Redundant entries were removed during preprocessing.
- Inconsistent formatting across sources was standardized within Excel.

Timeframe

The analysis covers a five-year period (2022–2026), enabling a comparison of cybersecurity workforce requirements before and after the COVID-19 pandemic. The timeframe is divided into two parts: (1) Pre-COVID/Post-early pandemic baseline period; and (2) Post-COVID period (increased digital transformation and AI adoption). Temporal analysis is conducted using the posting date fields available in the Excel datasets, allowing for trend identification in AI-related skill demand over time.

Data Categories and Preprocessing

Each Excel dataset includes structured columns, including Job Title, Organization, Job Description, Required Skills/Qualifications, Location, and Posting Date.

The following preprocessing steps were performed to prepare the datasets for analysis:

- **Data Cleaning:** Removal of null values, duplicates, and incomplete records
- **Normalization:** Standardization of text (lowercasing, punctuation removal)
- **Tokenization:** Breaking job descriptions into analyzable text units
- **Stop-word Removal:** Eliminating non-informative words

KSA Identification and Categorization

KSAs were extracted from job descriptions and categorized into four primary groups:

- **Technical Cybersecurity Skills** (e.g., network security, penetration testing)
- **AI/ML-Related Skills** (e.g., machine learning, AI tools, automation)
- **Soft Skills** (e.g., communication, teamwork, critical thinking)
- **Business/Management Skills** (e.g., risk management, compliance, leadership)

A **multi-label classification approach** was used, as each job posting may include multiple KSAs across categories.

AI Tools and Prompts for Data Analysis

AI tools such as ChatGPT (OpenAI, 2023) and Gemini (Google, 2024) were used to enhance data analysis. These tools supported extraction of KSAs from unstructured job descriptions, identification of AI-related terminology and competencies, and classification of job roles into cybersecurity domains. These steps were taken to ensure reliability: (1) AI-generated outputs were cross-validated with manual sampling; (2) Consistency checks were applied across multiple prompts; and (3) iterative refinement was used to improve classification accuracy. In addition, the following prompts were used and refined iteratively with repeated testing to ensure consistency, completeness, and minimal ambiguity.

a) KSA Extraction Prompt: “Extract and categorize all KSAs from the following job description into technical, AI-related, soft, and business skills.”

b) AI Skill Identification Prompt: “Identify all AI, machine learning, or automation-related skills mentioned in this job description.”

c) Job Classification Prompt: “Classify this cybersecurity job into offensive, defensive, or GRC categories based on responsibilities.”

This study uses the following data analysis techniques (Field, 2024):

- Frequency analysis was used to count occurrences of KSAs across datasets and measure the prevalence of AI-related skills;
- Trend analysis was conducted to track changes in skill demand over time and compare pre- and post-COVID periods;
- Comparative analysis examined differences between public and private sector job requirements, particularly in AI adoption;
- The impact of AI was quantified using the frequency of AI-related keywords, the proportion of job postings requiring AI skills, and the growth rate of AI-related KSAs over time; and
- Finally, data visualization was performed using Excel tools, including bar charts to illustrate KSA distributions, line graphs to show temporal trends, and comparative charts to highlight differences between sectors.

Findings and Discussions

The analysis of cybersecurity job postings from both datasets reveals distinct patterns in the distribution of Knowledge, Skills, and Abilities (KSAs), across the private-sector dataset (N = 576), and the public-sector dataset (N = 11,434).

Public Sector

A total of **11,434 job postings** across ten cybersecurity work roles were analyzed: *Cybersecurity*, *Security Analyst*, *Cyber Analyst*, *Information Security*, *Security Operations Center Analyst*, *Security Engineer*, *Cloud Security*, *Threat Intelligence*, *Penetration Tester*, and *Cyber Defense*. For each posting, the **job title and description** fields were analyzed using a keyword-based approach to identify the presence of selected

Knowledge, Skills, and Abilities (KSAs) categories. The following KSA categories based on the proposed Cybersecurity Competency Model were examined:

- AI / Generative AI
- Machine Learning / Deep Learning
- Large Language Models (LLMs)
- Creative / Critical Thinking
- Business / Management Skills
- Communication Skills
- Teamwork Skills
- Lifelong Learning / Professional Development
- Cybersecurity Technical Skills

Because job postings may reference multiple skills simultaneously, an additional analysis was conducted to measure the **relative share of total skill mentions**. The total number of skills mentions identified across the dataset is 18,832. Table 4 below shows the KSA distribution in public-sector cybersecurity job postings. Percentages were normalized relative to this total using this formula:

$$\frac{\text{Count of jobs mentioning a KSA Category}}{\text{Total Jobs}} * 100$$

Table 4. KSA Distribution in Public-Sector Cybersecurity Job Postings (N = 18,832)

KSA Category	Count	Percentage (%)
AI / GenAI	666	3.54
ML / DL	77	0.41
LLM	21	0.11
Creative / Critical Thinking	66	0.35
Business / Management	3,408	18.09
Communication	391	2.08
Teamwork	4,557	24.19
Lifelong Learning	653	3.47
Cybersecurity Technical	9,393	49.86
Total Skill Mentions	18,832	100

Across all datasets, cybersecurity technical competencies and teamwork skills consistently appear as the most common requirement, followed by business and management skills. The relative absence of AI-related requirements across all roles suggests that AI expertise has not yet become a standard requirement in cybersecurity job descriptions. Figure 2 and Figure 3 below are generated to visualize the distribution of the skill mentions: The bar chart in Figure 2 illustrates the absolute number of times each skill category was mentioned across all public sector postings. The pie chart in Figure 3 shows the relative share of total skill mentions in the normalized distribution of KSAs across all public sector cybersecurity job postings. These visualizations reinforce the finding that management, leadership, and collaboration competencies remain central to cybersecurity job requirements, while AI-related competencies appear only sporadically.

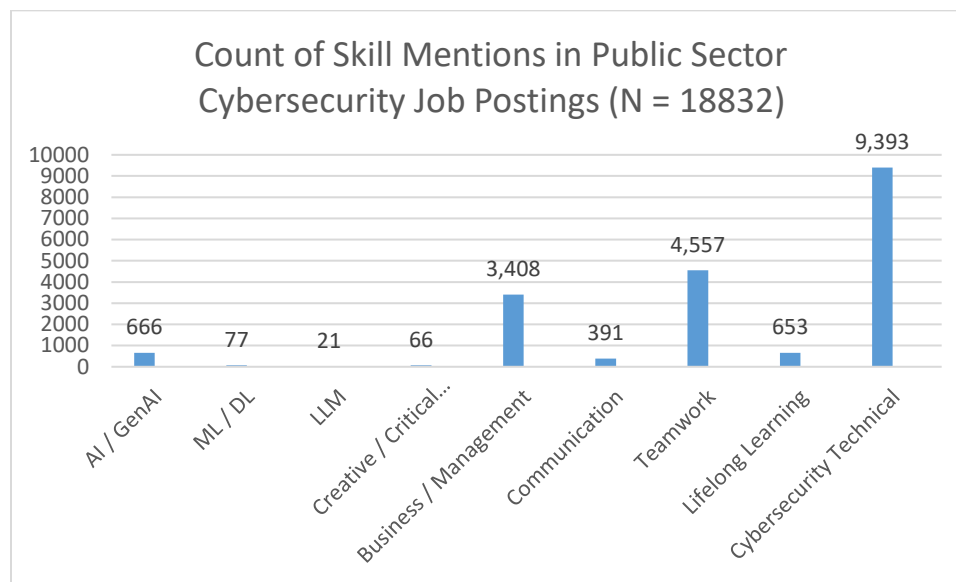


Figure 2. Count of Skill Mentions by KSA Category In Public Sector Job Postings

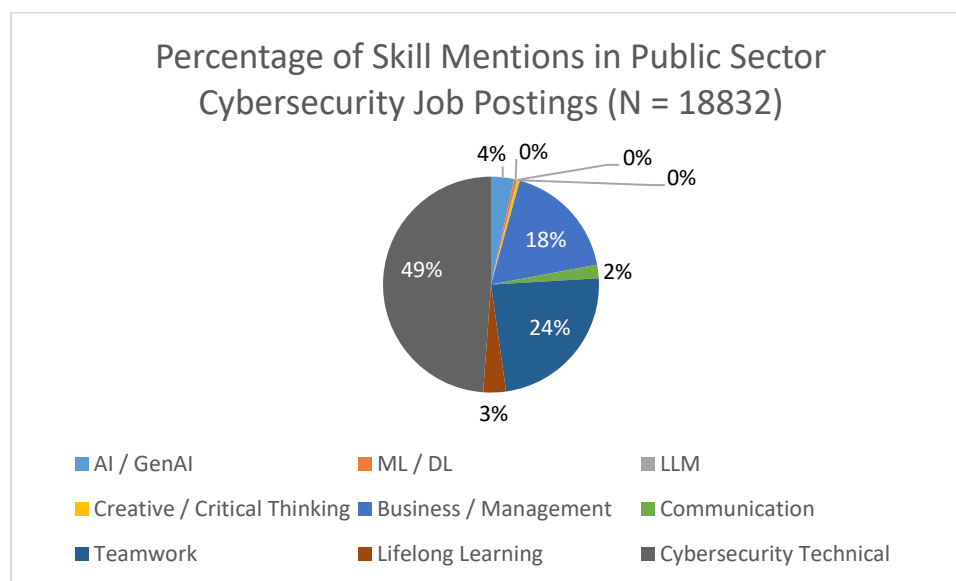


Figure 3. Relative Share of Skill Mentions In Normalized Distribution of KSAs across Public Sector Postings

B. Private Sector

Cybersecurity job posting data was collected from the private sector listings including Indeed and LinkedIn. A total of **576 job postings** across four cybersecurity roles were analyzed: Cyber Offense Specialist, Security Risk Analyst, IT Cybersecurity Specialist, and Information Security. For each posting, the **Duties** and **Requirements** sections were analyzed using a keyword-based search approach to identify the presence of selected **KSA** categories. The same KSA category for the public is used for the private sector. Table 5 below shows the distribution of mentions by KSA category across private sector data.

Table 5: Distribution of Skills Mentioned in Private Sector Postings (N = 429)

Skill Category	Count	Percentage (%)
AI / GenAI	3	0.70%
ML / DL	0	0.00%
LLM	1	0.23%
Creative / Critical Thinking	1	0.23%
Business / Management	129	30.07%
Communication	83	19.35%
Teamwork	61	14.22%
Lifelong Learning	65	15.15%
Cybersecurity Technical	86	20.05%
Total Skill Mentions	429	100%

Among all private sector cybersecurity job postings, management or leadership skills account for approximately 30% of all skill mentions, followed by cybersecurity technical skills (20%) and communication skills (19%). Teamwork and lifelong learning competencies account for 14% and 15% respectively, highlighting the importance of collaboration and continuous professional development in cybersecurity careers.

AI-related competencies remain minimal, representing less than 1% of total skill mentions, indicating that while AI technologies are advancing rapidly, they have not yet become a dominant skill requirement in cybersecurity job postings.

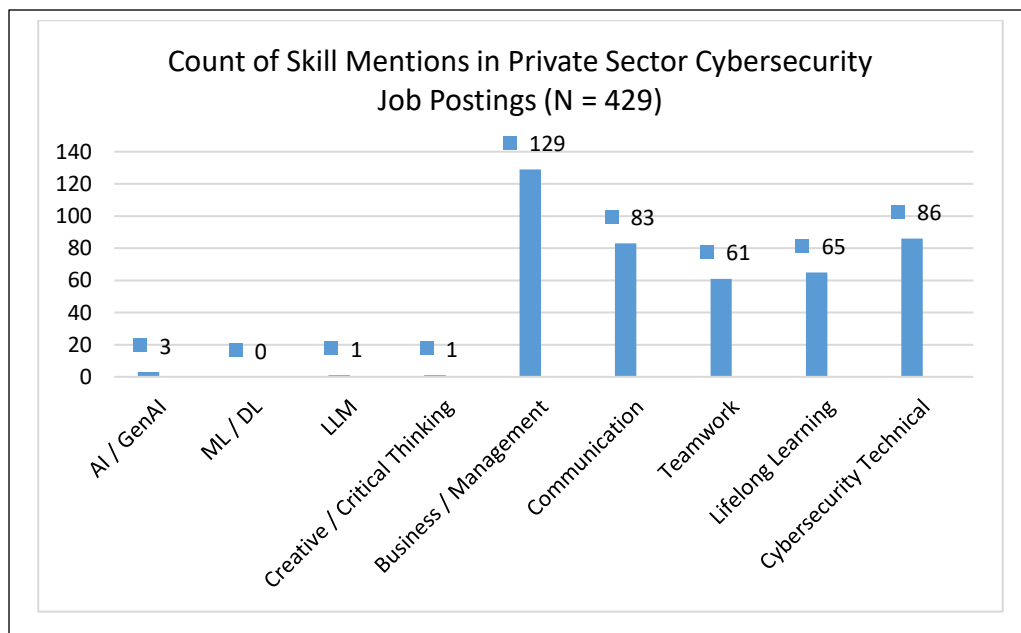


Figure 4. Count of Skill Mentions by KSA Category In Private Sector Job Postings

These visualizations are consistent with the finding on public sector postings that leadership, technical, and collaborative competencies remain central to cybersecurity job requirements while AI-related competencies appear to lag behind in postings.

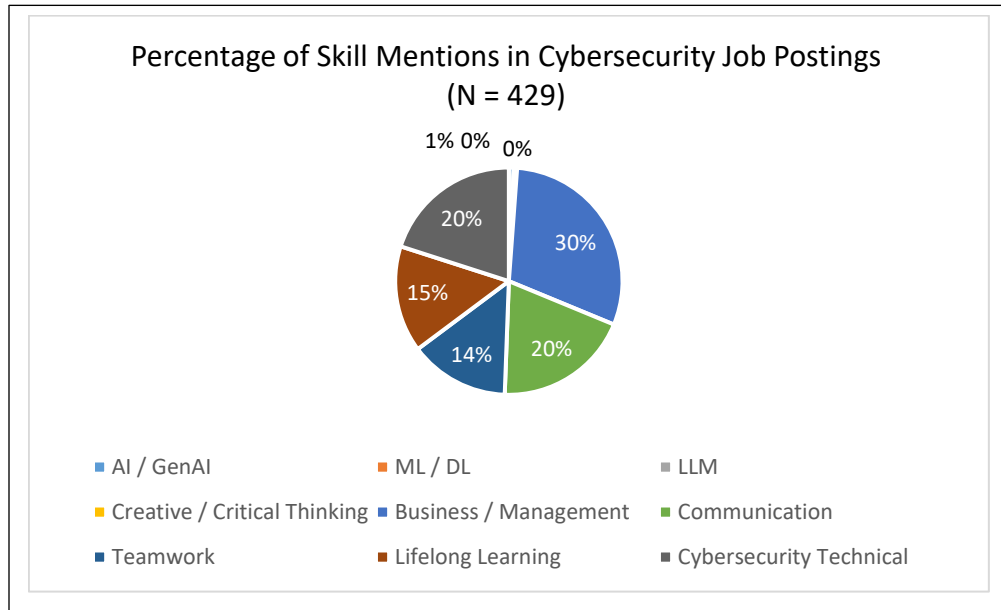


Figure 5. Relative Share of Skill Mentions In Normalized Distribution of KSAs across Private Sector Postings

Pre/Post COVID-19 Periods

Public and private sector cybersecurity job postings in the U.S. are grouped by year and consolidated into COVID-19 periods (transition, early post-COVID, post-COVID). AI-related postings were identified using keyword-based searches (e.g., “AI,” “machine learning,” “automation”) within job titles and descriptions. The total number of postings and the number containing AI-related terms were counted for each period, and the AI share (%) was calculated as the proportion of AI-related postings relative to the total number of postings in that period. It is important to note most of the public sector postings were collected in 2026 with only a limited number of postings available from earlier years. An additional analysis was conducted to measure the relative share of total skill mentions as postings may reference multiple skills simultaneously.

Table 6: Normalized AI Skill Presence Pre/Post COVID-19 Period

Period	Years Covered	Total Job Postings	Job Postings with AI Terms	AI Share (%)
Pre-COVID	≤ 2019	<i>Not available in dataset</i>	<i>Not available</i>	<i>N/A</i>
Transition	2020–2021	2	0	0.00
Early Post-COVID	2022–2023	47	0	0.00
Post-COVID	2024–2026	11,961	1,028	8.59

Table 6 indicates a clear temporal shift in the presence of AI-related competencies within cybersecurity job postings. No data is available for the pre-COVID period (≤2019), limiting direct baseline comparison. During the transition (2020–2021) and early post-COVID (2022–2023) periods, AI-related skills are absent, with 0% of postings referencing AI terms.

In contrast, the post-COVID period (2024–2026) shows a notable increase, with **8.59% of job postings including AI-related requirements**. This pattern suggests that the integration of AI into cybersecurity

roles is a relatively recent development, gaining momentum after the pandemic. The sharp rise in AI-related mentions likely reflects increased adoption of AI-driven tools and automation in cybersecurity practices, although the overall proportion indicates that AI remains an emerging rather than dominant requirement.

Overall Findings

Several key findings emerge from the analysis of the public and private sector job posting datasets. First, cybersecurity technical skills and business/management or leadership competencies remain the most dominant requirements across both datasets. Second, AI-related KSAs remain relatively low overall but show a clear emerging and rapid upward trend post COVID-19, as illustrated in the Total Job Postings column in Table 6 above. Third, private sector cybersecurity job postings in the U.S. emphasize management or leadership, communication, and teamwork skills whereas public sector job postings emphasize technical cybersecurity skills.

Conclusion

Rapid development in artificial intelligence (AI) has led to more automation and growth of efficiency and productivity as well as public concerns over potential negative impacts on job security and workforce stability. This research focuses on the AI impacts on cybersecurity workforce in the United States. Based on the review of relevant research literature and the cybersecurity industry expectations for the workforce, this study proposes an adapted model of cybersecurity competency model incorporating AI related KSAs for cybersecurity workforce. Data on KSAs for major cybersecurity work roles was collected from public sector and private sector job postings in the United States for the past five years. Quantitative analysis of the datasets shows continued dominance of cybersecurity technical skills and business/management or leadership competencies in the cybersecurity job postings, along with a relatively low but rapidly rising occurrence of AI-related KSAs, especially in post-COVID-19 years.

Cybersecurity remains to be a fast-growing workforce area in the U.S. in the future. Meanwhile, AI, and GenAI in particular, is increasingly adopted in many industries including cybersecurity. This study is only a preliminary effort to discover the impacts of AI on the U.S. cybersecurity workforce. Continuous research in this area remains significant. Future research on this topic may include more in-depth studies of specific AI models and solutions, such as Claude Mythos from Anthropic, and their benefits and risks for cybersecurity industry and workforce. Further research may also include education and training curriculum and course design to make the best use of AI for the benefit of cybersecurity and cybersecurity workforce.

Acknowledgement

This research is supported by a grant award from the United States National Science Foundation (NSF) – NSF Grant ID 2234554.

References

- Akinwale, O. E., Kuye, O. L., & Doddanava, I. (2024). Scourge of replacing contemporary work environment with artificial intelligence (AI-dark-side): the role of capacity development in quality of work-life and organizational performance. *Journal of Systems and Information Technology*, 27(1), 116-145. DOI: [10.1108/JSIT-08-2024-0297](https://doi.org/10.1108/JSIT-08-2024-0297)

- Anto, M. E. (2025). The impact of artificial intelligence chatbots on workforce dynamics and managerial decision-making. *XIBA Business Review*, 8(2), 1-6.
- Balasubramanian, P., Liyana, S., Sankaran, H., Sivaramakrishnan, S., Pusuluri, S., Pirttikangas, S., & Peltonen, E. (2025). Generative AI for cyber threat intelligence: applications, challenges, and analysis of real-world case studies. *Artificial Intelligence Review*, 58(336), 1-134. <https://doi.org/10.1007/s10462-025-11338-z>.
- Bonfiglioli, A., Crino, R., Gancia, G., & Papadakis, I. (2025). Artificial intelligence and jobs: evidence from US commuting zones. *Economic Policy*, 145-194.
- Capoot, A. (2026, April 7). *Anthropic limits Mythos AI rollout over fears hackers could use model for cyberattacks*. CNBC. <https://www.cnn.com/2026/04/07/anthropic-claude-mythos-ai-hackers-cyberattacks.html>
- Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.
- Dahiya, R. M. (2025). A systematic literature review on the impact of artificial intelligence on employment dynamics. *Advances in Consumer Research*, 2(5), 2031-2037.
- Datta, P., & Acton, T. (2025). Promises and perils of Generative AI in cybersecurity. *MIS Quarterly Executive*, 24(2), 5, 166-184. <https://aisel.aisnet.org/misqe/vol24/iss2/5>.
- Field, A. (2024). *Discovering statistics using IBM SPSS statistics*. Sage publications limited.
- Gimble, M., Kinder, M., Kendall, J., & Lee, M. (2026). Evaluating the impact of ai on the labor market: current state of affairs. Retrieved on 4/26/2026 from <https://budgetlab.yale.edu/research/evaluating-impact-ai-labor-market-current-state-affairs>
- Goldman Sachs. (2026, March 28). How Will AI Affect the US Labor Market? Retrieved on 4/26/2026 from <https://www.goldmansachs.com/insights/articles/how-will-ai-affect-the-us-labor-market>
- Google. (2024). *Gemini* Large language model. Retrieved from <https://deepmind.google/technologies/gemini/>
- Hampole, M., Papanikolaou, D., Schmidt, L.D.W., & Seegmiller, B. (2025). Artificial intelligence and the labor market. National Bureau of Economic Research (NBER). Retrieved on 4/26/2026 from <https://www.nber.org/papers/w33509>
- Hasanov, I., Virtanen, S., Hakkala, A., & Isoaho, J. (2024). Application of large language models in cybersecurity: A systematic literature review. *IEEEAccess*, 12, 176751-176778. DOI: [10.1109/ACCESS.2024.3505983](https://doi.org/10.1109/ACCESS.2024.3505983).

- Ibrar, W., Mahmood, D., Al-Shamayleh, A. S., Ahmed, G., Alharthi, S. Z., & Akhunzada, A. (2025). Generative AI: A double-edged sword in the cyber threat landscape. *Artificial Intelligence Review*, 58(285), 1-27. <https://doi.org/10.1007/s10462-025-11285-9>.
- Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organizational cyber security: An outcome of a systematic literature review. *Journal of Data and Information Management*, 8, 1-15. <https://doi.org/10.1016/j.dim.2023.100063>.
- Jones, G., Kasimatis, D., Pitropakis, N., Macfarlane, R., & Buchanan, W. (2025). Analyzing the role of LLMs in cybersecurity incident management. *International Journal of Information Security*, 24(228), 1-14. <https://doi.org/10.1007/s10207-025-01144-7>.
- Kan, Z., Zhao, S., Chi, W., & Zhou, J. (2024). AI types and organizational implications in various task contexts: a quantitative review from China. *Asia Pacific Business Review*, 1-29. <http://doi.org/10.1080/13602381.2024.2409804>.
- Kavya, S., & Sumathi, D. (2025). Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection. *Artificial Intelligence Review*, 58(5), 1-46. <https://doi.org/10.1007/s10462-024-11055-z>.
- Lier, S. K., Eppers, T. M., Gerlach, J., Muller, P., & Breitner, M. H. (2025). An iterative five-phase process model to successfully implement AI for cybersecurity in a corporate environment. *Electronic Markets*, 35(56), 1-21. <https://doi.org/10.1007/s12525-025-00802-x>.
- Markel, K. S., Tale, M., & Belz, A. (2025, August). Jobpulse: A Big Data Approach to Real-Time Engineering Workforce Analysis and National Industrial Policy. In *2025 IEEE Technology and Engineering Management Society Conference-Global (TEMSCON Global)* (pp. 1-7). IEEE.
- Metin, B., Wynn, M., Tunali, A., & Kepir, Y. (2025). Business logic vulnerabilities in the digital era: a detection framework using artificial intelligence. *Information*, 16(585), 1-22. <https://doi.org/10.3390/info16070585>.
- Mishra, R. (2025). Web Scraping for Job Listings Using Python and BeautifulSoup. *Scientific Journal of Artificial Intelligence and Blockchain Technologies*, 2(3), 63-70.
- Mohammed, S. S., Mohammed, H. I., Mohammed, N. S., Shafiq, N. M., Flayyih, H. Q. (2026). Future directions in artificial intelligence for cybersecurity: emerging trends and key developments. *Passer Journal of Basic and Applied Sciences*, 8(1), 400-409. DOI: [10.24271/PSR.2025.521050.2126](https://doi.org/10.24271/PSR.2025.521050.2126).
- Murray, S. (2025). How artificial intelligence impacts the US labor market. Retrieved on 4/26/2026 from <https://mitsloan.mit.edu/ideas-made-to-matter/how-artificial-intelligence-impacts-us-labor-market>
- NIST/NICE (National Initiative for Cybersecurity Education). (2025, April 28). *NICE Framework v2.2.0*. Retrieved on 4/27/2026 from <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions#components>

- Nowrozy, R. (2024). GPTs or grim position threats? The potential impacts of Large Language Models on non-managerial jobs and certifications in cybersecurity. *Informatics*, 11(45), 1-22. <https://doi.org/10.3390/informatics11030045>.
- OpenAI, C. (2023). Large language model. 2023a). Retrieved from <https://chat.openai.com/chat>.
- Perez, F., Conway, N., & Roques, O. (2022). The autonomy tussle: AI technology and employee job crafting responses. *Relations industrielles / Industrial Relations*, 77(3). <http://doi.org/10.7202/1094209ar>.
- Santoni de Sio, F. (2024). Artificial Intelligence and the future of work: mapping the ethical issues. *Journal of Ethics*, 28, 407-427. <https://doi.org/10.1007/s10892-024-09493-6>.
- Schmitt, M., & Flechais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57(324), 1-24. <https://doi.org/10.1007/s10462-024-10973-2>.
- Smitha, C., Mani, S., Arumugam, A., & Kumari, S. A. (2025). Evaluating the impact of AI-powered reskilling programs on Bengaluru's IT professionals. *The IUP Journal of Information Technology*, 21(1), 95-104. DOI: [10.71329/IUPJIT/2025.21.1.95-104](https://doi.org/10.71329/IUPJIT/2025.21.1.95-104).
- Subin, S., & Son, H. (2026, April 10). *Powell, Bessent discussed Anthropic's Mythos AI cyber threat with major U.S. banks*. CNBC. <https://www.cnbc.com/2026/04/10/powell-bessent-us-bank-ceos-anthropic-mythos-ai-cyber.html>
- Syllaidopoulos, I., Ntalianis, K. S., & Salmon, I. (2025). A comprehensive survey on AI in counter-terrorism and cybersecurity: challenges and ethical dimensions. *IEEE Access*, 13, 91740-91764. DOI: [10.1109/ACCESS.2025.3572348](https://doi.org/10.1109/ACCESS.2025.3572348).
- US BLS (Bureau of Labor Statistics). (2026). *Occupational outlook handbook: Information security analysts*. Retrieved on 4/26/2026 from <https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6>
- US DoD (Department of Defense) Cyber Exchange Public. (2025). *The DoD cyber workforce framework (DCWF)*. Retrieved on 4/27/2026 from <https://www.cyber.mil/dod-workforce-innovation-directorate/dod-cyber-workforce-framework>
- US DoL (Department of Labor). (2014). Cybersecurity Competency Model. Retrieved on 4/30/2025 from <https://www.careeronestop.org/Competencymodel/competency-models/cybersecurity.aspx>
- Wang, H., Lai, X., Huang, S., Dai, X., Zhao, X., & Wang, Y. (2026). The influence of prior perception, attitude, and immediate knowledge of AI on adolescents' preferences for high- and low-replaceable jobs. *Behavioral Sciences*, 16(26), 1-18. <https://doi.org/10.3390/bs16010072>.

- Wang, P., D'Cruze, H. (2024). AI-Assisted Pentesting Using ChatGPT-4. In: Latifi, S. (eds). *ITNG 2024: Advances in Intelligent Systems and Computing, vol 1456*. Springer, Cham.
- Wang, P., Hayes, N., Bertocci, M., Williams, K., & Sbeit, R. (2020). The role of industry partnerships and collaborations in information technology education. *Advances in Intelligent Systems and Computing, 1134* (Chapter 2). Springer Nature Switzerland AG.
- Wilson, S. (2023). *Cybersecurity and artificial intelligence: Threats and opportunities*. Contrast Security.
- Wu, D., Lin, H., Zhang, Q., & Ren, X. (2025). The impact of artificial intelligence usage on employee moonlighting intention: a moderated mediation model. *Work: A Journal of Prevention, Assessment and Rehabilitation*, 82(1), 252-263. DOI: [10.1177/1051981525134138](https://doi.org/10.1177/1051981525134138).
- Xavier, D. F., Korunka, C., & Reiter-Palmon, R. (2025). AI integration and workforce development: exploring job autonomy and creative self-efficacy in a global context. *PLoS One* 20(6): e0319556. <https://doi.org/10.1371/journal.pone.0319556>.
- Yu, J., & Qi, C. (2024). The impact of generative AI on employment and labor productivity. *Review of Business*, 44(1), 53-67.