The Cybersecurity Employment Paradox: Reconciling Workforce Shortage Narratives with Labour Market Realities in the United States, United Kingdom, and European Union

Elijah Adeyeye

Elitech-Hub Limited, Nigeria

ORCID iD: 0009-0005-4853-7813

Author Note

The author is the founder of a cybersecurity training and consulting organisation and has a professional interest in the labour market examined in this manuscript. This positionality is disclosed for transparency. The analysis relies on independently produced, publicly available secondary data and does not use proprietary organisational data.

Abstract

For over a decade, cybersecurity has been marketed as a field defined by near-zero unemployment, chronic understaffing, and a global shortage running into the millions. At the same time, a growing body of anecdotal and survey evidence shows trained, certified professionals, particularly at entry level, struggling to secure their first role, while established practitioners report layoffs, hiring freezes, and stagnant wages. This paper examines that apparent contradiction across the United States, United Kingdom, and European Union using secondary labour-market data from CyberSeek, the U.S. Bureau of Labor Statistics, ISC2's Cybersecurity Workforce Study, the UK Department for Science, Innovation and Technology (DSIT), and the European Union Agency for Cybersecurity (ENISA). The paper finds that the "workforce gap" is not a single measurable quantity but several distinct constructs (perceived organisational need, unfilled postings, and structural shortfall) that are routinely conflated in public discourse. It further finds that labour market strain is concentrated overwhelmingly at the entry-level and among mid-career professionals during periods of macroeconomic contraction, while demand for professionals with two to six years of specialised experience remains genuinely tight. The paper concludes that the popular narrative of undifferentiated abundance is a methodological and rhetorical artefact rather than an empirical finding, and offers implications for job seekers, training providers, and policymakers.

Keywords: cybersecurity workforce, skills gap, labour market, entry-level employment, ISC2, DSIT, ENISA, CyberSeek

Introduction

Few claims in the technology sector are repeated as consistently, or as uncritically, as the claim that cybersecurity offers near-guaranteed employment to anyone willing to acquire the

relevant skills. Training providers, certification bodies, government agencies, and media outlets have for years cited a global shortfall of several million unfilled cybersecurity positions as evidence that the field is both recession-proof and chronically hungry for new talent. Bootcamps and university programmes have expanded rapidly on the strength of this narrative, and it has become a recruiting pitch for career changers seeking a reliable route into well-paid technical work.

Set against this narrative is a body of practitioner testimony that tells a markedly different story. Entry-level job seekers holding recognised certifications report submitting hundreds of applications without success. Experienced professionals describe being laid off during a period in which the industry was ostensibly desperate for their skills. Hiring managers describe being unable to fill senior or specialised roles while simultaneously being flooded with applications for junior positions. The result is a public conversation in which two apparently incompatible claims are advanced with equal confidence: that the field is short of hundreds of thousands, or millions, of workers, and that trained workers cannot get hired.

This paper treats that contradiction as an empirical question rather than a matter of anecdote or sentiment. It asks three related questions. First, what do the major workforce statistics actually measure, and are they measuring the same thing? Second, does the available secondary data support a genuine, undifferentiated labour shortage, or a more specific and unevenly distributed one? Third, what explains the persistence of the abundance narrative given the evidence available to challenge it?

The stakes of this question are not confined to the three jurisdictions examined here. Training providers and career changers in regions without their own large-scale, government-commissioned labour market surveys, much of the Global South included, rely disproportionately

on the same headline global figures this paper interrogates, since locally validated alternatives typically do not exist. A career changer deciding whether to invest months of income and savings into cybersecurity training is, in practice, making that decision on the strength of a globally circulated shortage figure that this paper finds to be internally contested even within the jurisdictions that produce it. This makes the question of what these figures actually measure a matter of direct practical consequence well beyond the US, UK, and EU labour markets from which the underlying data in this paper is drawn.

This paper's contribution is not the discovery of new primary data, but a structured, comparative reading of existing, credible, publicly available data that is rarely placed side by side. Individually, DSIT's UK shortfall figure (DSIT et al., 2025), ISC2's global perceived-need figure (ISC2, 2025), and CyberSeek's US posting count (CyberSeek, n.d.) are each reported accurately by their respective publishers. The confusion this paper addresses arises almost entirely downstream of publication, in how these figures are subsequently cited, compared, and conflated by secondary sources, training providers, and media coverage that do not preserve the methodological caveats attached to each original figure.

The paper proceeds as follows. The next section reviews prior literature and public commentary on the cybersecurity skills gap, including a significant 2024–2025 controversy over the reliability of the most widely cited global figure. This is followed by the methodology, setting out the secondary data sources and comparative approach used. Findings are then presented across the United States, United Kingdom, and European Union, followed by a discussion of what these findings mean for the persistence of the shortage narrative and for the training industry that has grown around it. The paper closes with recommendations for job seekers, training providers such as bootcamps, and policymakers.

Literature Review

The origin and persistence of the "gap" figure

The figure most frequently cited in public discourse, a global shortfall of approximately 4.8 million cybersecurity professionals, originates from ISC2's annual Cybersecurity Workforce Study (ISC2, 2024), a large-scale survey of practitioners and decision-makers conducted since 2015. For several years, ISC2's reporting on this figure anchored a wide range of secondary commentary, marketing material, and government policy discussion.

In late 2024, this figure became the subject of direct public criticism. A senior cybersecurity practitioner and CISO wrote an open letter to ISC2's board arguing that the organisation was knowingly promoting a misleading picture of a plentiful job market, pointing to evidence of stagnant actual employment alongside the widely cited multi-million figure, and drawing on direct conversations with a number of unemployed cybersecurity professionals (Winkler, 2024). The criticism centred on a methodological objection: the figure was derived from survey respondents' perception of how many additional staff their organisation would ideally need, not from verified job postings, approved headcount, or hiring budget. Critics argued that treating a perceived-need figure as equivalent to actual market demand had misled several years of career changers and training investment.

ISC2's own 2025 Workforce Study, based on responses from a record 16,029 practitioners and decision-makers, subsequently discontinued reporting the workforce gap estimate altogether, stating that respondents had increasingly prioritised the need for critical skills within existing teams over the need for additional headcount (ISC2, 2025). This is a notable finding in its own right: the organisation most closely associated with the multi-million shortage figure removed it from its own flagship report within roughly a year of the figure being challenged.

Alternative accounts: hiring practices rather than talent scarcity

A separate strand of practitioner commentary, distinct from the ISC2 controversy but predating it by several years, has argued that the apparent skills gap reflects dysfunctional hiring practices rather than a genuine scarcity of qualified people. This critique holds that many job postings bundle the requirements of several distinct roles into a single listing, request years of experience disproportionate to the seniority of the role, or are posted without a validated intention to fill them at the terms advertised. Under this account, the large number of open postings cited as evidence of a shortage is partly an artefact of how those postings are written and validated, rather than a clean measure of unmet demand.

Academic treatments of the skills gap

Academic literature on the cybersecurity skills gap has generally taken a narrower and more empirically cautious approach than industry reporting. A sub-field analysis of job postings against a nine-category cybersecurity taxonomy finds that the gap is not uniform across the discipline: it is concentrated in specific functional areas, including governance, risk and compliance, and analytical or research-oriented roles, while other areas show closer alignment between what is taught and what is demanded (Ramezan, 2023). Comparative work examining curricula against industry demand in European contexts reaches a broadly similar conclusion (Jumaan et al., 2026), and a related strand of work applying document-frequency analysis to job advertisements and university syllabi across German-speaking Europe finds the same pattern using an independent method (Goupil et al., 2022): mismatches between industry demand and academic supply cluster around specific skill categories rather than appearing uniformly across the discipline, meaning that "the skills gap" behaves less like a single scarcity and more like a set of localised shortages in particular sub-domains.

This body of work is consistent with a separate strand using Delphi methods with cybersecurity experts to identify core knowledge areas (Parekh et al., 2018), which has found persistent disagreement over what constitutes foundational competence in the field. If practitioners and educators themselves do not agree on what a graduate should know, employer dissatisfaction with graduate preparedness and graduate frustration with employer expectations become, to some extent, mechanically inevitable. Each side is implicitly working from a different definition of competence. This provides a partial, structural explanation for why employers and training providers frequently talk past one another when discussing the gap: they may not be disagreeing about the same underlying phenomenon at all.

The role of certification and bootcamp marketing

A further consideration relevant to this paper's later discussion of training providers is the incentive structure surrounding certification and bootcamp marketing. Multiple industry commentators, writing from inside the training and hiring ecosystem, have observed that certifications such as CompTIA Security+ and the Certified Ethical Hacker credential are frequently marketed as a near-sufficient condition for employment, while simultaneously being described by hiring managers as necessary but insufficient: a baseline credential that filters candidates without materially differentiating between them once the applicant pool for a given entry-level posting reaches the scale now typical of the market. This gap between marketing framing and hiring-manager framing of the same credential is itself a contributor to the disappointment reported by newly certified job seekers who expected the certification to function as a more decisive signal than employers treat it as being.

Summary

Taken together, the existing literature and commentary suggest that "the cybersecurity skills gap" is not a single, stable, well-measured phenomenon. It is a label applied to at least three conceptually distinct constructs: perceived organisational need (as surveyed by ISC2 and similar bodies), unfilled job postings (as counted by labour-market intelligence platforms such as CyberSeek and Lightcast), and a modelled structural shortfall between projected supply and demand (as estimated by government-commissioned labour market studies). This paper treats the distinction between these constructs as central to resolving the apparent paradox, and structures its comparative analysis accordingly.

Methodology

This paper adopts a secondary-data, comparative-analysis approach rather than primary survey research. The rationale for this choice is twofold. First, several institutions already conduct large-sample, methodologically transparent surveys of the cybersecurity workforce on an annual or near-annual basis, offering more statistical power than an independent primary study could achieve within the scope of a single paper. Second, the central research question (whether commonly cited figures measure what they are popularly understood to measure) is itself a question about the properties of existing datasets, and is best answered by close comparative reading of those datasets rather than by generating new ones.

Data sources

The paper draws on the following primary sources for each jurisdiction:

United States. CyberSeek (a joint initiative of the U.S. Department of Commerce's National Institute of Standards and Technology, CompTIA, and Lightcast) is used for real-time job posting volume and role-level data (CyberSeek, n.d.). The U.S. Bureau of Labor Statistics (BLS)

Occupational Outlook Handbook is used for wage and projected growth data for information security analyst roles (U.S. Bureau of Labor Statistics, n.d.). ISC2's Cybersecurity Workforce Study (2023, 2024, and 2025 editions) is used for practitioner-reported organisational strain, including layoffs, budget cuts, and hiring freezes (ISC2, 2024, 2025).

United Kingdom. The DSIT-commissioned "Cyber Security Skills in the UK Labour Market" series, produced by Ipsos and Perspective Economics, is used as the primary UK data source (DSIT et al., 2025). This series has been published annually since approximately 2018 and combines representative business surveys, qualitative interviews with recruiters and employers, and secondary analysis of job posting data from labour market intelligence platforms. The companion "UK Cyber Security Sectoral Analysis" report is used for sector-level employment and revenue figures (Ipsos & Perspective Economics, 2025).

European Union. ENISA's NIS Investments report series and associated EU-level commentary are used for organisational-level data on hiring difficulty, budget allocation, and structural workforce trends (ENISA, 2025). Given the comparative absence of a single EU-wide labour-market survey equivalent in rigour to the UK's DSIT series, EU-level figures in this paper should be read as less methodologically uniform than the UK or US figures, and this limitation is treated explicitly in the discussion.

Analytical approach

For each jurisdiction, the paper distinguishes between three categories of figure wherever the underlying data permits: (a) perceived-need estimates derived from practitioner or employer surveys; (b) job-posting-volume estimates derived from labour market intelligence platforms; and (c) modelled structural shortfall estimates that attempt to net supply against demand over a defined period. Where a single source reports multiple such figures for the same jurisdiction and year, this

is treated as a finding in itself, since it demonstrates the scale of possible variation attributable to methodology alone rather than to underlying market conditions.

The paper does not attempt to adjudicate which figure is "correct" in an absolute sense. Its analytical claim is narrower and, the author argues, more defensible: that the divergence between these figures is itself the primary explanation for the coexistence of shortage rhetoric and entry-level saturation in public discourse.

Comparability across jurisdictions

Cross-country comparison of labour market statistics is inherently constrained by differences in occupational classification systems, survey timing, and sampling methodology, and cybersecurity-specific data is no exception. The UK's DSIT series and the EU's ENISA-coordinated reporting do not use identical definitions of who counts as a "cybersecurity professional," nor do they survey at the same point in the calendar year, and the US data drawn from CyberSeek and BLS reflects a different occupational classification system again. Where this paper presents cross-jurisdictional comparisons, these should be read as indicative of a shared pattern, the divergence between perceived-need and validated-demand figures, rather than as precise quantitative comparisons of shortage magnitude between countries. This limitation is a direct consequence of the current absence of a harmonised international cybersecurity labour market survey, a gap this paper's concluding recommendations address directly.

Findings

United States: high-level abundance, entry-level congestion

CyberSeek data shows a substantial number of open cybersecurity job postings in the United States, reported at over 514,000 in 2026, a figure regularly cited as evidence of chronic

demand (CyberSeek, n.d.). BLS projects continued above-average growth in information security analyst employment, and reports entry-level salaries for the occupation that exceed the national median wage across all occupations, alongside a median cybersecurity salary in the low six figures once mid-career and senior roles are included (U.S. Bureau of Labor Statistics, n.d.).

At the same time, ISC2's 2025 Workforce Study, based on a record 16,029 respondents, documents continuing organisational strain. Layoffs were reported by 24% of respondents and budget cuts by 36% in the twelve months prior to the survey, with both figures concentrated disproportionately among the largest organisations: 32% of large-organisation respondents reported layoffs, 46% reported budget cuts, 49% reported hiring freezes, and 41% reported promotion freezes (ISC2, 2025). These figures represent a slight improvement on the prior year, but remain elevated, and coexist with the headline demand figures in the same reporting period.

Separately, practitioner and hiring-manager commentary points in the same direction: the supply of new entrants, via degree programmes, bootcamps, and certifications combined, is widely reported to be growing faster than entry-level opening volume, though a rigorously sourced national figure quantifying that gap was not identified in the course of this research and would be a natural target for the future work discussed below. Labour market commentary from early 2026 similarly notes that hiring demand is concentrated among candidates with two to six years of experience, with entry-level opportunities described as comparatively limited even as overall postings remain elevated relative to other technology sectors.

The clearest single data point illustrating the gap between headline and ground-level reality is the fate of the 4.8 million figure itself. As discussed earlier, the organisation that produced and popularised this number discontinued it in its most recent flagship report following direct public criticism that it conflated perceived organisational need with actual hiring demand (ISC2, 2024,

2025; Winkler, 2024). CyberSeek's more conservative, posting-based figure of roughly half a million open US positions (CyberSeek, n.d.), an order of magnitude smaller, is arguably a more defensible measure of realised demand, though it still does not distinguish entry-level from experienced-hire postings, nor does it validate that all postings reflect a genuine, funded intention to hire at the advertised level.

United Kingdom: a shortfall that has collapsed by an order of magnitude in two years

The UK offers the most methodologically transparent national dataset available for this study, and its trend data is particularly instructive. DSIT's most recent labour market report estimates the UK cybersecurity workforce at 143,000 professionals, a 5% increase on the prior year. The annual workforce shortfall, defined as the modelled gap between demand and available supply of new entrants, was estimated at 3,800 in the most recent report, down from 3,500 the year before that, and down sharply from 11,100 two years prior. Over the same period, average monthly job postings fell by approximately 33% (DSIT et al., 2025).

This is a striking finding: the UK's own government-commissioned shortfall estimate for the national cybersecurity workforce fell by roughly two-thirds within two reporting cycles, driven primarily by falling job-posting volume rather than a surge in new entrants, even as the overall workforce continued to grow. This complicates any simple narrative of an ever-widening shortage; on the UK's own preferred metric, the shortage has been narrowing, not widening, in the most recent reporting period.

At the same time, a separate estimate, produced by ISC2 using its global workforce-demand model rather than DSIT's UK-specific labour market survey, puts the UK's cybersecurity skills gap at approximately 93,000, roughly twenty-four times larger than DSIT's shortfall figure for the same country in a comparable period (ISC2, 2025; DSIT et al., 2025). Both figures are published by

credible organisations; the discrepancy is attributable entirely to differences in what each model measures, and neither source prominently flags the scale of that discrepancy when the figures are cited.

UK entry-level salary data further complicates the narrative of guaranteed high pay: entry-level analyst salaries typically start between £30,000 and £35,000, a respectable but unremarkable graduate salary in the UK context, with the sector's highest-profile compensation figures (senior architects, CISOs) concentrated among a much smaller population of experienced professionals, disproportionately based in London and the South East (Ipsos & Perspective Economics, 2025).

European Union: structural framing coexists with budget-driven contraction

EU-level data is comparatively fragmented relative to the UK's single authoritative annual series, and figures for the EU's cybersecurity workforce shortfall vary considerably depending on source and methodology, ranging from a commonly cited figure of roughly 300,000 across Europe to jurisdiction-specific estimates such as a projected gap of up to 106,000 in Germany alone. ENISA's own NIS Investments reporting frames the shortage as a structural market condition rather than a cyclical hiring challenge, and documents that a majority of surveyed organisations report continuing difficulty both attracting and retaining cybersecurity talent (ENISA, 2025).

Notably, ENISA's most recent reporting also documents a shift in organisational strategy away from headcount expansion and toward technology-centric and outsourced approaches to cybersecurity resourcing, with median European cybersecurity budgets reported at approximately €1.5 million and a growing share of that budget directed toward tooling and managed services rather than additional personnel (ENISA, 2025). This is consistent with the pattern observed in the US and UK data: organisations continuing to describe talent scarcity as a strategic concern, while

simultaneously reducing their reliance on headcount growth as the primary response to that concern.

Cross-jurisdictional summary

Across all three jurisdictions, the same structural pattern recurs. Headline shortage figures, typically derived from surveys of perceived organisational need, are substantially larger than figures derived from validated job postings or government-commissioned labour market shortfall models, sometimes by an order of magnitude for the same country in the same period. Organisational strain (layoffs, budget cuts, hiring freezes) is well documented in all three jurisdictions and disproportionately affects larger organisations and, by extension, more experienced professionals employed at scale within them. Demand for professionals with several years of specialised experience appears genuinely to outstrip supply in all three markets; demand for entry-level talent, by contrast, shows clearer evidence of saturation, driven by a rapid expansion in the supply of certified and degree-qualified new entrants relative to entry-level opening volume.

Table 1 summarises the scale of divergence between perceived-need and validated-demand figures identified in this paper for each jurisdiction, where comparable figures are available. The magnitude of divergence, up to roughly twenty-four-fold for the UK where the most methodologically transparent comparison is possible, is itself the paper's central empirical finding, independent of which underlying figure any reader considers more credible.

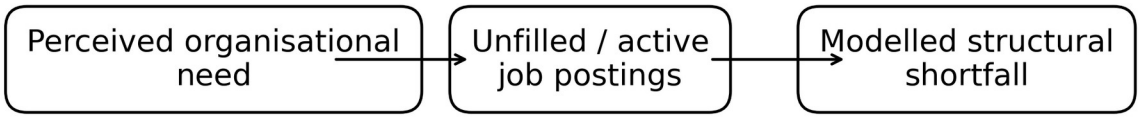
Table 1. Divergence between perceived-need and validated-demand estimates by jurisdiction

Jurisdiction	Perceived-need estimate	Validated/modelled demand estimate	Approximate ratio
United States	4.8 million (global figure;	~514,000 active postings	Not directly

Jurisdiction	Perceived-need estimate	Validated/modelled demand estimate	Approximate ratio
	discontinued by ISC2)	(CyberSeek)	comparable
United Kingdom	~93,000 (ISC2 global model)	3,800 annual shortfall (DSIT labour market survey)	~24:1
European Union	~299,000 (ENISA NIS Investments 2025)	No single EU-wide validated-demand equivalent	Not directly comparable

Figure 1

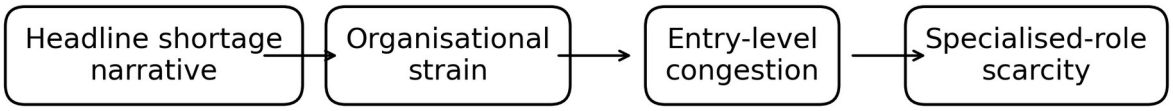
Three Distinct Constructs Commonly Labelled as the Cybersecurity Workforce Gap



Note. The constructs are conceptually distinct and should not be treated as interchangeable measures of labour shortage.

Figure 2

Interpretive Model of the Cybersecurity Employment Paradox



Conceptual synthesis of the comparative interpretation

Note. Conceptual synthesis of the comparative interpretation developed in the manuscript; it is not a statistical model.

The UK case is the clearest illustration available in this dataset because it is the only jurisdiction studied here with two independently produced, contemporaneous estimates for the same country and a broadly comparable period: DSIT's own commissioned labour market survey (DSIT et al., 2025), and ISC2's global workforce-demand model applied to the UK (ISC2, 2025). That these two credible, professionally produced estimates differ by roughly an order of magnitude for the same national workforce is, on its own, sufficient to explain why a job seeker reading UK cybersecurity coverage might reasonably come away with two entirely different impressions of how difficult the market is, depending on which source they encounter first.

Domain-level variation within the "gap"

A further pattern relevant to both this paper and to the companion analysis of under-explored cybersecurity domains is that the reported shortage is not evenly distributed across the discipline's sub-fields. Academic mapping of job postings against curricula, discussed earlier (Ramezan, 2023), identifies governance, risk and compliance (GRC) and specialised research or threat-analysis roles as areas of persistent under-supply relative to demand, in contrast to more heavily subscribed generalist entry points such as SOC analyst roles, where the ratio of qualified

applicants to open positions is markedly less favourable to the applicant. Industry commentary consistent with this pattern identifies cloud security, application security, and AI-security-adjacent roles as commanding premium compensation and facing genuine hiring difficulty, while entry-level "IT/security support technician" and generalist analyst postings attract disproportionately large applicant pools. This domain-level unevenness suggests that the aggregate national or global "gap" figures examined above obscure more than they reveal: a national labour market can simultaneously show saturation in its largest entry point and genuine scarcity in its smaller, more specialised sub-fields, and a single top-line number cannot represent both conditions at once.

The macroeconomic and automation context

The organisational strain documented across all three jurisdictions in The findings above did not occur in a vacuum. The period covered by the most recent editions of the data sources used in this paper coincides with a broader contraction in technology-sector hiring generally, driven by higher interest rates, post-pandemic overhiring correction, and, increasingly, the early effects of AI-assisted productivity tooling on technical headcount planning. ENISA's finding that European organisations are shifting cybersecurity budgets away from personnel and toward technology and managed services is consistent with this broader pattern (ENISA, 2025), and DSIT's own 2025 report notes that just over half of surveyed UK cybersecurity businesses already have staff using AI tools in day-to-day work (Ipsos & Perspective Economics, 2025).

This matters for interpreting the paper's central findings for two reasons. First, it suggests that at least part of the organisational strain documented here (layoffs, hiring freezes, budget cuts) reflects general macroeconomic and technology-sector conditions rather than being specific to cybersecurity, or evidence against the existence of a genuine underlying skills need. A sector can face a genuine long-run shortage of specialised talent while still reducing headcount in a short-run

downturn; the two are not contradictory. Second, and more speculatively, the early productivity effects of AI tooling on routine security operations work (log triage, alert correlation, first-pass vulnerability scanning) may be beginning to compress demand specifically at the entry-level, generalist end of the market, which has historically been the segment most reliant on exactly the kind of repetitive, rules-based tasks that current AI tooling is best suited to partially automate. If this pattern continues, it would reinforce, from an additional and independent direction, this paper's earlier finding on domain-level variation within the gap that the "gap" is concentrated in specialised and judgement-intensive roles rather than in generalist entry points — with the important caveat that the evidence for this specific causal mechanism remains preliminary in the sources reviewed here and warrants dedicated future study rather than confident assertion.

Discussion

Why the abundance narrative persists

The persistence of an undifferentiated "cybersecurity has no unemployment" narrative, despite evidence that would complicate it, is plausibly explained by the incentive structures of the organisations most responsible for producing and repeating the underlying figures. Certification bodies and training providers, including bootcamps and university programmes, have a direct commercial interest in a narrative of guaranteed employability; professional membership organisations have an interest in framing their field as strategically important and under-resourced; and media coverage of technology employment tends to favour large, simple, alarming numbers over methodologically qualified ones. None of this requires bad faith on the part of any individual actor; it is sufficient that the largest, simplest number is also the most reportable one, and that no single actor in the reporting chain has a strong incentive to interrogate its construction.

The ISC2 case study discussed earlier is instructive precisely because it shows this dynamic breaking down under direct, public, credentialed criticism. It took a named practitioner publicly challenging the methodology, rather than years of accumulated entry-level frustration, to produce a change in how the figure was reported.

Implications for training providers

For organisations such as bootcamps and vocational training providers, including those, like Elitechub, positioned around practical, experience-oriented training, this paper's findings suggest a specific strategic implication. Marketing built on undifferentiated shortage figures risks setting expectations that the entry-level segment of the market cannot support, particularly in saturated urban markets. A more defensible and arguably more durable value proposition is one built around addressing the specific, evidenced failure point identified in this paper: the absence of validated practical experience as a barrier to entry, rather than an absence of jobs in the abstract. Training models that generate demonstrable, evaluable work product (a documented detection built, a real vulnerability assessment conducted, a written incident analysis) respond directly to the pattern identified in current market commentary, where employers report being able to differentiate candidates by evidence of applied capability rather than by certification alone.

This paper's domain-level finding above further suggests that training providers face a strategic choice between two distinct models: a high-volume, generalist entry-point model competing in the most congested part of the market, or a narrower, specialisation-oriented model targeting the sub-domains where the underlying data continues to show genuine scarcity. Neither model is inherently superior, but the two require different curricula, different marketing claims, and different measures of graduate success, and conflating them (training generalists while

marketing specialist-level scarcity statistics) risks setting graduates up to compete in the market's most crowded segment while believing they have been prepared for its least crowded one.

Implications for job seekers

For individual job seekers, the practical implication is that persistence at entry level should be calibrated against realistic expectations about a genuinely congested segment of the market, while specialisation, particularly in the domains identified in the academic literature as under-supplied, such as governance, risk and compliance, cloud security, and specialised technical research roles, represents a more evidenced path to differentiation than continued accumulation of general-purpose entry-level certifications alone.

A further implication follows from the United States and United Kingdom findings above that organisational strain (layoffs, hiring freezes, budget cuts) is concentrated among the largest employers. Job seekers, particularly at mid-career level, may find more stable demand among smaller, specialised security firms, managed security service providers, and government or defence-adjacent employers, which this paper's UK and US data both suggest have been comparatively insulated from the cyclical enterprise layoffs affecting large organisations during periods of economic contraction. This is consistent with practitioner commentary noting that experienced professionals displaced from large-enterprise roles are often reabsorbed relatively quickly elsewhere in the market, even though the initial displacement itself contributes materially to public perception that the shortage narrative cannot be true.

Directions for future research

Three extensions of this paper's approach would be particularly valuable. First, a longitudinal tracking study following a defined cohort of newly certified entry-level job seekers

across one or more of the jurisdictions studied here, measuring actual time-to-first-role against the headline shortage figures circulating at the point they began their job search, would provide a direct empirical test of this paper's central claim using primary rather than secondary data. Second, a systematic content analysis of job postings themselves (coding for bundled role requirements, disproportionate experience requirements relative to advertised seniority, and salary transparency) would allow the "dysfunctional hiring practices" account discussed earlier to be tested directly rather than relied upon as plausible commentary. Third, replication of this paper's comparative approach in jurisdictions outside the US, UK, and EU — particularly in African and South-East Asian markets where training providers rely heavily on globally circulated figures without a local equivalent to DSIT's survey, as noted in the introduction, would test whether the pattern identified here is a general feature of how labour market statistics are produced and consumed, or specific to the three markets examined.

Limitations

This paper relies entirely on secondary data and does not independently verify the underlying survey instruments used by ISC2, DSIT, or ENISA. Cross-jurisdictional comparison is complicated by genuine differences in occupational classification, survey sampling frames, and reporting periods; the figures presented here should be read as indicative of a general pattern rather than as precisely commensurable across countries. The EU-level data in particular reflects a more fragmented evidence base than the UK's single authoritative annual series, and future research incorporating a harmonised EU-wide labour market survey, should one become available, would strengthen the comparative claims made about the European Union above.

Conclusion and Recommendations

The apparent contradiction between headline claims of a multi-million-person global cybersecurity shortage and the lived experience of trained professionals struggling to find work is not, this paper argues, evidence that either claim is fabricated. It is evidence that both claims are true of different, poorly distinguished parts of the same labour market, measured by instruments that are frequently conflated in public discourse. Perceived organisational need, validated job postings, and modelled structural shortfall are three different quantities; conflating them produces exactly the confusion this paper set out to examine.

For **job seekers**, the recommendation is to treat entry-level cybersecurity as a genuinely competitive segment requiring differentiated, demonstrable practical experience, while recognising that demand for professionals with several years of specialised experience remains comparatively strong across all three jurisdictions studied.

For **training providers**, the recommendation is to build marketing and curriculum design around the specific, evidenced gap — applied experience and narrow, legible technical proof of capability — rather than around undifferentiated shortage figures that do not survive comparison with government-commissioned labour market data.

For **policymakers**, particularly in jurisdictions without a UK-equivalent annual labour market survey, the recommendation is to invest in methodologically transparent, regularly repeated labour market measurement that distinguishes perceived need from validated demand, on the grounds that the current absence of such a distinction imposes real costs on the individuals who make career and training decisions based on the resulting figures.

More specifically, this paper's findings point toward four concrete steps that would materially improve the quality of public discourse on this topic without requiring new primary data collection:

1. **Disaggregation by experience band.** Future reporting by ISC2, DSIT, ENISA, and comparable bodies would be substantially more useful to job seekers and training providers if headline shortage and demand figures were consistently broken down by required years of experience, rather than reported as a single undifferentiated national or global total. This paper's findings suggest that an entry-level-only figure and an experienced-hire-only figure would tell two genuinely different, and separately actionable, stories.

2. **Consistent labelling of construct type.** Publishers and, more importantly, secondary sources citing these figures should consistently distinguish between perceived-need estimates, validated posting counts, and modelled structural shortfalls, rather than using the terms "gap," "shortage," and "shortfall" interchangeably across three methodologically distinct kinds of figure.

3. **Domain-level reporting.** Given the finding above on domain-level variation that shortage is unevenly distributed across cybersecurity's sub-disciplines, aggregate national figures would benefit from routine domain-level breakdowns of the kind currently produced only sporadically by academic researchers rather than by the major annual industry surveys.

4. **A standing EU-wide labour market survey.** The absence of an EU-wide instrument comparable in rigour and consistency to the UK's DSIT series is a genuine gap in the current evidence base, and this paper's EU findings should be read with that limitation firmly in mind. A harmonised, annually repeated EU survey, ideally coordinated at the ENISA level with consistent national methodology, would substantially strengthen future comparative research of the kind attempted here.

None of these recommendations require resolving the underlying disagreement about whether cybersecurity does, in some absolute sense, face a talent shortage. They require only that the public conversation about that question, and the career and business decisions built on it, rest on figures whose construction is transparent enough to be compared, rather than simply repeated.

Author Positionality and Conflict of Interest Statement

The author is the founder of a cybersecurity training and consulting organisation and, as such, has a professional interest in the market this paper examines. This positionality is disclosed in the interest of full transparency and is noted as a specific reason for the paper's methodological choice to rely exclusively on independently produced, publicly available secondary data (CyberSeek, BLS, ISC2, DSIT, and ENISA) rather than proprietary data from the author's own organisation, and to avoid drawing conclusions more favourable to any specific training model than the underlying data supports. The recommendations for training providers offered earlier are intended as a general implication of the findings, rather than as a description or endorsement of any specific existing programme, including the author's own.

References

CyberSeek. (n.d.). *Cybersecurity supply/demand heat map*. National Institute of Standards and Technology, CompTIA, & Lightcast. Retrieved August 11, 2026, from https://www.cyberseek.org

Department for Science, Innovation and Technology, Ipsos, & Perspective Economics. (2025). *Cyber security skills in the UK labour market 2025: Technical report*. UK Department for Science, Innovation and Technology.

https://assets.publishing.service.gov.uk/media/6893291f303b0dad411d4e50/Cyber_security_skills_in_the_UK_labour_market_2025_-_technical_report.pdf

European Union Agency for Cybersecurity. (2021). *Addressing the cybersecurity skills shortage and gap through higher education*. https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

European Union Agency for Cybersecurity. (2025). *NIS investments report 2025*. https://www.enisa.europa.eu/publications/nis-investments-2025

Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, F., & Thiesse, F. (2022). *Towards understanding the skill gap in cybersecurity*. arXiv. https://arxiv.org/abs/2204.13793

Ipsos & Perspective Economics. (2025). *UK cyber security sectoral analysis 2025*. UK Department for Science, Innovation and Technology. https://assets.publishing.service.gov.uk/media/67cad8b18c1076c796a45c25/Cyber_Security_Sectoral_Analysis_Report_2025.pdf

ISC2. (2024). *2024 ISC2 cybersecurity workforce study*. https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen

ISC2. (2025). *2025 ISC2 cybersecurity workforce study*. https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

Jumaan, S., Kuzminykh, I., Xiao, H., & Ghita, B. (2026). *Understanding the skills gap between higher education and industry in cybersecurity*. Springer.

Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2018). Identifying core concepts of cybersecurity: Results of two Delphi processes. *IEEE Transactions on Education, 61*(1), 11-20. https://doi.org/10.1109/TE.2017.2715174

Ramezan, C. A. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. *Journal of Information Systems Education, 34*(1).

U.S. Bureau of Labor Statistics. (n.d.). Information security analysts. In *Occupational Outlook Handbook*. U.S. Department of Labor. Retrieved August 11, 2026, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Winkler, I. (2024, October). *An open letter to the ISC2 board* [LinkedIn post]. LinkedIn. https://www.linkedin.com/pulse/open-letter-isc2-board-ira-winkler-gvoge