Open Access License Notice

Bridging the Cybersecurity Skills Gap: Aligning Educational Programs with Industry Needs

Joshua Ball
Codio
Cambridge, MA
0009-0007-3976-8825

Maura Lyons
Codio
Cambridge, MA
0009-0003-5621-8586

Kendra Evans
Codio
Cambridge, MA
0009-0006-5343-4875

Abstract—The cybersecurity industry faces a persistent shortage of skilled professionals, as employers report significant challenges in hiring qualified candidates. This study examines the specific technical and non-technical skills that employers find most lacking in new hires and evaluates the importance of practical experience in workforce readiness.

Through a survey of 200 senior cybersecurity leaders, we assess which skills are most valued, which are most frequently lacking, and how employer satisfaction varies by education model. The findings indicate that while hands-on experiences, such as real-world projects and capstone work, are linked to higher satisfaction, traditional training programs — including university and boot camp models—show no statistically significant difference in employer satisfaction.

Notably, the hiring challenges noted by employers are not fully explained by NICE-aligned technical competencies, underscoring the need for better alignment between training expectations and industry demands. These results emphasize the value of contextualized, practical experience rather than reliance on predefined skill taxonomies.

Keywords—*cybersecurity, industry-academia collaboration, skills gap, workforce development, hands-on learning*

I. INTRODUCTION

As organizations face an increasing volume of cybersecurity threats, the demand for skilled professionals continues to rise. While previous research has highlighted the overall workforce shortage in cybersecurity, this study focuses specifically on the skills gap—defined as the mismatch between employer expectations and new hire capabilities.

Industry leaders frequently report difficulty finding candidates with both the technical proficiency and practical experience required for entry-level roles. Existing frameworks, such as the NICE Cybersecurity Workforce Framework, provide structure for defining cybersecurity roles, yet they do not fully capture employer hiring challenges. For example, while frameworks outline competencies, hiring managers often prioritize practical readiness, adaptability, and real-world problem-solving—factors not always emphasized in traditional curricula [1].

To better understand these challenges, this study analyzes survey responses from 200 cybersecurity decision-makers, identifying which technical and non-technical skills are most lacking in new hires and whether collaboration with academic institutions improves hiring outcomes. By distinguishing between workforce supply issues and the specific skills employers find missing, this research contributes to aligning education and training approaches with industry needs.

There have been many important efforts within academia and industry to better understand the cybersecurity skills gap and offer possible solutions. To best examine the gap specifically, it is crucial to unpack the current cybersecurity field. The 2023 report “The Life and Times of Cybersecurity Professionals,” authored by Vi and Oltsik, provides a strong basis for such an understanding. The authors surveyed over 300 information security and IT professionals to better understand the career progression of cyber security professionals, determine employees’ satisfaction levels with these jobs, measure the skill shortage’s impact, and monitor leadership status [2].

According to this report, current cybersecurity professionals find a career in their field to be increasingly more difficult as the landscape becomes more complex and the work becomes more challenging [2, 3, 4]. Vi and Oltsik point towards internal issues like budget deficits and workload complexity compounding with external issues like regulatory compliance challenges as drivers of the increasing difficulty. Additionally, most cyber professionals are unsatisfied with their career choices, with many considering leaving their positions within the year [2, 3]. Finally, Vi and Oltsik found that the cyber skills gap impacts 71% of organizations, and the majority of cyber professionals believe the gap has only become wider over the past few years. This research makes clear that there are fundamental issues in the cybersecurity field, not only with new graduates’ lack of knowledge but also with current professionals [2, 3].

To shift towards the gap specifically, the cybersecurity skill gap has been defined in previous research as the gap between what college graduates are capable of and what industry employers expect of them [5, 6, 7, 8]. We widen this

understanding to refer more broadly to the disparity between the demand for skilled cybersecurity professionals and the availability of qualified individuals, thereby including those who are already employed in cybersecurity but may be lacking the necessary skills to manage the current landscape. The cyber security skills gap is widely recognized as an important and critical issue in the field [5, 6, 7, 8].

With an understanding of the turmoil within the cybersecurity field, we can now turn to unpacking the causes of the skill gap. Many researchers have also examined its causes, and while we discuss various drivers, there is no single cause of the gap. Rather, it is a nuanced and complex issue resulting from varying factors related to education at large, industry, and individuals, and it necessitates nuanced and complex solutions. For example, some researchers point towards university programs' tendency to overweight areas like policy planning to the detriment of technical computing fundamentals in the curriculum [9]. This can lead to graduates who lack technical skills and so are unprepared for technical positions [9]. Additionally, some posit that graduates also lack soft skills such as teamwork, communication, and problem-solving, which are all essential for an organization to run successfully [2, 3, 9].

Research also indicates that cybersecurity is insufficiently diverse as women, African Americans, and Latinos are underrepresented in educational and professional settings, which may be contributing to the skill gap [2, 3, 4, 10, 11]. Various sources outline strategies to increase diversity within cybersecurity and computing more generally, which may be extrapolated to understand pitfalls in creating environments that foster such diversity in educational settings. Maintaining more diverse educational programs enables a more diverse workforce. For example, Osman et al interviewed minority cybersecurity professionals and students to understand how to better attract underrepresented minorities and diversify the workforce. Their recommendations suggest that late exposure, lack of communication and mentorship, false and harmful stereotypes, and insufficiently effective curriculum, among other factors, might drive the lack of diversity and so the cybersecurity skills gap [10]. An insufficiently diverse workforce may be contributing to the difficulty in solving new problems, as diverse backgrounds and experiences can help people address issues in unique ways [4, 11]. A diverse workforce enables a variety of problem-solving approaches and thought patterns from different team members, yielding innovative solutions.

It does not seem that educational programs are the sole cause of the cybersecurity skills gap. Multiple sources tap failures in the industry to provide competitive compensation to candidates, which undermines the hiring process and deters potential cyber professionals [2, 3, 12]. Additionally, culture within the field, like the supposed need to have a reputation as a cyber leader, can deter candidates from certain organizations, thereby widening the gap and placing more burden on those already employed [3, 12]. As mentioned above, many current cybersecurity professionals are unsatisfied with their career choices and strongly consider leaving their roles [2]. Pairing these findings, obtaining qualified candidates and retaining them once hired is difficult, creating the perfect storm for a skills gap.

With an understanding of some of the varied causes of the skills gap, we can begin to explore its impacts on organizations. Not only do insufficiently protected systems become prime targets for malicious actors, compromising the integrity of the systems, but the gap also compromises the integrity of an organization's financial and temporal resources, causing employee discontent. For example, almost one-third of CISOs surveyed by Vi and Oltsik reported that the skills shortage has had a significant impact on their organization. Further, CISOs report that the skills gap increases workloads, drives higher rates of employee burnout, and leads to jobs staying open for weeks or even months [2].

The literature provides numerous recommendations to help close the gap, especially on the education side. For example, it repeatedly suggests focusing on experiential learning to hone technical skills, diversifying the workforce through varied means, and collaborating with industry [4, 10, 11, 13]. These recommendations provide excellent strategies to which we hope to add nuance through our investigation.

The cybersecurity skills gap is a complex issue that poses worrying consequences for organizations' security and professionals' well-being. Varied research is needed to best understand its causes and suggest solutions, a need we aimed to address in part with this paper. We sought to unpack what skills educational programs and institutions should prioritize teaching to students to best prepare them for industry, how practical experiences are perceived by managers when evaluating new hires, and how industry-academia collaboration relates to employer satisfaction with new hires.

Most research addresses these questions through meta-reviews or qualitative research through interviews. We sought to expand the literature through a qualitative survey, specifically investigating what skills are in most demand, a research area not covered in depth at the time of the survey.

II. METHODS

We recruited survey participants via SurveyMonkey's proprietary audience database and network, "SurveyMonkey Audience," which consists of over 175 million individuals around the world who have completed other SurveyMonkey instruments. SurveyMonkey balances its US database of survey takers according to census data of age and gender. Survey takers received either a donation to a charity of their choice, a chance to win a sweepstakes prize, or credits they could redeem for gift cards.

The eligibility requirements were being a senior executive responsible for an organization's cybersecurity strategy, operations, and workforce development. 200 complete, eligible responses were received. Only the respondents who

completed the survey were considered in the subsequent analysis.

A. Survey Design

While this survey design drew on past research, such as the literature reviewed, it does not seek to replicate any one study as, at the time of investigation, no existing instrument surveyed exactly what we were looking to understand. The survey was designed to capture multiple themes: skills most important in the skills gap, how hiring managers perceive new hires, and how organizations act to close the gap. Each question is addressed in the results section below.

The survey sought to reinforce and extend results that emphasize the importance of hands-on experience and industry-academic collaboration and the widespread impact of the skills gap on an organization, its employees, and the skills it implies [2, 5, 9, 10].

The survey was comprised of sixteen main questions, eleven demographic questions, and one qualification question. Within these, there were two ranking questions, four questions that allowed respondents to select as many responses as they felt necessary, three questions in which respondents could select three answers specifically, and seven that only allowed for one response, such as the five statements with which participants could agree or disagree.

B. Respondent Demographics

At the time of the survey, all participants were serving in a senior executive or leadership role with primary responsibility for their organization's cybersecurity strategy, operations, and workforce development.

Overall gender of respondents was 71.5% male and 28.5% female. Respondents were also provided with the choices non-binary, a gender not listed here, and preferred not to answer, but no respondent selected any of those options.

Most participants were between 30-44 years of age, as 126 or 63%, of participants indicated so. 20.5% of respondents were 45-60 years old, 14.5% were 18-29, and 2% were 60 and above.

The most common organization type was telecommunications, technology, internet, and electronics, in which 29.5% of respondents work. This was followed by finance and financial services, construction machinery and homes, and manufacturing, in which 12.5%, 10%, and 10% of respondents work, respectively.

The average professional and skills development spend per organizational employee was $1,765.73.

C. Limitations

We are using an unstandardized survey instrument, which can lead to bias. Additionally, we are recruiting from a disparate community, which can lead to a lack of representative respondents. It is also worth noting that this survey was voluntary, which may have skewed the respondent pool to be more heavily representative of those with strong opinions on cybersecurity. Additionally, the survey was composed around sets of skills proposed by a cybersecurity educator. Given this fact, the survey itself might have specifically impacted the findings to lean more towards the inherent biases of the survey writers, like favoring hands-on experience.

Survey biases were examined by assessing industry representation and skill perception differences among respondents. No major industry skews were detected; however, responses varied based on company size and sector. Larger enterprises tended to report higher dissatisfaction with new hires, while smaller firms placed greater emphasis on hands-on experience.

D. Statistical Analysis

We imported and used several Python tools libraries to explore the relationships between organizational factors, cybersecurity skill importance rankings, hiring challenges, and other factors:

- Pandas: For data manipulation and cleaning.
- NumPy: For numerical operations and handling of missing data.
- Scipy: For conducting statistical tests, such as Kruskal-Wallis H-test, Mann-Whitney U tests, and Chi-Square tests.
- Statsmodels: For building and evaluating regression models, including Ordinary Least Squares (OLS) regression.
- Scikit-learn: For cluster analysis (KMeans clustering) and logistic regression.
- Matplotlib and Seaborn: For data visualization, including interaction plots, correlation matrices, and ROC curves.

The analyses encompassed several statistical methods, including correlation analysis, non-parametric tests, cluster analysis, and regression models. Each method was selected based on the nature of the data and the specific research questions being addressed.

1) Mean Rank Importance and Correlation Analysis

Mean rank importance was calculated for various cybersecurity skills to determine which skills were most valued by organizations. This involved assigning numerical ranks to the importance of each skill as perceived by the organizations. Spearman's Rank Correlation Coefficient was used to explore relationships between skill importance rankings. This nonparametric measure is appropriate for ordinal data and assesses how well the relationship between two variables can be described using a monotonic function.

2) Cluster Analysis

Cluster analysis revealed three distinct organizational profiles, highlighting that employer skill priorities are not

uniform and instead correlate with industry sector, budget allocation, and organizational size.

We performed KMeans clustering to identify patterns in cybersecurity skills gaps and organizational priorities. The analysis incorporated variables such as skill importance rankings, organizational characteristics, and industry factors, resulting in three distinct clusters. Hierarchical Clustering was used to compare the stability and validity of the clusters obtained from KMeans clustering. Mann-Whitney U Tests were used to assess significant differences in continuous variables (e.g., spending patterns, employee allocation) across clusters. Due to the ordinal nature of the data, Kruskal-Wallis Tests were applied to compare skill importance rankings across clusters. Chi-square tests were employed to evaluate associations between categorical variables (e.g., top 3 valued skills, hiring challenges) and cluster membership.

3) Regression Analysis

Ordinal logistic regression was used to examine how organizational factors influenced the importance rankings of cybersecurity skills. Logistic regression models were developed to predict the likelihood of organizations facing hiring challenges related to specific technical skills. Model performance was assessed by generating Receiver Operating Characteristic (ROC) Curves to evaluate the models' discriminatory power and calculating the Area Under the Curve (AUC) to quantify the models' ability to distinguish between organizations that face hiring challenges and those that do not.

OLS regressions were performed to examine the relationship between employer satisfaction (dependent variable) and the valued practical experience forms (independent variables), such as internships, real-world projects, simulations, and case studies. Models were evaluated by assessing the R-squared value to determine the proportion of variance in satisfaction scores explained by the practical experience variables. Residual plots were analyzed to check for linearity and homoscedasticity, acknowledging that while some assumptions may be violated due to the nature of the data, the regression provided useful insights.

4) Interaction Plots and Correlation Analysis

Interaction Plots were generated to visualize the relationships between skill importance, organizational factors (such as spending and organization size), and hiring challenges. Pearson Correlation Coefficient was calculated to analyze associations between continuous variables representing valued practical experiences in hiring (e.g., internships, simulations) and employer satisfaction with new hires. Pearson's correlation was used when data met the assumptions of normality and interval measurement levels; otherwise, Spearman's rank correlation coefficient was employed.

5) Ordinary Least Squares (OLS) Regression

We performed OLS regression to examine the relationship between employer satisfaction (dependent variable) and valued practical experience forms (independent variables), such as internships, real-world projects, simulations, and case studies. The R-squared value was used to determine the proportion of variance in satisfaction scores explained by the practical experience variables. Residual plots were analyzed to check for linearity and homoscedasticity, acknowledging that while some assumptions may be violated due to the nature of the data, the regression provided useful insights.

III. RESULTS

We divide the results into two sections. In the first section, we build on previous research by replicating prior work at scale and adding nuance and specificity to the skills themselves and managers' views of new hires. In the second section, we use the statistical methods described above to explore relationships between various dimensions of the skills gap.

A. Descriptive Results

When asked to rank technical skills in order of importance when evaluating new hires, network security, cloud security, and encryption were most frequently ranked as the most important skills, as shown in Figure 1. Ethical hacking, AI and machine learning, and security architecture were the least important skills.

The top three most lacking technical skills in respondents' organizations were cloud security, with 49.5% of respondents selecting it; network security, with 37% of responses; and threat intelligence, with 36% of responses (Figure 1). However, the top three most valued skills in respondents' organizations were also network security (60%), cloud security (54.5%), and encryption (31.5%). While there is a sharp cut-off between network and cloud security compared to encryption, it is notable that encryption does not rank as highly in other questions.

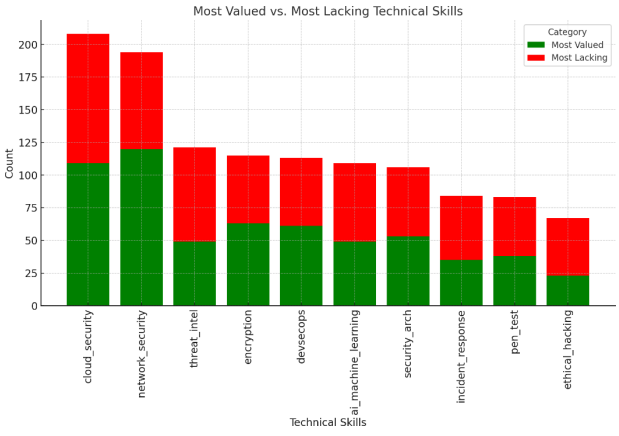

Fig. 1. Most lacking and valued technical skills in respondents' organizations.

To further cement cloud and network security's importance, they were the top two responses when participants were asked to select the skills for which their organizations were challenges hiring, as shown in Figure 2, with 38% and 34.5% of responses, respectively. The third most frequently selected skill was AI and machine learning (32.5%). Shifting towards non-technical skills, there was a fairly even distribution among the six skills provided when respondents were asked to select the top three, they found most lacking in their organization. The top responses were problem-solving/critical thinking (63%), oral communication (57%), and teamwork (50%). When asked to rank these skills in order of importance when evaluating new hires, problem-solving/critical thinking was ranked as the most important, followed closely by oral communication and teamwork.

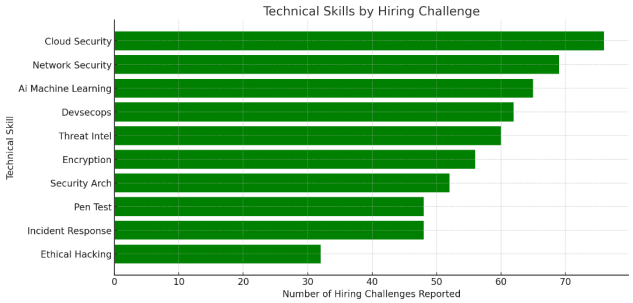

Fig. 2. Technical skill hiring challenges in respondents' organizations.

Respondents were then provided with a series of statements with which they could strongly agree, agree, disagree, or strongly disagree. Overall, the statements tended toward a positive view of new hires, and most responses agreed. For example, 85% of respondents agreed or strongly agreed with the notion that current cybersecurity education programs at traditional universities and colleges prepare students well for real-world challenges. Further, 85% also agreed or strongly agreed that online universities prepare students well for real-world challenges, and 88.5% agreed or strongly agreed that bootcamp programs prepare students well for real-world challenges. 63% of respondents strongly agreed, and 32.5% agreed that hands-on experience, like internships and practical projects, is important in new hires. 86.5% of respondents agreed or strongly agreed with the notion that they expect new hires to be immediately ready to work.

Finally, 88.5% of respondents agreed or strongly agreed that they are satisfied with the performance of new hires within 30 days of employment.

Given the importance of hands-on experience, it is notable that when asked what specific areas they believed to be most deficient in new hires, 63.5% of participants selected practical experience, making it the top answer. It was closely followed by up-to-date knowledge (56.5%), industry best practices (48.5%), and general professional skills (45.5%). When asked what practical experiences they valued most when evaluating new hires, real-world projects were the most frequently selected experience (73%). Internships were the second most frequently selected (58.5%), followed by case studies (48%).

Shifting towards the organizations themselves, we asked respondents questions to better understand their role in lessening the skills gap. We found that 81.5% of respondents' organizations collaborate with education programs and institutions to better prepare cybersecurity students for the workforce. Additionally, when asked how their organizations ensure cybersecurity employees' knowledge and technical skills are up-to-date, 67.5% selected accredited certification programs (e.g., CISSP, CISM, CEH), 63% selected internal training programs (cybersecurity curriculum, hands-on training with cyber ranges and simulation labs), 41% selected subscriptions to advanced training platforms (e.g., SANS, Cybrary, Pluralsight), and 41% selected practical exercises (internal and external penetration testing, capture the flag competitions). Other responses, research and experimentation, community and forum participation, mentorship and coaching, external consultancy and assessments, and performance-linked learning were selected by 38.5% and 18.5% of respondents, from most to least in the written order.

B. Statistical Results

1) Mean Rank Importance and Correlation Analysis

The analysis of mean rank importance among cybersecurity skills indicates that network security (mean rank = 2.33) and cloud security (mean rank = 3.27) are the highest-ranked competencies among employers, reflecting their foundational role across all organizational sizes. Conversely, ethical hacking (mean rank = 8.77) and AI/machine learning (mean rank = 7.64) were ranked lower, suggesting that while these emerging fields are valuable, they may not be prioritized for immediate workforce needs.

Shown in Figure 3, Spearman's rank correlation analysis provided further insights into skill interdependencies, revealing moderate negative correlations between ethical hacking and AI/machine learning ($\rho = -0.43$, $p < 0.05$) and between penetration testing and AI/machine learning ($\rho = -0.38$, $p < 0.05$). These results suggest that as organizations prioritize traditional security skills, they may deprioritize emerging technologies like AI. This trend aligns with previous research indicating that the NICE framework places greater emphasis on well-established cybersecurity disciplines over newer AI-driven security methodologies [1].

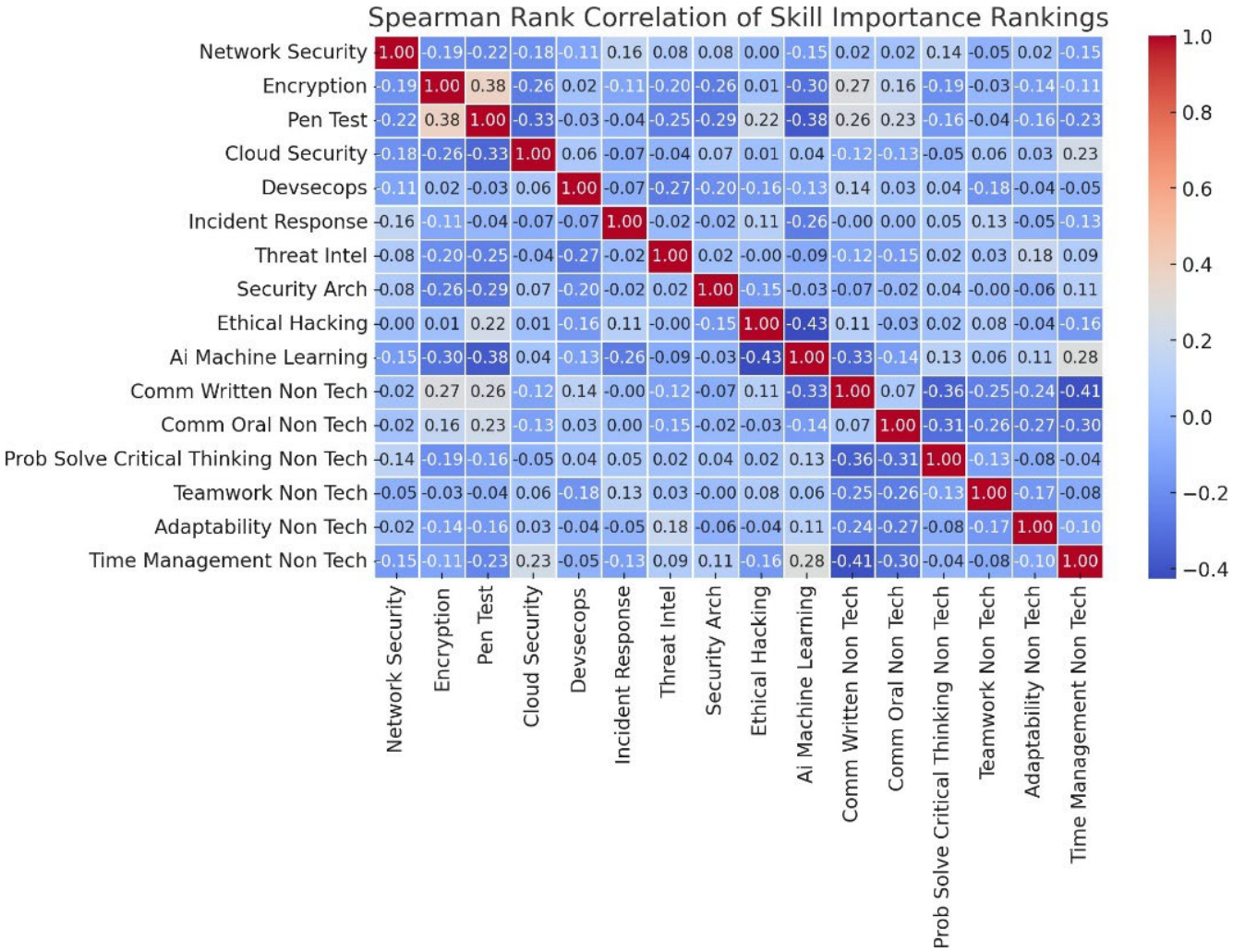

Fig. 3. Spearman rank correlation of skill importance rankings.

Similarly, a moderate positive correlation ($\rho = 0.31$, $p < 0.05$) was found between encryption and penetration testing, indicating that organizations focusing on cryptographic security also place a higher value on ethical hacking methodologies, an observation that corresponds with NICE work roles emphasizing offensive security techniques. These results suggest that while the NICE framework provides structured skill categorization, employer prioritization of skills is highly contextual, dependent on both organizational risk tolerance and evolving threat landscapes.

2) Cluster Analysis

Cluster analysis revealed three distinct organizational profiles, highlighting that employer skill priorities are not uniform and instead correlate with industry sector, budget allocation, and organizational size, as shown in Figure 4.

1. Cluster 0: High-Investment, Broad-Spectrum Organizations: These organizations exhibit high cybersecurity education spending and prioritize a broad skillset across both defensive and offensive security disciplines. Strong alignment with NICE work roles in network defense and secure software development indicate a preference for full-spectrum workforce readiness.

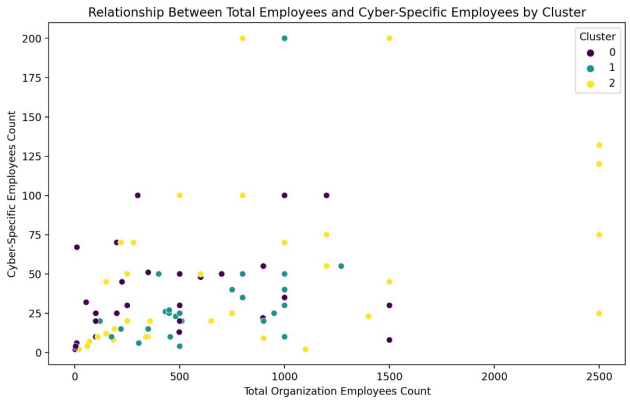

Fig. 4. Total employees and cyber-specific employees by cluster.

2. Cluster 1: Moderate-Investment, Industry-Specific Specialization: Focuses heavily on specialized AI and machine learning roles, particularly within government, finance, and healthcare sectors where AI-driven security solutions are gaining traction. Lower alignment with NICE categories related to general cybersecurity administration suggest a greater emphasis on domain-specific AI applications rather than broad-based security expertise.
3. Cluster 2: Lower-Investment, Essential Security Skill Focus: These organizations maintain lower spending on cybersecurity education but prioritize core security functions such as encryption and penetration testing. NICE work roles in cyber operations and secure network engineering align closely with the hiring priorities in this cluster, reinforcing the importance of essential security skills in resource-constrained environments.

The findings indicate that the NICE framework's broad competency categories do not fully capture the industry-specific specialization observed within certain clusters. While some NICE-aligned skills remain universally valued (e.g., network security), sector-specific needs, such as AI-driven cybersecurity for financial institutions, are not well-differentiated in existing frameworks.

3) Non-Parametric Tests

Given the ordinal nature of the skill importance rankings, Kruskal-Wallis H-tests were applied to compare differences across clusters. Significant differences ($p < 0.05$) were observed for several skills—including encryption, penetration testing, DevSecOps, incident response, threat intelligence, security architecture, ethical hacking, and AI/machine learning—indicating that organizations differ in how they prioritize these competencies.

However, no significant differences emerged for network security, cloud security, and incident response, suggesting that these core skills are uniformly valued across organizations. For binary outcomes, Chi-square tests were conducted to assess associations between cluster membership and key categorical variables. Significant associations were observed for:

- The selection of encryption, AI/machine learning, and penetration testing as top-valued skills (p-values ranging from 1.46×10^{-6} to 9.02×10^{-14}), which demonstrates that the value placed on these skills varies markedly between clusters.
- Hiring challenges for AI/machine learning, penetration testing, and ethical hacking (p-values from 5.48×10^{-19} to 8.07×10^{-3}), indicating that employer difficulties in these areas differ significantly across clusters.
- In addition, significant associations between cluster membership and specific industries (e.g., Tech, Manufacturing, Retail) were identified, reinforcing the notion that domain-specific factors influence both skill valuation and hiring challenges.

4) Predictive Power for Hiring Challenges

Ordinal logistic regression was initially applied to examine the influence of organizational characteristics (such as total employee count and annual education spending) on skill importance rankings. However, these models demonstrated low explanatory power, suggesting that the factors driving employer skill priorities are more nuanced than captured by the available variables.

Logistic regression models were developed to assess the likelihood of organizations encountering hiring challenges for specific technical skills. ROC curve analyses yielded AUC values ranging from 0.60 to 0.80 for most skills. Notably, skills such as network security, penetration testing, and AI/machine learning exhibited AUC values closer to or above 0.70, implying that factors like organizational size and spending patterns are moderately predictive of hiring challenges. Conversely, lower AUC values for other skills indicate that unmeasured factors may play a more critical role.

Receiver Operating Characteristic (ROC) curves were generated, with Area Under the Curve (AUC) values ranging from 0.6 to 0.8 for most skills, suggesting moderate discriminatory power. Skills like Penetration Testing (Figure 5), Network Security (Figure 6), and AI/Machine Learning (Figure 7), had AUC values closer to 0.7 or above, indicating reasonably good predictive power. This implies that certain organizational factors, such as spending patterns or employee size, are more strongly correlated with hiring challenges in these areas. Lower AUC values for other skills suggest that other unmeasured factors contribute to hiring challenges.

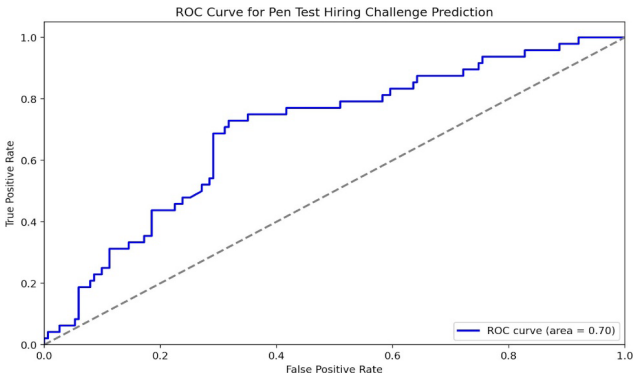

Fig. 5. ROC Curve for Network Security hiring challenges.

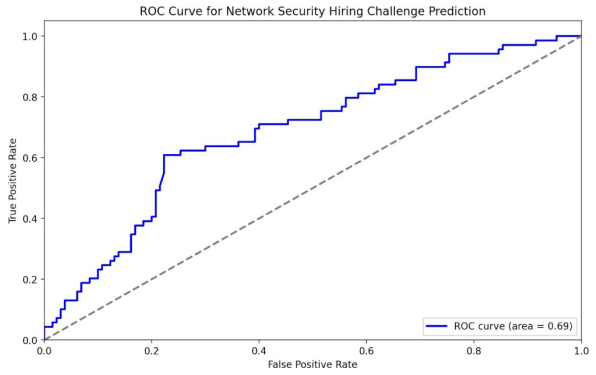

Fig. 6. ROC Curve for Network Security Hiring Challenges.

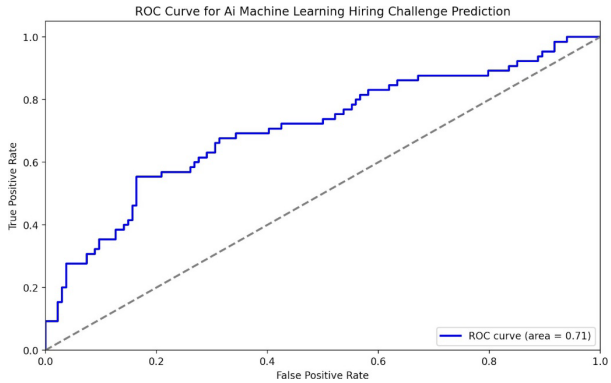

Fig. 7. ROC Curve for AI/ML Hiring Challenges.

5) *Interaction Analyses*

Interaction plots were used to visualize the relationship between skill importance, organizational spending, and size. For instance, smaller organizations tended to emphasize foundational skills such as cloud security (Figure 8), while larger organizations, facing more complex operational challenges, placed greater emphasis on advanced capabilities such as incident response, DevSecOps (Figure 9), and threat intelligence (Figure 10).

6) *Ordinary Least Squares (OLS) Regression on Employer Satisfaction with New Hires*

An OLS regression model examined how practical experience modalities—such as internships, real-world projects, simulations, and case studies—relate to employer satisfaction with new hires.

Fig. 8. Interaction plot for Cloud Security importance by organization employee count and spending on training and education.

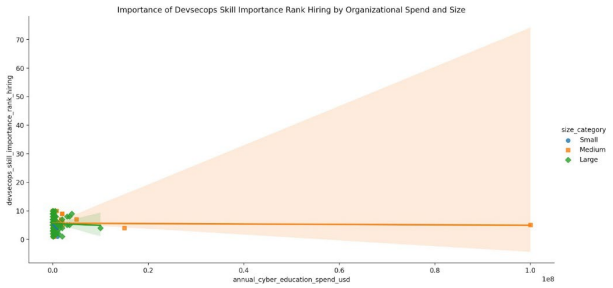

Fig. 9. Interaction plot for DevSecOps importance by organization employee count and spending on training and education.

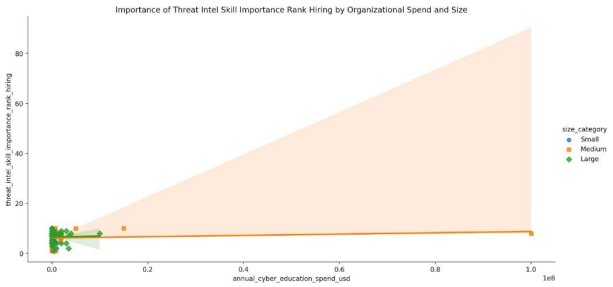

Fig. 10. Interaction plot for Threat Intelligence importance by organization employee count and spending on training and education.

The results indicated that valuing simulations was a significant positive predictor of satisfaction ($\beta = 0.23$, $t = 2.27$, $p = 0.024$), while case studies approached significance ($\beta = 0.17$, $t = 1.74$, $p = 0.084$). However, the overall model explained only about 4.9% of the variance in satisfaction scores ($R^2 = 0.049$), suggesting that additional factors beyond the scope of this analysis influence employer satisfaction.

7) *New Hires Analysis of Collaboration and Skill Deficiencies*

Correlation analyses incorporating academic collaboration status, organizational spending, employee counts, and reported skill deficiencies revealed that organizations engaging in industry-academia collaborations tended to report higher awareness of deficiencies in practical experience ($r = 0.124$) and industry-specific best practices ($r = 0.156$). T-tests further showed that these organizations had significantly higher satisfaction scores for new hires ($t = 3.44$, $p = 0.001$). Moreover, deficiencies in best practices and industry-specific knowledge were significantly associated with satisfaction scores ($t = 2.29$, $p = 0.026$), indicating that employers who are more aware of these gaps adjust their expectations accordingly.

IV. DISCUSSION

This study provides valuable insights into the cybersecurity skills gap, highlighting the relative importance of skills, the role of practical experience, and the benefits of industry-academia collaboration. The results reinforce existing literature while offering new perspectives essential for addressing the cybersecurity workforce challenges.

Network security and cloud security emerged as the most crucial technical skills, reflecting their foundational nature.

Interestingly, while AI and machine learning were ranked lower in importance overall, they emerged as a significant hiring challenge, particularly for certain organizational clusters. This dichotomy may reflect the rapidly evolving nature of AI in cybersecurity, where its potential is recognized, but integration into existing security frameworks is still developing.

Our results underscore the critical role of non-technical skills, particularly problem-solving/critical thinking, oral communication, and teamwork. These findings echo previous research highlighting the importance of soft skills in cybersecurity roles [2, 3, 9]. Educational programs should integrate opportunities for students to develop these skills alongside technical competencies, perhaps through collaborative projects, case studies, and presentations, all of which can strengthen skills like communication and teamwork. However, it is important to keep in mind that factors such as language competency, social anxiety and/or preference for individual work, and non-inclusive learning environments, among others, might challenge the development of non-technical skills. Based on the findings, several actionable recommendations for educational institutions and training programs are proposed:

1. Educational programs should integrate more hands-on, experiential learning opportunities such as internships, real-world projects, simulations, and case studies to address employer perceptions of new hires lacking practical experience.
2. Despite being lower in current priority, skills like AI and machine learning should still be incorporated to prepare students for future industry shifts and advancements.
3. Educational institutions should actively seek partnerships with industry players to keep curricula up to date with industry needs, provide practical experiences, and continuously refine educational content based on feedback from the field.

While our study provides valuable insights, it has limitations that should be addressed in future research. While the sample size is adequate for our analyses, it could be expanded in future studies to increase generalizability.

V. CONCLUSION

Our findings emphasize the need for educational programs to integrate hands-on learning for technical skills alongside contextual soft skills development. In close collaboration with industry partners, educational institutions must continually adapt their programs to meet the changing needs of the cybersecurity landscape. Future studies could explore the long-term impacts of different types of practical experience on job performance and career progression in cybersecurity. Additionally, investigating the specific mechanisms by which industry-academia collaborations can most effectively address skills gaps would be valuable.

REFERENCES

[1] R. Straight, 'Beyond Human-Centric Models in Cybersecurity Education: A Pilot Posthuman Analysis of the NICE Workforce Framework for Cybersecurity', Journal of Cybersecurity Education, Research and Practice, vol. 2024, no. 1, Nov. 2024. https://doi.org/10.62915/2472-2707.1210

[2] Vi and J. Oltsik, "The Life and Times of Cybersecurity Professionals Volume VI 1 The Life and Times of Cybersecurity Professionals The Life and Times of Cybersecurity Professionals Volume VI 2," 2023. Accessed: Sep. 13, 2024. [Online]. Available: https://www.issa.org/wp-content/uploads/2023/08/ESG-eBook-ISSA-2023.pdf

[3] K. Scarfone, "Cybersecurity Skills Gap: Why It Exists and How to Address It | TechTarget," SearchSecurity, Jan. 29, 2024. https://www.techtarget.com/searchsecurity/tip/Cybersecurity-skills-gap-Why-it-exists-and-how-to-address-it

[4] X. Mountrouidou et al., "Securing the Human," Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education, Dec. 2019, doi: https://doi.org/10.1145/3344429.3372507.

[5] J. Crabb, C. Hundhausen, and A. Gebremedhin, "A Critical Review of Cybersecurity Education in the United States," Mar. 2024, doi: https://doi.org/10.1145/3626252.3630757.

[6] S. Attwood and A. Williams, "Exploring the UK Cyber Skills Gap through a mapping of active job listings to the Cyber Security Body of Knowledge (CyBOK)," Jun. 2023, doi: https://doi.org/10.1145/3593434.3593459.

[7] L. Axon, K. Fletcher, M. Stolz, A. E. Kaafarani, and S. Creese, "Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda IIoT Capability Gaps," Digital Threats: Research and Practice, Mar. 2022, doi: https://doi.org/10.1145/3503920.

[8] F. Goupil, P. Laskov, I. Pekaric, M. Felderer, A. Dürr, and F. Thiesse, "Towards Understanding the Skill Gap in Cybersecurity," Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 1, Jul. 2022, doi: https://doi.org/10.1145/3502718.3524807.

[9] W. Crumpler and J. Lewis, "The Cybersecurity Workforce Gap," 2019. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

[10] M. Osman, M. Namukasa, C. Ficke, I. Piasecki, T. J. OConnor, and M. Carroll, "Understanding How to Diversify the Cybersecurity Workforce: A Qualitative Analysis," Journal of Cybersecurity Education, Research and Practice, vol. 2023, no. 2, Oct. 2023, doi: https://doi.org/10.32727/8.2023.23.

[11] L. Zabierek and A. Pipikaite, "Here's why cybersecurity needs to become more diverse," World Economic Forum. https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce/

[12] J. Oltsik, "The cybersecurity skills shortage: A CISO perspective," CSO Online. https://www.csoonline.com/article/2074581/the-cybersecurity-skills-shortage-a-ciso-perspective.html

[13] A. Konak, 'Experiential Learning Builds Cybersecurity SelfEfficacy in K-12 Students', J. Cybersecurity Educ. Res. Pract., vol. 2018, no. 1, Jul. 2018, [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/6/