Issue Brief

The Cyber Shortage Paradox

Authors
Ali Crawford
Matthias Oschinski



CSET CENTER for SECURITY and EMERGING TECHNOLOGY

November 2026

Executive Summary

Cybersecurity has become a central pillar of U.S. economic and national security policy. Recent federal strategies emphasize expanding the cybersecurity workforce to protect critical infrastructure, secure emerging technologies, and maintain the country's competitive advantage. Yet despite years of investment in cybersecurity education and workforce development, hundreds of thousands of cyber job openings remain unfilled, reinforcing the widespread belief that the United States faces a severe cybersecurity talent shortage.

This report challenges the existing narrative by asking whether it accurately reflects labor market conditions. Rather than assuming unfilled vacancies indicate an insufficient supply of workers, we examine whether the cybersecurity labor market exhibits the economic characteristics expected of a genuine labor shortage.

Our findings suggest a more nuanced reality. While demand for cybersecurity talent remains elevated, we find little meaningful evidence of an economy-wide shortage. Instead, hiring challenges are concentrated within particular occupations, industries, and geographic regions. Moreover, the labor market does not display the wage growth or worker mobility that traditional economic theory predicts when labor is genuinely scarce. Together, these findings suggest that many hiring difficulties are driven less by an absolute shortage of cybersecurity professionals than by structural mismatches among the location of talent, the skills employers seek, and the industries competing for that talent.

Several findings stand out. First, demand pressure is concentrated in a relatively small number of cybersecurity occupations rather than distributed across the workforce. Second, occupations experiencing the greatest hiring pressure do not exhibit correspondingly stronger wage growth, challenging the notion of widespread labor scarcity. Third, hiring difficulties differ across industries. Manufacturing appears to face geographically dispersed demand that complicates recruitment, while sectors such as retail trade appear constrained by comparatively lower compensation despite high hiring demand. These patterns indicate that the causes of hiring difficulty differ across employers and cannot be addressed through a single federal workforce strategy, but perhaps could be mitigated by a combination of targeted federal investment and state policy incentives.

These findings carry important implications for policymakers. Expanding the cybersecurity talent pipeline remains important, but increasing the number of credentialed workers alone is unlikely to resolve persistent hiring challenges. More

targeted approaches—including improving skills alignment, strengthening employer investment in workforce development, addressing regional imbalances, and tailoring interventions to industry-specific needs—are likely to produce better outcomes than policies built on the assumption of a universal cybersecurity labor shortage.

Table of Contents

Executive Summary 1
Introduction 4
Methodology 6
- Job Postings (Lightcast) 6
- Employment and Wages (BLS OEWS) 7
- Hiring Behavior (BLS JOLTS) 7
- Scope of Cybersecurity Occupations 7
- Limitations 8

Analysis 9
- Demand Pressure 9
- Wage Response 11
- Industry-Specific Tests 14
- Hiring Behavior 18
- Region-Specific Tests 20

Findings 24
Conclusion 27
Authors 28
Acknowledgments 28
Appendix 29
Endnotes 42

Introduction

Although artificial intelligence (AI) continues to dominate policy conversations, the March 2026 Cyber Strategy for America elevates a different, more fundamental constraint on national security: the supply of cyber talent.[1] The strategy explicitly identifies the cyber workforce as a strategic asset that must be expanded, better aligned, and more effectively deployed to support economic and national security priorities.

A series of federal initiatives—including the July 2025 AI Action Plan and the August 2025 American Talent Strategy—similarly center workforce development as a necessary component of national prosperity.[2] These efforts call for strengthening cybersecurity around critical infrastructure, mitigating security risks from frontier AI systems, expanding training pathways for talent, upskilling the incumbent workforce, and aligning education systems more closely with industry needs. Taken together, these recommendations reflect a growing concern: The effectiveness of these policies ultimately hinges on whether the nation can produce and sustain cyber talent at scale.

Yet despite this policy momentum, historical cyber workforce supply and demand trends provide a more sobering reality. Domestic cyber job vacancies have fluctuated between 200,000 and 600,000 openings over the past five years, with the United States only having about 75 percent of cyber talent to meet current demand.[3] At face value, these figures suggest a persistent talent shortage, which has been the dominant narrative for the last few years.

However, they also raise a more difficult question: Is the issue truly due to a general lack of supply, or is it more nuanced and cannot be solved by simply expanding the amount of cyber talent? To better understand these dynamics, CSET developed a novel approach to measuring cybersecurity labor demand and conducted three diagnostic tests to determine whether there is a genuine shortage of cyber talent.

Our analysis finds that:

1. **Demand pressure is elevated.** Our analysis indicates there is little meaningful evidence of a general cyber talent shortage as commonly described in the discourse. Demand pressure is concentrated within specific occupations such as data scientists, database architects, and database administrators and does not affect all occupations equally.

2. **Wages are not rising.** More critically, these high-demand occupations do not show the wage growth traditional economic theory would predict. The

correlation between demand pressure and wage growth is negligible, and quartile analysis reveals non-monotonic patterns inconsistent with genuine scarcity.

3. **Effects are dispersed.** Industries with high demand pressure face fundamentally different challenges. Manufacturing shows substantial geographic dispersion yet offers competitive wages, while retail and trade struggle to compete on compensation. This suggests that geographic location and corresponding talent availability is a critical factor, and that while cyber roles have been touted as "well-paying jobs," it does not seem to be the case in all industries.

Methodology

While no single or universally accepted definition of a labor shortage exists in economics, we were able to construct a measure of labor market demand pressure and assemble a set of corroborating indications to ask whether the cybersecurity labor market displays the signatures that a broad talent shortage would produce.[4] Put simply, our measure for labor market demand pressure captures how aggressively employers are seeking to hire relative to the size of the workforce already performing that work.

We define this demand pressure as a postings-to-employment (P/E) ratio, which corresponds to the number of job postings for a given occupation divided by the number of employed workers in that occupation. Thus, a higher P/E ratio for any given occupation indicates greater demand pressure relative to the existing workforce. Because the measure is normalized by employment, it reflects the intensity of hiring demand rather than its absolute volume. This allows us to compare occupations of different sizes. A high P/E ratio means employers are advertising many openings relative to the existing workforce in that occupation, signaling intense hiring demand.

Our analysis draws on four data sources, all covering 2019 to 2024. Using this data we (1) isolated cybersecurity demand from general information technology (IT) demand using a machine learning classification model, (2) calculated P/E ratios at the occupation and industry level, (3) analyzed whether demand pressure behaves as a real shortage, and (4) assessed geographic concentration of demand.

Job Postings (Lightcast)

For our analysis, we used job posting data from Lightcast. The job postings include the posting dates and are mapped to Standard Occupational Classification (SOC) codes, North American Industry Classification System (NAICS) codes, and geographic metropolitan statistical areas (MSAs). We use this metadata to analyze job postings by year, industry, and region. Based on our classification, the dataset covers approximately 21.2 million cyber-related job postings.

We use these job postings for the regional analysis, as the dataset includes postings across 925 MSAs from 2019 to 2024. We calculate three regional concentration metrics: (1) the percentage of postings in the top 10 MSAs based on count of postings, (2) the Herfindahl-Hirschman Index (HHI) measuring market concentration, and (3) the number of MSAs required to account for 80 percent of postings. We use three complementary metrics rather than one because each can move independently. An

industry can be concentrated on one measure and dispersed on another. Thus, a combination of measures is more diagnostic.

Employment and Wages (BLS OEWS)

Employment counts and annual median wages were drawn from the Bureau of Labor Statistics (BLS) Occupational Employment and Wage Statistics (OEWS) database. Employment data was mapped to SOC codes, and we used industry-by-occupation cross-tabulations for our industry-level wage differential analysis. Employment counts served as the denominator in the P/E ratio. Median wages supported the wage growth analysis, and the wage premium was calculated as the median wage for cyber occupations per our classifier divided by the all-jobs median wage.

Hiring Behavior (BLS JOLTS)

To complement our analysis, we assessed hiring difficulty and worker mobility using data from the BLS Job Openings and Labor Turnover Survey. JOLTS is reported by industry rather than by occupation. For our purposes, monthly data was aggregated by year at the two-digit NAICS industry level. For the 16 major industries in JOLTS, we analyzed industry hires, job openings, voluntary separations (quits), and employment level. JOLTS also helps with a second problem. Online job postings can include ghost jobs that overstate actual labor demand. Because JOLTS is an employer survey of actual openings and hires, we validated our postings-based measure against JOLTS to confirm that the signal reflects genuine hiring activity.

Scope of Cybersecurity Occupations

Lightcast and OEWS data organize the labor market by SOC code, but no SOC code corresponds cleanly to cybersecurity roles. Rather, cybersecurity roles are distributed across many SOC codes that also contain large numbers of general IT positions. To isolate genuine cybersecurity demand, CSET developed a machine learning classifier, informed by the NICE Workforce Framework, to classify technical and nontechnical cybersecurity roles. Job postings were labeled using programmatically defined rules, developed in Snorkel Flow, enabling the classifier to identify cybersecurity-relevant

positions at scale.[*] Following evaluation and refinement, the model was applied to the full dataset, meaning each job posting was tagged as a cyber role or not.

We then assigned each occupation a cyber-share, which is the proportion of postings in that SOC code that are classified as cybersecurity relevant by our model. For example, SOC 15-1299 (all other computer occupations) has a 34 percent cyber-share, while SOC 15-1252 (software developers) has a 6 percent cyber-share. These occupation-level shares were used as weights when aggregating across occupations, so that all reported aggregate statistics reflect cybersecurity work rather than the broader IT pool.

Our analysis covers a set of 27 cybersecurity occupations. Of the original 28-occupation classification, SOC 55-9999 (military-only occupations) is excluded. These occupations fall outside civilian labor market analysis and are not covered in OEWS employment data.

Limitations

This analysis has several limitations that suggest directions for future research. Our data does not include posting-level experience requirements, preventing us from directly testing whether high-P/E occupations disproportionately seek mid-career talent while training programs produce entry-level workers. We cannot directly compare employer skill demands with training program curricula to reveal whether the specific skills requested in high-P/E postings align with what certifications teach. Future work will examine these experience- and skills-alignment questions to better understand why more credentialed workers do not solve hiring difficulties.

[*] Snorkel Flow is a programmatic labeling platform implementing the weak-supervision paradigm of Ratner et al. (2017), in which subject-matter experts author labeling functions—heuristic rules of unknown accuracy and coverage—whose outputs are combined by a generative model into probabilistic labels for training a downstream classifier. CSET has applied the same approach to Lightcast job postings to identify AI development roles; see Subbu Rathinam and Kinoshita (2026).

Analysis

The aim of our analysis is to assess whether the market for cybersecurity roles is characterized by a traditional labor shortage. If that were the case, a blanket policy response would be to produce more cyber talent. If, however, the situation is more nuanced, and our analysis suggests that it is, a series of more tailored policy approaches is required.

Our analysis proceeded in three steps. First, we assessed whether cyber roles exhibit higher demand pressure compared to the overall labor market. We found that this is indeed the case. Second, we tested whether wages are responding to the higher demand pressure in cyber roles, as would be the case in a general labor shortage situation. Our wage analysis does not support the hypothesis of a general labor shortage.

Third, we took a more disaggregated view by examining cyber roles at the industry level. We used industry-specific data to complement our wage analysis by adding information from the JOLTS dataset. This enabled us to analyze changes in hiring behavior with regard to cyber roles. It also allowed us to assess the nature of the cybersecurity talent shortage in more detail. For some industries, hiring challenges occur due to wage differentials; for others, the difficulties are more region specific.

Demand Pressure

To determine whether cybersecurity occupations demonstrate higher demand pressure compared to the labor market as a whole, we compared the P/E ratio for all cybersecurity jobs against the P/E ratio for all occupations, by year. Both postings and employment for each of the 27 cybersecurity-relevant occupations were weighted by that occupation's share from the CSET classifier.[*] The all-occupations ratio was computed as total postings across all occupations divided by economy-wide employment. The resulting ratio of the two, shown in the fourth column in Table 1, indicates how much more intensely employers are hiring in cybersecurity relative to the overall labor market. For example, a value of 3.63 means that cyber roles see 3.63 times as many postings per employed worker as the average occupation.

[*]A detailed explanation of our approach is outlined in the Appendix.

Table 1. Aggregated Demand Pressures (P/E ratio) for Cybersecurity Jobs, 2019–2024

Year	All Jobs P/E	Cyber P/E	Cyber-to-All Ratio
2019	0.235	0.853	3.63
2020	0.250	0.737	2.95
2021	0.310	0.682	2.20
2022	0.329	0.764	2.32
2023	0.256	0.461	1.80
2024	0.239	0.402	1.68

Note: P/E ratio refers to the postings-to-employment ratio. A cyber-to-all ratio of 3.63 means cyber roles see 3.63 times as many postings per employed worker as the average occupation.

Source: CSET analysis of BLS and Lightcast U.S. job postings data.

The second column in Table 1 shows aggregated P/E ratios for all jobs from 2019 to 2024. The third column depicts P/E ratios for our group of 27 cybersecurity occupations based on our classifier. The fourth column shows that cyber-specific P/E ratios are consistently higher than the all-jobs P/E ratios in the time frame of analysis. This indicates that demand pressure is higher among cybersecurity occupations when compared to all occupations. We also find that the cyber-to-all ratio was highest in 2019 and then moderated to 1.68 by 2024. The increase in all the P/E ratios in 2022 with a subsequent sharp decline in 2023 is consistent with the post-COVID tech hiring boom followed by widespread tech sector layoffs in 2023.

This “shortage” does not affect all cyber occupations equally. To identify where demand pressure is the highest, we calculated each occupation’s individual P/E ratio, averaged across the study period.*

Our results show that demand pressure is highest for data scientists, with an average P/E ratio of 1.9, followed by database architects (1.7) and database administrators (1.5). Aerospace engineers (0.16), all other engineers (0.14), and physical scientists (0.13) exhibit the lowest demand pressure among cybersecurity occupations. This

* Table 14 in the Appendix displays individual P/E ratios averaged across all years.

indicates that demand pressure is concentrated in specific occupations. In particular, management roles and some engineering roles show comparatively low P/E ratios, despite high cyber shares within their occupational groups.

Wage Response

Traditional economic theory suggests that persistent labor shortages should trigger wage increases. Hence, as a next step in our analysis, we assessed whether higher demand pressure in cybersecurity jobs translates into higher wage growth. We found that annual median wages for cybersecurity roles are consistently higher than the all-jobs median. Yet despite elevated demand pressure, cyber wage growth rates are similar to all-jobs wage growth, and not higher as demand pressure would predict. This pattern contradicts a simple labor shortage explanation, as that would trigger broader wage competition in cyber roles.

Table 2 shows annual median wages for cybersecurity and all occupations and compares year-over-year wage growth for these two groups. Tables 3 and 4 depict annual median wages and wage growth for the top five and bottom five occupations in 2024, respectively. These figures show that wage growth varies significantly across individual cyber occupations. This indicates occupation-specific demand rather than a shortage affecting all cyber roles equally.

Table 2. Aggregated Annual Median Wages for Cybersecurity and All Jobs, 2019–2024

Year	Cyber Median Wage	All Jobs Median Wage	Cyber YoY	All Jobs YoY
2019	$93,554	$39,810	-	-
2020	$97,366	$41,950	+4.07%	+5.38%
2021	$103,290	$45,760	+6.08%	+9.08%
2022	$108,299	$46,310	+4.85%	+1.20%
2023	$113,540	$48,060	+4.84%	+3.78%
2024	$116,526	$49,500	+2.63%	+3.00%

Note: YoY refers to year-over-year percent charge.

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

Table 3. Top Five Cybersecurity Occupations by Average YoY Growth, 2019–2024

SOC Occupation Code	SOC Occupation Name	2024 Median Wage	Average YoY Growth
17-2061	Computer Hardware Engineers	$155,020	+5.81%
15-1254	Web Developers	$90,930	+5.72%
15-1299	Computer Occupations, All Other	$108,970	+4.24%
17-2072	Electronics Engineers, Except Computer	$127,590	+3.95%
15-2051	Data Scientists	$112,590	+3.72%

Note: YoY growth refers to year-over-year growth.

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

Table 4. Bottom Five Cybersecurity Occupations by Average YoY Growth, 2019–2024

SOC Occupation Code	SOC Occupation Name	2024 Median Wage	Average YoY Growth
13-1081	Logisticians	$80,880	+1.59%
13-1151	Training and Development Specialists	$65,850	+1.49%
19-2099	Physical Scientists, All Other	$117,960	+1.48%
15-1253	Software QA Analysts and Testers	$102,610	+1.47%
19-2021	Atmospheric and Space Scientists	$97,450	+0.75%

Note: YoY growth refers to year-over-year growth.

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

Cyber jobs still seem to pay well. The data shows that cyber workers earn more than twice the median wage of all U.S. workers. To confirm our findings, we examined whether occupations with a higher demand pressure show higher wage growth. To do this, we performed a variety of statistical tests. First, we calculated the correlation coefficient between the overall demand pressure and wage growth for cyber occupations. Then, we checked the overall correlation between demand pressure and wage premium. The cyber wage ratio—that is, the cyber median pay versus the economy-wide median—is remarkably stable at approximately 2.3 times the median wages for all jobs across the time frame.

As a final test regarding the relationship between demand pressure and wage growth, we grouped cyber occupations by P/E ratio and into four quartiles, as shown in Table 5. There is neither a clear correlation between demand pressure and wage growth nor between demand pressure and the wage premium. If demand pressure drove wage growth, there would be a clear progression, with each quartile exhibiting higher wage growth than the previous. Yet, the third quartile actually shows lower wage growth than the first quartile.

Table 5. P/E Ratio and Wage Growth of Cybersecurity Occupations, 2019–2024

Test	Result	Interpretation
Correlation between P/E and wage growth	r = +0.064	Near zero - no relationship
Correlation between P/E and cyber wage ratio	r = -0.067	Near zero - no relationship
P/E Quartile 1 (lowest, avg 0.14)	2.79% wage growth	Baseline
P/E Quartile 2 (avg 0.27)	3.12% wage growth	Slightly higher than Q1
P/E Quartile 3 (avg 0.41)	2.10% wage growth	Lower than Q1
P/E Quartile 4 (highest, avg 1.08)	3.53% wage growth	Only marginally higher than Q1

Note: P/E ratio refers to postings-to-employment ratio.
Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

Industry-Specific Tests

Although we determined that there is little meaningful evidence of a traditional labor shortage according to economic theory, we wanted to analyze if these effects hold across all sectors to increase our understanding of hiring difficulties at the industry level. To calculate P/E ratios by industry, we applied OEWS employment data by occupation and industry and Lightcast job posting data by industry at the two-digit NAICS level. We then applied a minimum threshold of 5,000 annual cyber workers in each industry for analysis.*

* This led to the exclusion of agriculture, mining, construction, real estate, arts, and accommodation and food services. There are two reasons for exclusion: Industries with fewer than 5,000 average annual cyber workers are subject to high variance from individual employer hiring cycles, and they represent less than 5 percent of the private sector cyber employment.

First, we found that cyber jobs seem to be concentrated in SOC 15-1299, which is the occupation “Computer Occupations, All Other.” Table 6 shows the share of cybersecurity job postings classified under SOC 15-1299 across major industries. These figures use cyber-share weighting to isolate true cybersecurity demand from general IT postings.

As these numbers show, SOC 15-1299 represents between 60 percent and 86 percent of cyber postings across all major industries. This trend appears to be widening. According to our analysis, the share of occupations from the broader IT pool classified as 15-1299 has been growing, from 14.2 percent in 2019 to 16.2 percent 2024. This represents a relative increase of 14 percent in just five years and suggests a widening gap between formal classifications and actual labor market demand.

To examine the nature of the cybersecurity talent shortage in more detail, we disaggregated our analysis from the broader labor market to the industry level using two-digit NAICS codes. Looking at the distribution of cyber demand by industry shows that around 40 percent is concentrated in professional, scientific, and technical services (NAICS 54), followed by manufacturing, with a posting share of 16.3 percent. As Table 7 shows, the top five industries account for almost 90 percent of all private-sector cyber postings and around 75 percent of total cybersecurity workers.

Table 6. Cybersecurity Job Postings in "Computer Occupations, All Other" SOC Occupation, 2019–2024

Industry	Share of Cybersecurity Job Postings
Public Administration	60.2%
Utilities	73.6%
Educational Services	75.4%
Other Services	75.6%
Management of Companies	77.2%
Wholesale Trade	77.6%
Unclassified Industry	77.9%
Health Care & Social Assistance	78.8%
Manufacturing	79.4%
Professional, Scientific, & Technical Services	79.6%
Transportation & Warehousing	81.3%
Administrative & Support Services	81.5%
Retail Trade	82.5%
Information	83.8%
Finance & Insurance	86.0%
AVERAGE ACROSS INDUSTRIES	78.0%
OVERALL (weighted by posting volume)	80.0%

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

Table 7. Cybersecurity Job Posting Share by NAICS Industry, 2019–2024

Rank	NAICS Industry (NAICS code)	Number of Cybersecurity Employees	Posting Share
1	Professional, Scientific, and Technical Services (54)	209	40.3%
2	Manufacturing (31-33)	53	16.3%
3	Admin & Support Services (56)	32	14.1%
4	Finance & Insurance (52)	55	11.6%
5	Information (51)	71	7.7%
6	Retail Trade (44-45)	7	3.0%
7	Health Care & Social Assistance (62)	21	1.8%
8	Educational Services (61)	30	1.7%
9	Wholesale Trade (42)	24	1.7%
10	Transportation & Warehousing (48-49)	8	0.9%
11	Other Services (81)	6	0.6%
12	Management of Companies (55)	44	0.3%

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

Interestingly, demand pressure for cybersecurity workers is highest in industries not traditionally associated with tech employment. Table 8 shows industry-level P/E ratios and posting shares for cybersecurity roles. We see that retail trade (NAICS 44-45) exhibits the highest demand pressure for cybersecurity workers, followed by administrative and support services and manufacturing. In comparison, demand pressure appears to be relatively low in the professional, scientific, and technical services sector as well as in information—the two largest private-sector employers of cybersecurity talent.

Table 8. P/E Ratios of Cybersecurity Jobs by Industry, 2019–2024

Rank	NAICS Industry (NAICS Code)	P/E Ratio	Posting Share
1	Retail Trade (44-45)	1.907	3.0%
2	Admin & Support Services (56)	1.841	14.1%
3	Manufacturing (31-33)	1.273	16.3%
4	Finance & Insurance (52)	0.868	11.6%
5	Professional/Scientific/Technical (54)	0.794	40.3%
6	Information (51)	0.449	7.7%
7	Other Services (81)	0.448	0.6%
8	Transportation & Warehousing (48-49)	0.442	0.9%
9	Health Care & Social Assistance (62)	0.354	1.8%
10	Wholesale Trade (42)	0.287	1.7%
11	Educational Services (61)	0.230	1.7%
12	Management of Companies (55)	0.033	0.3%

Note: P/E ratio refers to postings-to-employment ratio

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

Hiring Behavior

Using industry data, we conducted tests that were complementary to the previous wage analysis in order to assess whether elevated P/E ratios reflect genuine labor market tightness. To do so, we combined job posting data with information from the BLS JOLTS database. JOLTS provides industry-level data on hiring difficulty, expressed as fill rates, and worker confidence in current labor market conditions, expressed in

quit rates. Applying these metrics can help us to distinguish between genuine labor shortages and other factors like ghost jobs or skills mismatches.

JOLTS reports labor market metrics at the industry level, not by occupation. Hence, in order to estimate occupation-specific labor market conditions for cyber roles, we weighted industry-level JOLTS metrics by each cyber occupation's industry distribution based on actual job posting patterns. For example, if data scientists have 45 percent of postings in professional services and 18 percent in finance, we applied those weights to the corresponding industry-level fill rates and quits rates.

For the purpose of our analysis, we calculate two different JOLTS metrics. First, the fill rate, defined as hires divided by job openings. Here a lower rate indicates that positions are harder to fill. Second, the quits rate, defined as the number of voluntary separations divided by employment. In other words, the quits rate shows how often workers leave a job voluntarily. Higher quits rates commonly signal worker confidence in finding better jobs, indicating a tight labor market where workers have more options.

Returning to the quartile analysis, we divided cybersecurity jobs into four groups, based on their respective P/E ratios. The results are depicted in Table 9 below. Looking at columns two and three, we see that jobs with the highest demand pressure (the top quartile) were hardest to fill. Here only 65 percent of openings resulted in hires, compared to 75 percent of jobs in the quartile with the lowest demand pressure. This confirms that P/E ratios capture real hiring challenges.

That said, workers were not quitting their current jobs to chase these high-demand opportunities. This becomes clear when we focus on column four in Table 9. In the case of a genuine labor shortage, we would expect the quits rate to climb across quartiles. Workers in the most in-demand roles would enjoy the strongest outside options and would leave their current jobs more readily for better offers. Instead, quits remain essentially flat (2.37 percent to 2.50 percent), even as postings grow markedly harder to fill.

Taken together with our earlier finding that wages show no corresponding response to demand pressure, this asymmetry is difficult to reconcile with a broad scarcity of workers. If high-demand cyber roles were genuinely short of talent, we would expect to see this reflected in all three of these metrics: harder hiring, rising quits rates as workers chase better offers, and climbing wages as employers compete for scarce candidates. We observe only the first. Employers struggle to fill roles, yet workers who could fill them are neither being bid away nor bid up.

Table 9. Quartile Analysis of Cybersecurity Occupations

P/E Quartile	Average P/E	Average Fill Rate	Average Quits Rate
Q1 (Low P/E)	0.17	75.10%	2.37%
Q2	0.28	71.50%	2.43%
Q3	0.43	68.80%	2.50%
Q4 (High P/E)	1.20	65.40%	2.50%

Note: P/E ratio refers to postings-to-employment ratio.
Source: CSET Analysis of JOLTS data.

Region-Specific Tests

Taking note of the significant variation in P/E ratios across industries and the fact that demand pressures appear to be highest in industries not traditionally associated with tech employment, the final piece of our analysis focuses on the regional distribution of cyber job postings. The industries with the highest demand pressure—manufacturing, administrative and support services, and retail trade—demonstrate greater geographic dispersion. In other words, these industries post jobs across more dispersed locations where local cyber talent pools might be smaller.

Table 10 displays three measures of geographic concentration for the manufacturing, administrative and support services, and retail trade industries. The professional, scientific, and technical services sector, which is the largest employer of cybersecurity workers, is included as a reference group. The top 10 MSA share measures how much activity in each of these industries sits in the largest markets. The Herfindahl-Hirschman Index (HHI) measures whether a few individual metros dominate, since it weighs larger shares disproportionately. The number of metro areas needed to account for 80 percent of postings shows how widely job activity extends beyond the largest markets.

When an industry is unambiguously concentrated or dispersed, the three measures align. This is the case for manufacturing and administrative and support services, both of which are geographically less concentrated than the reference group on all three indicators.

Table 10. Geographic Concentration of Cybersecurity Job Postings by Industry, 2019–2024

Industry	P/E Ratio	Top 10 CBSAs	HHI	CBSAs for 80%
Professional, Scientific, & Technical Services (Reference Group)	0.79	50.70%	797	38
Manufacturing	1.27	45.30%	404	46
Administrative & Support Services	1.84	43.20%	302	44
Retail Trade (Highest P/E)	1.91	53.50%	447	33

Note: P/E ratio refers to postings-to-employment ratio, CBSA refers to core based statistical areas, and HHI refers to the Herfindahl-Hirschman index.

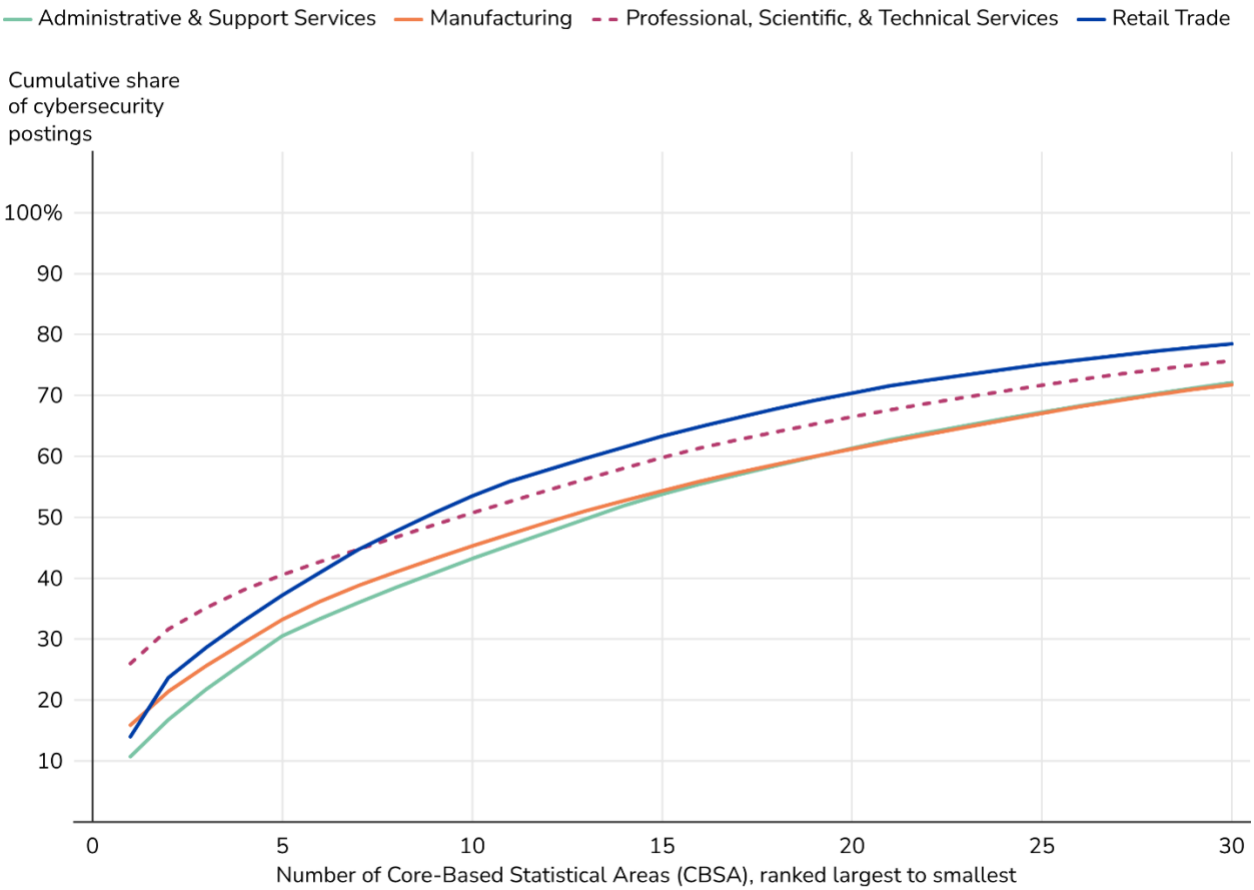
Source: CSET analysis of JOLTS data.

Retail and trade, in contrast, illustrates why a single measure can mislead. Its postings are no less concentrated in large metros than the reference group. In fact, its top 10 MSA share (53.5 percent) is slightly higher, and it reaches 80 percent of postings in fewer metros (33 versus 38). Yet, the data suggests that professional, scientific, and technical services is more top-heavy, as illustrated by the higher HHI. This indicates that for professional, scientific, and technical services, cyber demand concentrates in a small number of tech hubs, followed by a long list of smaller markets that each account for only a few postings.

Retail and trade, on the other hand, distributes its postings more evenly across a comparable set of larger consumer metros, with no single dominant center. A key takeaway here is that these two industries are concentrated differently, rather than one being uniformly more concentrated than the other. This distinction is easiest to see when using these three measures together.

To illustrate our regional results, we assessed where each industry's cyber job postings actually cluster across the country. Figure 1 plots how much each of the four industries' cyber hiring is accounted for by its largest metropolitan areas, building up from the single biggest metro outward. Two stories emerge from our data.

Figure 1. Geographic Concentration of Cybersecurity Job Postings by Industry, 2019–2024



Source: CSET analysis of Lightcast U.S. job postings data.

Cyber employment in professional, scientific, and technical services is heavily concentrated in one dominant hub. Washington, D.C., alone accounts for roughly a quarter of that industry's cyber postings, after which demand thins out quickly. Retail trade looks different. It has no single dominant hub. Rather, its postings are spread across a broader band of larger metro areas. This difference in shape is what makes the two lines in Figure 1 cross.

Professional, scientific, and technical services starts highest on the graph, because its one big hub gives it an early lead, but it flattens out soon after. Retail trade starts out lower but keeps climbing, so that once you move past the first handful of cities, it actually has more cyber hiring in the leading metros than any of the other three industries. In other words, these two industries are not simply "more" or "less" concentrated than one another; they are concentrated in different ways. This is why we use several complementary measures, because a single statistic would obscure a distinction that matters for where cyber talent is actually in demand.

These results suggest that hiring difficulties in the retail sector are less correlated with geographic dispersion. To investigate alternative explanations, we compared industry-occupation wage data from OEWS and found that retail pays cyber workers an average of 14 percent less than professional services for comparable positions.

Findings

Our analysis finds four key insights that not only deepen our understanding of the cybersecurity workforce landscape but provide some clarification to suggest that the United States is not experiencing a blanket shortage of cyber talent. Instead, our data shows that specific industries are experiencing difficulties, and that these industries may have other factors that contribute to this problem aside from a lack of supply. It is possible that some of the talent exists but it is not concentrated in these specific industries.

Demand pressure is higher among cybersecurity occupations. The analysis indicates that there is elevated demand for cybersecurity talent. At the industry level, we observed particularly elevated demand pressures in the retail trade and manufacturing sectors, and it is likely that these sectors are experiencing a genuine shortage of cyber talent. State and federal policy responses can be tailored specifically to these industries.

However, there are additional factors that contribute to this problem, as talent supply limitations cannot be understood in isolation. AI, of course, continues to change how cybersecurity is prioritized and conducted within companies and to reshape how critical cyber skills are defined.[5] At the same time, employers may be underinvesting in upskilling incumbent workers, and the education and training systems might not be agile in their response to shifting industry needs. If the workforce appears insufficient, it may reflect not only a quantitative shortfall but also structural inefficiencies in how cyber talent is developed, signaled, and utilized.

Additionally, entry-level pathways into cybersecurity continue to shrink, and limited employer participation in skills-based training programs weakens the connection between education systems and labor market demand. Prior research from CSET highlights this dynamic, finding that a perceived lack of entry-level cyber jobs discourages students from pursuing cybersecurity careers, even as employers report difficulty in filling roles.[6]

Despite the demand pressure, wages are not rising to compete for talent. In a standard labor shortage situation, employers compete for talent by raising wages. High-demand occupations should show fast wage growth as a result. The absence of this pattern in our data suggests employers are not competing primarily on wages, which in turn suggests there is not a broad shortage of cyber talent. Even though the manufacturing sector shows substantial geographic dispersion—only 45.3 percent of job postings in the top 10 MSAs compared to 50.7 percent for the professional services sector—it still offers competitive wages to attract the talent it requires.

In contrast, the retail trade sector struggles to compete on compensation. Despite the highest P/E ratio of any industry, retail trade presents with high geographic concentration within larger metro areas, as 53.5 percent of job postings are situated in the top 10 MSAs. Industry-occupation wage analysis reveals that the retail trade sector pays cyber workers an average of 14 percent less than professional services for comparable positions.

The characterization of a cyber job is likely changing. As mentioned above, the nature of how cybersecurity is prioritized and practiced continues to evolve at the pace of technological change. We believe these changes contribute to the perceived shortages of cyber talent, and they are also reflected in the data: Approximately 80 percent of cybersecurity job postings fall into SOC 15-1299. This catchall code captures roles that do not fit into established classifications with clearly defined knowledge and tasks, suggesting that cyber roles are evolving or changing in ways that are currently not captured by existing job classifications. This concentration holds across industries, from manufacturing (79.4 percent) to professional services (79.6 percent) to retail (82.5 percent).

This 80 percent figure is weighted by cyber-share, meaning we isolated postings that are substantively cybersecurity work rather than general IT work with a cyber component. If we instead look at all postings across every cyber-related SOC code, including roles that are primarily general IT, the share falling into the 15-1299 code drops to 15 percent. In other words, the closer a posting is to being genuinely cybersecurity focused, the more likely it is to defy existing job classifications.

This gap between weighted and unweighted figures reinforces our point: It is specifically cyber work, not IT work in general, that current classification systems struggle to capture. Part of this reflects a structural lag: SOC codes are updated relatively infrequently, and classification systems can take years to catch up with how a fast-moving field like cybersecurity is actually developing. It also speaks to the potential for a skills mismatch as one of the reasons for the perceived talent shortage. To put it simply, employers might not be finding the specific talent they need.

Better data collection, identification, and sharing is still needed. As the discussion above illustrates, collecting and sharing cybersecurity workforce data remains difficult. For one, we identified a limitation of the SOC taxonomy's ability to classify modern cybersecurity roles. This system is the federal government's official framework for classifying occupations and only receives major updates every ten years, the most recent of which occurred in 2018. A key problem with these infrequent updates is that new specializations emerge continuously.

In the domain of cybersecurity, new roles such as cloud security engineers, DevSecOps specialists, or threat intelligence analysts are all relatively recent additions. When these roles appear in job postings, the classification system lacks dedicated codes to assign them and subsumes them under 15-1299. This is not a novel problem but one that continues to occupy the interest of the federal government. For example, the National Science Foundation only recently concluded a yearlong study to assess the feasibility of producing national estimates and statistical information on the cybersecurity workforce.[7]

Conclusion

In conclusion, our analysis finds that the cybersecurity workforce is not suffering from a blanket talent shortage but is instead experiencing both broken industry-specific talent pipelines and an era of job characteristic changes. Policy responses must be tailored, industry specific, and driven by continued federal investment in tandem with local and state governments to incentivize a functioning workforce ecosystem. Simply producing more credentialed workers will not solve the problem. Workforce development initiatives must go beyond headcount metrics and measure success by how many graduates enter positions that align with actual employer needs.

At the same time, employers must be specific. When 80 percent of cybersecurity job postings fall into a catchall occupational category, it becomes nearly impossible to align training with demand. Employers should specify required skills with granularity, requiring not just "cybersecurity experience" but specific platforms, tools, and capabilities. They should differentiate "must have" from "nice to have" qualifications and provide realistic experience requirements. This enables training providers to align curricula with actual needs, job seekers to make informed decisions, and policymakers to measure whether interventions are working.

However, while we believe that our approach provides a comprehensive view of the current state of cyber workforce supply, it is worth noting that job posting volume alone cannot establish or define the shortage independently. Our analysis was not designed to measure the effectiveness of existing training programs, the value of credentials, or specific outcomes of federal investments.

Such challenges are not new. Previous federal efforts, including the National Cyber Workforce and Education Strategy, similarly emphasized the need for a "whole-of-nation" approach to strengthening long-term cyber talent pipelines.[8] The new Cyber Strategy for America also aims to eliminate roadblocks that prevent industry, academia, government, and the military from aligning on cyber workforce initiatives. However, persistent gaps suggest that alignment alone is insufficient without a clearer understanding of how cyber talent supply is generated and where it breaks down.

Authors

Ali Crawford is a senior research analyst at CSET, where she focuses on cyber and AI education and workforce development.

Matthias Oschinski is a senior fellow at CSET, where he leads the research on workforce and education. His primary research is focused on the AI and cyber workforce, the process of AI adoption, the impact of AI on education and educational institutions, and how to improve labor market information.

Acknowledgments

For a thorough and helpful review of an early draft of this report, we would like to thank Tobi West, Seeyew Mo, and Michael Prebil for their time and contributions to the final version of this report. We would also like to thank Kyle Crichton, Jack Karsten, and Catherine Aiken for their internal reviews. Finally, we are grateful for the support of our CSET external affairs team for bringing this report to life.



© 2026 by the Center for Security and Emerging Technology. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/4.0/.

Document Identifier: doi: 10.51593/20250022

Appendix

A. Data Sources and Coverage

a. Job postings data (Lightcast)

i. Source: Lightcast

ii. Coverage: 2019–2024 annual job posting counts

iii. Unit of observation: 5-digit SOC code × NAICS 2-digit industry × year

iv. Geographic detail: MSA level for geographic analysis

v. Total postings analyzed: Approximately 21.2 million cyber-related job postings (after cyber-share weighting)

b. Cyber job identification

i. Cybersecurity-relevant positions identified using CSET's machine learning classifier developed in Snorkel Flow, informed by the NICE Workforce Framework. The classifier distinguishes cybersecurity roles from general IT positions across both technical and nontechnical occupations.

c. Cyber-share weighting

i. Each occupation assigned a "cyber-share" representing the proportion of postings in that SOC code that are genuinely cybersecurity relevant (vs. general IT). For example:

1. SOC 15-1299 (Computer Occupations, All Other): 33.9% cyber-share

2. SOC 15-1252 (Software Developers): 6.0% cyber-share

ii. Cyber-share weights applied to both numerator (postings) and denominator (employment) when calculating aggregate statistics to isolate true cybersecurity demand from general IT work.

d. Employment and wage data

i. Source: BLS OEWS

ii. Coverage: 2019–2024 annual median wages and employment counts

iii. Unit of observation: 5-digit SOC code × year

iv. Additional detail: Industry × occupation cross-tabulations for wage differential analysis

v. Employment counts: Used as denominator in P/E ratio calculations

vi. Median wages: Used for wage growth analysis and industry wage comparisons

vii. Wage premium: Calculated as cyber median wage ÷ all-jobs median wage

e. JOLTS data

i. Source: BLS JOLTS

ii. Coverage: 2019–2024 monthly data aggregated to annual

iii. Unit of observation: NAICS 2-digit industry × year

iv. Variables used:

1. Hires (monthly)
2. Job openings (monthly)
3. Voluntary separations / quits (monthly)
4. Employment level (monthly)

v. Metrics calculated:

1. Fill rate = Hires ÷ Job openings
2. Quits rate = Quits ÷ Employment

vi. Industry coverage: 16 major industries reported in JOLTS (excludes Agriculture, some small sectors)

f. Geographic data

i. Source: Lightcast posting counts by MSA

ii. Coverage: 925 MSAs, 2019–2024 aggregated

iii. Variables calculated:

1. Percentage of postings in top 10 MSAs
2. HHI
3. Number of MSAs required to account for 80% of postings

B. Methodology

a. Postings-to-employment (P/E) ratio calculation

i. Basic formula: P/E = (Job Postings) ÷ (Employment)

ii. Occupation-level P/E (unweighted): P/E_occ = Postings_occ ÷ Employment_occ

iii. Occupation-level P/E (cyber-share weighted): P/E_occ_weighted = (Postings_occ × cyber_share_occ) ÷ (Employment_occ × cyber_share_occ) = Postings_occ ÷ Employment_occ

1. *Note: Cyber-share cancels when calculating single-occupation P/E, but affects aggregation across occupations.*

iv. Aggregate P/E (across all cyber occupations): P/E_aggregate = ∑(Postings_occ × cyber_share_occ) ÷ ∑(Employment_occ × cyber_share_occ)

1. *Note: This weighting ensures we measure demand pressure for actual cybersecurity work, not general IT positions that happen to fall under "cyber-related" SOC codes.*

b. Industry-level P/E calculation

i. Formula: P/E_industry = Postings_industry ÷ Employment_industry

ii. Where:

1. Postings_industry = ∑(Postings_occ,ind × cyber_share_occ) across all occupations in that industry
2. Employment_industry = ∑(Employment_occ,ind × cyber_share_occ) across all occupations in that industry
3. Industry filters applied:
    a. Excluded Government (NAICS 99): Recruits via USAJobs, not commercial job boards
    b. Excluded industries with <5,000 average annual cyber workers: Agriculture (11), Mining (21), Construction (23), Real Estate (53), Arts (71), Accommodation & Food (72)
4. Justification for size threshold:
    a. Industries with fewer than 5,000 average annual cyber workers were excluded on two grounds: statistical reliability (small samples subject to high variance from individual employer hiring cycles) and policy relevance (collectively representing less than 5% of private-sector cyber employment). The remaining industries cover more than 95% of cybersecurity workers.

c. JOLTS triangulation methodology

i. Challenge: JOLTS reports industry-level metrics, not occupation-level.

ii. Solution: Weight industry-level JOLTS metrics by each occupation's industry distribution based on job posting patterns.

iii. Step 1: Calculate occupation industry weights

1. For each occupation o, calculate the share of its postings in each industry i: weight_o,i = Postings_o,i ÷ ∑(Postings_o,all_industries)

iv. Step 2: Calculate weighted JOLTS metrics

    1. For each occupation o, calculate its weighted fill rate: $FillRate_o = \sum(weight_{o,i} \times FillRate_i)$

    2. Where $FillRate_i$ is the industry-level fill rate from JOLTS.

v. Example:

    1. If Data Scientists have:

        a. 45% of postings in Professional Services (fill rate 72%)

        b. 18% of postings in Finance (fill rate 68%)

        c. 37% in other industries...

    2. Then:

        a. $FillRate_{DataScientists} = (0.45 \times 0.72) + (0.18 \times 0.68) + ...$

vi. Dynamic vs. Static Weights:

    1. Two approaches tested:

        a. Static (aggregated): Use overall 2019–2024 industry distribution

        b. Dynamic (year-specific): Use year-specific industry weights

vii. Robustness check results:

    1. Dynamic weights: r = -0.254, quartile decline 10.2 pp

    2. Static weights: r = -0.274, quartile decline 12.9 pp

viii. Results nearly identical; reported analysis uses dynamic weights for JOLTS calculations but static aggregates for descriptive industry statistics (concentration, 15-1299 dominance) for clarity.

d. Geographic concentration metrics

i. Metric 1: Top 10 MSA Share

1. Top10_pct = (Postings in top 10 MSAs) ÷ (Total postings) × 100

2. Higher percentage = more concentrated in major metros.

ii. Metric 2: HHI

1. HHI = ∑(market_share_msa²) × 10,000

2. Where market_share_msa = Postings_msa ÷ Total_postings

a. HHI > 1,800 = highly concentrated

b. HHI < 1,000 = competitive/dispersed market

c. Standard antitrust measure adapted for geographic concentration

iii. Metric 3: MSAs for 80% of postings

1. Sort MSAs by posting volume (descending), count how many MSAs needed to reach 80% cumulative share.

2. Fewer MSAs = more concentrated.

e. 15-1299 Classification Analysis

i. Unweighted share: Share_unweighted = (Postings in 15-1299) ÷ (All cyber-related SOC postings) × 100

1. Result: ~15% (14.2% in 2019 → 16.2% in 2024)

ii. Weighted share (by industry):

1. For each industry: Share_industry = (15-1299 postings × cyber_share_15-1299) ÷ ∑(Postings_all_SOCs × cyber_share_each_SOC) × 100

a. Result: ~79-80% across most industries

iii. Interpretation of difference:

1. The 15% unweighted figure measures 15-1299 against all postings in cyber-related SOCs (including Software Developers, Network Admins, etc.). The 80% weighted figure measures 15-1299 against actual cybersecurity work after filtering out non-cyber portions of each occupation. The difference reveals that most postings in "cyber-related" SOCs are general IT, while the actual cyber work is concentrated in the catchall.

C. Statistical Tests

a. Correlation analysis

i. Pearson correlation coefficient: r = Cov(X,Y) ÷ (SD_x × SD_y)

1. Tests performed:

a. P/E vs. Wage Growth: r = +0.064 (n=162 occupation-years)

b. P/E vs. Wage Premium: r = +0.062

c. P/E vs. Fill Rate: r = -0.274 (n=162)

d. P/E vs. Quits Rate: r = +0.214 (n=162)

ii. Sample size: 27 occupations × 6 years = 162 observations

iii. Statistical significance: All correlations tested at $\alpha = 0.05$ level

b. Quartile analysis

i. Occupations grouped into four equal-sized groups based on P/E ratios:

1. Q1 (lowest 25% of P/E): 7 occupations

2. Q2 (25th–50th percentile): 7 occupations

3. Q3 (50th–75th percentile): 6 occupations

4. Q4 (highest 25% of P/E): 7 occupations

ii. For each quartile, calculated:

1. Average P/E ratio
2. Average wage growth
3. Average fill rate (JOLTS-weighted)
4. Average quits rate (JOLTS-weighted)

iii. Test for monotonic pattern: Visual inspection and Spearman rank correlation to test whether metrics progress consistently across quartiles.

D. Occupation and Industry Lists

a. Cybersecurity Occupations Analyzed

Table 11. High-P/E cybersecurity occupations (P/E > 1)

SOC Occupation Code	SOC Occupation Name	P/E Ratio
15-2051	Data Scientists	2.22
15-1243	Database Architects	1.91
15-1242	Database Administrators	1.54
15-1299	Computer Occupations, All Other	1.44
15-1254	Web Developers	1.31

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

Table 12. Low-P/E cybersecurity occupations (P/E < 0.3)

SOC Occupation Code	SOC Occupation Name	P/E Ratio
17-2011	Aerospace Engineers	0.16
17-2199	Engineers, All Other	0.14
19-2099	Physical Scientists, All Other	0.13
15-1251	Computer Programmers	0.23
13-1151	Training and Development Specialists	0.23

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

b. Industries Analyzed

i. Excluded:

1. NAICS 99 (Government)—structural differences in recruitment
2. NAICS 11 (Agriculture), 21 (Mining), 23 (Construction), 53 (Real Estate), 71 (Arts), 72 (Accommodation & Food)—<5,000 avg annual cyber workers

Table 13. P/E ratios of cybersecurity industries

NAICS Code (2-digit)	NAICS Industry Name	P/E Ratio
54	Professional, Scientific, & Technical Services	0.79
31-33	Manufacturing	1.27
56	Administrative & Support Services	1.84
44-45	Retail Trade	1.91
52	Finance & Insurance	0.87
51	Information	0.45
62	Health Care & Social Assistance	0.35
61	Educational Services	0.23
42	Wholesale Trade	0.29
48-49	Transportation & Warehousing	0.44
81	Other Services	0.45
55	Management of Companies	0.03

Source: CSET analysis of OEWS and Lightcast U.S. job postings data.

E. Robustness Checks

a. Dynamic vs. static industry weights (JOLTS)

i. Test: Do results change if we use year-specific industry weights instead of aggregated 2019–2024 weights?

ii. Method:

1. Static: Calculate each occupation's industry distribution across all years 2019–2024
2. Dynamic: Calculate each occupation's industry distribution separately for each year

iii. Results:

1. P/E vs. Fill Rate correlation: r = -0.274 (static) vs. r = -0.254 (dynamic)
2. Quartile decline in fill rates: 12.9 pp (static) vs. 10.2 pp (dynamic)
3. Monotonic pattern preserved in both approaches

iv. Conclusion: Results robust to weight specification. Findings do not depend on methodological choices.

v. Note: Professional Services share varied from 42.1% (2020 peak) to 34.3% (2022 trough) during COVID/tech layoff period, demonstrating why dynamic weights capture temporal variation. However, substantive conclusions remain unchanged.

b. Alternative P/E calculations

i. Test: Do results change with different aggregation approaches?

ii. Alternatives tested:

1. Simple average of occupation-level P/E ratios (unweighted)
2. Weighted average using employment weights
3. Weighted average using posting volume weights
4. Cyber-share weighted (reported approach)

iii. Result: Cyber-share weighting provides the most accurate measure of true cybersecurity demand by filtering out general IT work. Other approaches overstate demand pressure by including non-cyber positions.

F. P/E Ratios by Occupation (2019–2024)

SOC Occupation Code	SOC Occupation Name	Cyber-Share	Average P/E
15-2051	Data Scientists	5.5%	2.218
15-1243	Database Architects	10.8%	1.914
15-1242	Database Administrators	5.4%	1.536
15-1299	Computer Occupations, All Other	33.9%	1.437
15-1254	Web Developers	2.4%	1.313
13-1081	Logisticians	1.3%	0.831
15-1252	Software Developers	6.0%	0.638
17-2071	Electrical Engineers	3.5%	0.600
17-2112	Industrial Engineers	1.9%	0.532
15-1253	Software Quality Assurance Analysts and Testers	7.6%	0.506
33-9099	Protective Service Workers, All Other	1.5%	0.448
15-2031	Operations Research Analysts	6.4%	0.427
17-2072	Electronics Engineers, Except Computer	7.2%	0.390
15-1232	Computer User Support Specialists	13.0%	0.381
17-2141	Mechanical Engineers	2.3%	0.364
17-2161	Nuclear Engineers	6.6%	0.315
19-2021	Atmospheric and Space Scientists	1.8%	0.311
17-2061	Computer Hardware Engineers	6.5%	0.306
13-1041	Compliance Officers	6.6%	0.277
15-1211	Computer Systems Analysts	14.4%	0.266
15-1251	Computer Programmers	4.0%	0.232
13-1151	Training and Development Specialists	2.7%	0.232

17-2031	Bioengineers and Biomedical Engineers	1.5%	0.213
17-2011	Aerospace Engineers	6.9%	0.163
17-2199	Engineers, All Other	4.2%	0.143
19-2099	Physical Scientists, All Other	6.1%	0.131

Note: Two occupations from the original 28-occupation classification are excluded from this table: 11-3021 (Computer and Information Systems Managers), which is a management rather than technical role, and 55-9999 (Military Occupations), as military personnel are outside the scope of civilian labor market analysis and are not covered in OEWS employment data.

References

Causa, Orsetta, Emilia Soldani, Maxime Nguyen, and Tomomi Tanaka. "Labour Shortages and Labour Market Inequalities: Evidence and Policy Implications." OECD Economics Department Working Paper No. 1832. OECD Publishing, March 2025. www.oecd.org/en/publications/labour-shortages-and-labour-market-inequalities_14e62ec0-en.html.

Ferguson, Thomas, and Servaas Storm. "A New Era of Endless Labor Shortages? A Critical Analysis of McKinsey's New Report." Institute for New Economic Thinking, July 15, 2024. www.ineteconomics.org/perspectives/blog/a-new-era-of-endless-labor-shortages-a-critical-analysis-of-mckinseys-new-report.

Handel, Michael J. "Labor Shortages: What Is the Problem?" *Intereconomics 59*, no. 3 (June 2024): 136–142. https://doi.org/10.2478/ie-2024-0029.

OECD. "Understanding Labour Shortages: The Structural Forces at Play." *OECD Economic Outlook* 2024, no. 2 (December 2024). www.oecd.org/en/publications/oecd-economic-outlook-volume-2024-issue-2_d8814e8b-en/full-report/understanding-labour-shortages-the-structural-forces-at-play_321e116a.html.

Ratner, Alexander, Stephen H. Bach, Henry Ehrenberg, Jason Fries, Sen Wu, and Christopher Ré. "Snorkel: Rapid Training Data Creation with Weak Supervision." *Proceedings of the VLDB Endowment* 11, no. 3 (November 2017): 269–282. https://doi.org/10.14778/3157794.3157797.

Seghir, Majda. "The Evidence Gap in Labour Shortage Assessments." *Intereconomics* 59, no. 3 (June 2024): 143–145. https://doi.org/10.2478/ie-2024-0030.

Subbu Rathinam, Sonali, and Ronnie Kinoshita. "Identifying the AI Development Workforce." CSET, June 2026 https://doi.org/10.51593/20240037.

Endnotes

[1] White House, *President Trump's Cyber Strategy for America* (Washington, D.C.: White House, March 2026), www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf.

[2] White House, *Winning the Race: America's AI Action Plan* (Washington, D.C.: Office of Science and Technology Policy, July 2025), www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf; U.S. Department of Labor, U.S. Department of Commerce, and U.S. Department of Education, *America's Talent Strategy: Building the Workforce for the Golden Age* (Washington, D.C.: U.S. Department of Labor, August 2025), www.dol.gov/sites/dolgov/files/OPA/newsreleases/2025/08/Americas-Talent-Strategy-Building-the-Workforce-for-the-Golden-Age.pdf.

[3] CyberSeek, "Cybersecurity Supply and Demand Heat Map," accessed April 15, 2026, www.cyberseek.org/heatmap.html.

[4] Michael J. Handel, "Labor Shortages: What Is the Problem?," *Intereconomics 59*, no. 3 (June 2024): 136–142, https://doi.org/10.2478/ie-2024-0029; Majda Seghir, "The Evidence Gap in Labour Shortage Assessments," *Intereconomics* 59, no. 3 (June 2024): 143–145, https://doi.org/10.2478/ie-2024-0030.

[5] "2025 ISC2 Cybersecurity Workforce Study: Cybersecurity Professionals Navigate Evolving Workplaces While Seizing New Opportunities," (ISC2, December 2025), https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/insights/Features/2025/12/COMMS_2025_Cybersecurity_WFS_Report_Whitepaper.pdf.

[6] Ali Crawford, "The Future of Work-Based Learning for Cyber Jobs" (Center for Security and Emerging Technology, July 2025), https://doi.org/10.51593/20240057.

[7] National Center for Science and Engineering Statistics, "The Cybersecurity Workforce Data Initiative," National Science Foundation, accessed June 25, 2026, https://ncses.nsf.gov/initiatives/cybersecurity-workforce-data-initiative.

[8] Office of the National Cyber Director, *National Cyber Workforce and Education Strategy* (Washington, D.C.: White House, July 31, 2023), https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.