CSBR

The UK Cyber Skills Gap

Building Capability and Resilience

thecsbr.com

The UK's cyber skills challenge matters now because the threat environment has intensified at the same time as organisational resilience remains uneven.

Contents

We would like to thank Kassandra Kae, who worked as an intern for The CSBR for all her work on this report. We would also like to thank everyone who contributed to our discussions on the skills challenge and in particular to RGH Global for supporting our research in this area.

Context

The UK has a stronger base from which to address cyber skills than is sometimes recognized. The challenge now is to turn a growing set of initiatives into a more coherent national capability strategy.

- Cyber capability should be treated as a resilience issue as well as a workforce issue.
- The labour market story is no longer simply one of headline shortage; it is also about pathways, matching and progression.
- The most important capability gaps extend beyond specialist teams into leadership, operations, supply chains and everyday organisational practice.
- The UK already has several valuable building blocks in place, but they need to be joined up more clearly and used more consistently.

This briefing draws on recent official evidence, including the Government Cyber Action Plan, the NCSC Annual Review 2025, the Cyber Security Breaches Survey 2025, the Cyber Security Skills in the UK Labour Market 2025 report, and selected international frameworks and initiatives.

Executive Summary

The UK's cyber skills challenge matters now because the threat environment has intensified at the same time as organisational resilience remains uneven. Official evidence suggests that the country has made progress in growing the cyber workforce, yet the picture is more complex than a simple shortage narrative suggests. The UK has a stronger foundation than before, but capability is still distributed unevenly across organisations, sectors and levels of seniority. The result is that the question is not only how many specialists the UK has, but how well cyber capability is built, shared and sustained across the economy.[1,2,3,4]

The UK is not starting from scratch. The Government Cyber Action Plan, the NCSC's governance work, CyberFirst, apprenticeships, professional standards and Cyber Essentials all provide useful foundations. The next phase should therefore focus on four priorities: defining a clearer national capability framework, strengthening entry and progression routes, making leadership and shared responsibility a core part of cyber policy, and using demand-side levers to raise capability across SMEs and supply chains.[1,5,6,7,8,10,11]

The current cyber skills gap situation

The current position is best understood as a capability challenge developing within a more demanding threat environment. The NCSC's Annual Review 2025 emphasises that cyber security can no longer be treated as an issue for technical teams alone, while the Government Cyber Action Plan makes clear that weak resilience is closely linked to legacy technology, fragmented accountability, inconsistent leadership and uneven skills across the public sector.[1,2]

At labour market level, there are positive signs as well as continuing pressure. The latest official research estimates around 143,000 people in the UK cyber workforce and a narrower workforce gap than in previous years. At the same time, average monthly cyber job postings remained high in 2024, entry-level demand fell to 17%, and almost two-thirds of vacancies were concentrated at mid-level. That points to a more specific challenge around pathways, matching and progression rather than a single undifferentiated shortage.[4]

The structure of the cyber sector itself also deserves attention. In 2024, many UK cyber sector businesses operated with small cyber teams: 23% had one person in a cyber role, 14% had two, 22% had between three and four, and only 4% had more than 30. This suggests that much of the sector is building capability with limited internal scale, which strengthens the case for clearer progression routes, retention support and practical measures that work for smaller firms as well as larger employers.[4]

Percentage of UK cyber sector businesses by the number of people working in cyber roles (2024)

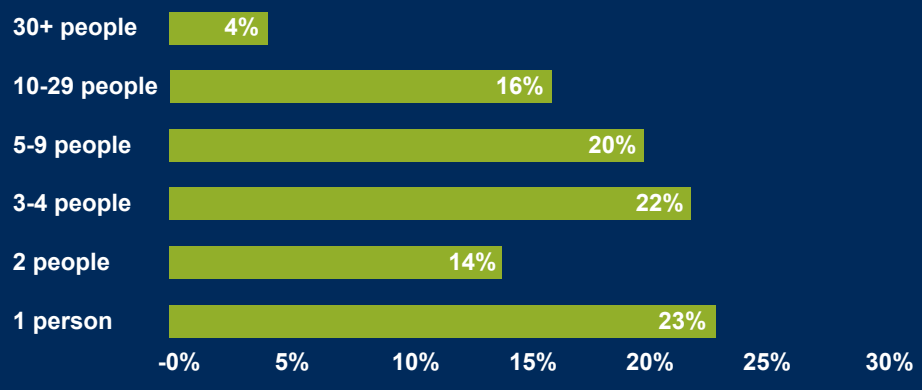


Figure 1

The structure of the UK cyber sector suggests that many businesses operate with small cyber teams, which has implications for progression, retention and organisational capacity.

The challenge also reaches beyond specialist hiring. The Cyber Security Breaches Survey 2025 found that 49% of businesses and 58% of government organisations reported a basic cyber skills gap. This supports a wider point: cyber resilience depends not only on specialist expertise, but also on stronger baseline capability, clearer leadership ownership and a more confident organisational culture.[3]

This has direct implications for how skills investment is measured and targeted. Focusing primarily on the number of specialist hires risks missing the larger capability question. The better question is to ask how well cyber awareness, risk literacy and incident-response readiness are distributed across the workforce, including in non-technical functions such as procurement, legal, finance and operations. Building that kind of horizontal capability requires different levers than building a specialist pipeline: clearer minimum expectations, better embedded training, and accountability structures that make cyber everyone's business.[3]

There are also useful international lessons. Singapore's Skills Framework for Infocomm Technology shows the value of visible career maps and shared language between employers, educators and learners. The U.S. NICE Framework offers a strong model for capability-based role definition, while the EU Cybersecurity Skills Academy demonstrates the value of coordinating training, partnerships and labour-market visibility. The UK does not need to copy these models directly, but it can draw confidence from the fact that clearer pathways and clearer definitions are now central to successful cyber skills policy internationally.[13,24,25]

The structure of the challenge: an hourglass market

Understanding the skills gap requires attention not only to its size but to its shape. The UK cyber labour market exhibits an hourglass structure: strong demand concentrated at the experienced end of the profession, a thin middle layer of progression opportunities, and too few genuine entry routes at the base. This is not simply a pipeline problem. It is a structural problem that reproduces itself: without entry routes, there is no pathway to mid-level; without a mid-level, there is no source of experienced hires; without experienced hires, organisations raise requirements further, deepening the entry barrier.

The labour market data supports this picture. In 2024, 17% of core cyber job postings were at entry level, while almost two thirds required mid-level experience. The estimated workforce gap of approximately 3,800 positions sits against a backdrop of 2,698 average monthly job postings that remain heavily concentrated in the middle of the experience distribution. This helps explain why the market can simultaneously feel tight for employers and inaccessible for graduates: the bottleneck is not the number of people interested in cyber, but the scarcity of roles willing to develop them from the start.[4]

A second structural problem reinforces the first. Trained staff leave: to better-paid private-sector roles, to burnout, or to the same competitor organisations that trained them. This "leaky bucket" dynamic means that investment in training does not necessarily translate into a more experienced workforce over time. It tends instead to recycle the shortage, perpetuating demand for experienced hires that were never given the chance to develop internally. The public sector is particularly exposed to this dynamic, given persistent constraints on pay and career flexibility.

Addressing the gap requires as much attention to retention and progression as to recruitment and initial training

What stands out in practice is the degree of institutional joining-up

The Singapore Cybersecurity Strategy 2021 identifies both a vibrant cybersecurity ecosystem and a robust talent pipeline as enablers. It places workforce growth alongside leadership, infrastructure, ecosystem building and public trust, rather than treating skills as a stand-alone problem to be solved in isolation.[12]

What stands out in practice is the degree of institutional joining-up. Singapore's Skills Framework for Infocomm Technology gives employers, learners and training providers a common language for roles, skills and progression. CSA's SG Cyber Talent initiative then builds dedicated pathways across stages of development, including SG Cyber Youth, SG Cyber Educators and SG Cyber Leaders. In parallel, SG Cyber Associates was launched to provide foundational and targeted cyber training for non-cyber professionals, with 10,000 training spaces for occupations such as auditors, lawyers and engineers. IMDA's TeSA programmes add further mid-career and employer-linked conversion routes, including career conversion, immersion and company-led training options.[13,14,15,16,17,18,19,20,21,22]

A comparative case study: Singapore
Cyber workforce growth: UK and Singapore (index)

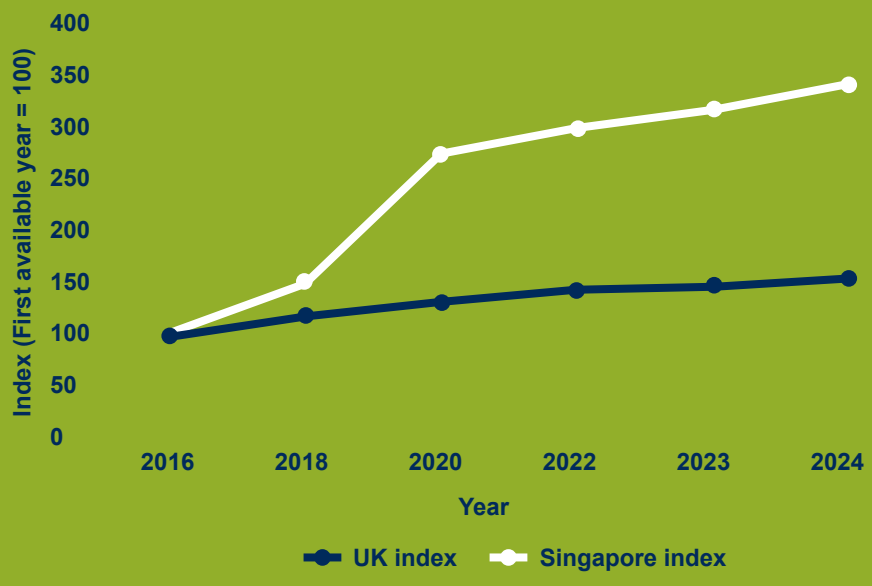


Figure 2

Indexed workforce growth suggests that both the UK and Singapore have expanded cyber capability, although the comparison should be treated as illustrative given differences in scale, institutional context and source data.

The table below offers an analytical comparison of selected Singapore mechanisms and their closest UK comparisons, highlighting where the UK already has comparable provision and where important differences remain.

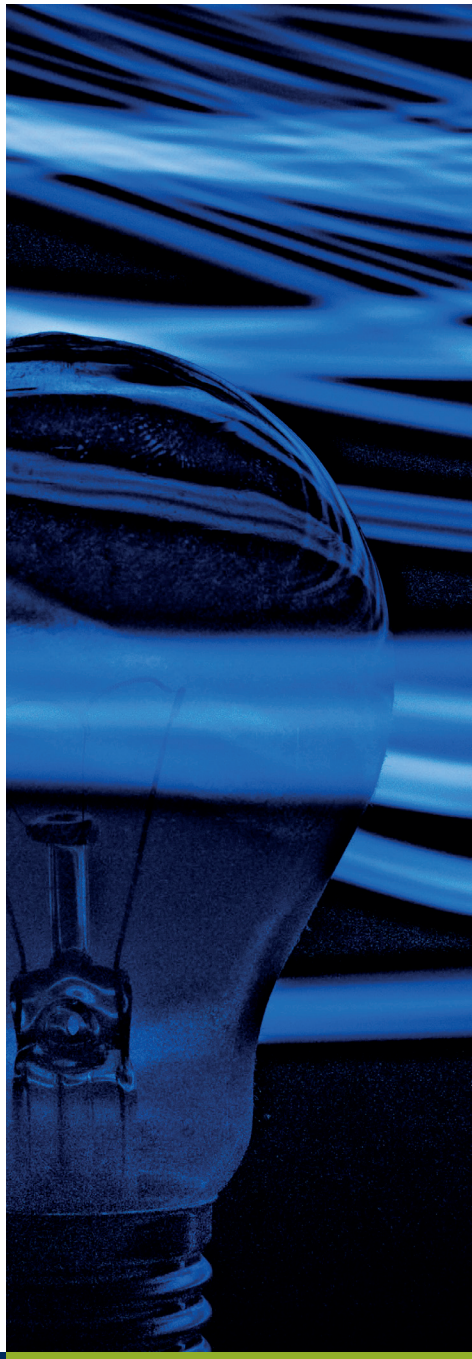
Singapore mechanism	What it does	UK equivalent	Gap for the UK
Skills Framework for ICT (IMDA)	Shared role taxonomy used by employers, educators and learners	Cyber Career Framework (UK Cyber Security Council)	UK framework not yet universally adopted by employers or embedded in procurement
SG Cyber Youth / CyberFirst schools equivalent	Structured school-age pipeline with competitions, bursaries and pathways into higher education	CyberFirst programme (NCSC)	UK activity is strong but less systematically connected to employment entry routes
SG Cyber Associates	Dedicated foundational training for 10,000 non-specialist professionals (auditors, lawyers, engineers)	Cyber Essentials and ad hoc awareness training	No obvious structured national pathway for non-specialist professional upskilling at comparable scale
SG Cyber Leaders	Leadership formation programme for senior executives and board members	NCSC Cyber Governance Code of Practice; Board Toolkit	UK tools are guidance-based; no clearly comparable structured leadership development programme was identified
TeSA career conversion programmes	Employer-linked mid-career conversion routes with government co-funding	Apprenticeships, bootcamps (partial)	UK conversion routes are less employer-integrated and lack consistent co-funding model
OT Cybersecurity Competency Framework	Specialist framework for operational technology security roles	No direct UK equivalent at this level of granularity	This suggests a potential gap as OT risk grows across critical national infrastructure

Taken together, the mapping suggests that the UK's gaps are not primarily about the absence of programmes, but about the absence of systematic connection between them. Singapore's advantage appears to lie in treating each mechanism as part of a more coherent national architecture, where a common skills language, a dedicated talent agency (CSA), and employer-integrated funding work in concert. The UK's equivalent building blocks exist, but they sit in different institutional homes, are funded on different cycles, and are not yet joined into a recognisable national offer.

The lesson for the UK is not that a different institutional system can be transplanted wholesale. It is that clarity, visibility and coordination matter. Singapore has invested in shared role definitions, non-specialist capability building, leadership and alternative entry routes at the same time. It has also supplemented this with more specialised frameworks such as the Operational Technology Cybersecurity Competency Framework. For the UK, the most relevant insight is that a stronger cyber workforce may be built not only by attracting more specialists, but also by making the wider capability system easier to navigate, easier to enter and easier to sustain.

Three specific lessons stand out.

First, the use of a single shared skills language across government, industry and education may help reduce friction in hiring and career progression. **Second,** the deliberate targeting of non-specialist professionals — rather than waiting for cyber-aware recruits to arrive — can accelerate the spread of baseline resilience without competing for the same scarce specialist pool. **Third,** the integration of leadership development into the talent strategy, rather than treating boards as an audience for guidance documents, reflects an approach the UK has not yet fully replicated.



Cyber talent pipeline reach: UK and Singapore

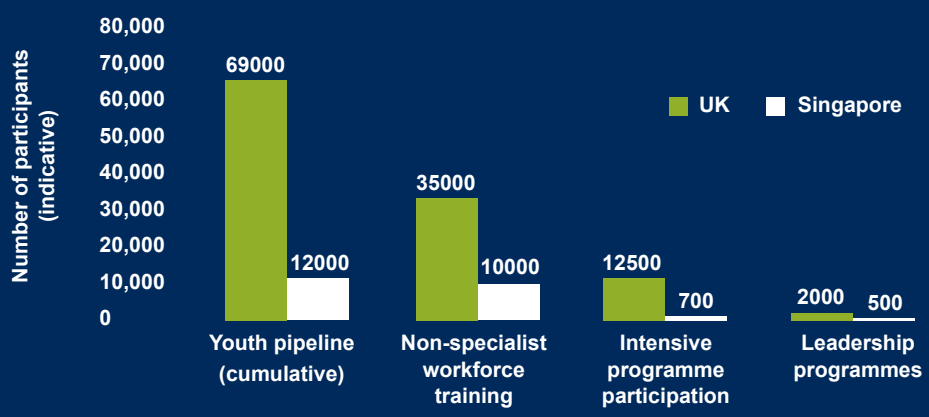


Figure 3

Publicly visible pipeline activity suggests that both the UK and Singapore are investing in cyber talent development, although the comparison should be read with care given the different scale of the two countries.

What the UK is currently doing to address it

The UK already has several important elements of a stronger response. The Government Cyber Action Plan provides a more coherent public-sector framework, centred on clearer accountability, stronger central functions and a more structured Government Cyber Profession. This matters because it begins to treat capability, career development and resilience as connected questions rather than separate policy silos.[1]

Alongside this, the NCSC has expanded practical support for boards and senior leaders. The Cyber Governance Code of Practice and the Cyber Security Toolkit for Boards are valuable steps towards making cyber a mainstream governance issue rather than a narrow technical matter. They help translate cyber risk into language that boards can use, own and act upon.[5,6]

On the talent side, CyberFirst, apprenticeships, professional standards and the Cyber Career Framework all help make the pipeline more visible. Cyber Essentials and related supply-chain guidance also provide a useful way of raising baseline expectations more broadly across smaller organisations. The opportunity now is to connect these initiatives more clearly into a recognisable national offer that supports learners, employers and career changers at each stage.[7,8,10,11]

The regulatory environment and its workforce implications

The Cyber Security and Resilience Bill, announced in the King's Speech and elaborated in a policy statement in April 2025, adds important new context for the skills question. The Bill proposes extending regulatory requirements to managed service providers, expand incident reporting obligations and give the Secretary of State powers to update the regulatory framework without primary legislation. Each of these measures has direct workforce implications.[26,27]

Expanded regulation creates new demand for compliance and assurance skills at the same time as it places additional burdens on organisations that are already stretched. If the regulatory architecture that emerges is fragmented — with different sectoral regulators applying different standards against different audit timelines — scarce cyber talent will be absorbed into compliance work rather than directed towards resilience. The Bill's success therefore depends partly on how well the NCSC Cyber Assessment Framework is used as a common baseline across sectors, reducing duplication and aligning expectations. The EU's experience with NIS 2, and the UK's own partial transposition of the original NIS regulations, offer cautionary lessons about what happens when regulatory coherence is not built in from the start.[26,28]

The Bill also raises questions about ICO capacity, incident data quality and the resourcing of sectoral regulators — all of which depend on people with analytical and technical skills that are in short supply. Legislation without the workforce to implement and interpret it will produce compliance 'contestation' rather than genuine resilience. This reinforces the point that skills policy and regulatory policy cannot be developed in separate silos: the demand that regulation creates must be factored into any credible assessment of what the cyber workforce needs to look like.[26]

Expanded regulation creates new demand for compliance and assurance skills at the same time as it places additional burdens on organisations that are already stretched.

Main themes

Cyber as a whole-of-society issue

A consistent theme is that cyber would be better understood as a whole-of-society resilience issue rather than a narrow IT concern. The consequences of weak cyber practice are not limited to systems failure. They extend to service disruption, organisational confidence and public trust. This points to a policy approach that treats cyber as a horizontal challenge across institutions, sectors and everyday organisational life, not as a specialist silo.

The evidence base for this position is now substantial. The NCSC Annual Review 2025 explicitly states that cyber resilience can no longer be treated as a matter for technical teams alone. The Cyber Security Breaches Survey 2025 shows that 49% of businesses report a basic technical skills gap — a figure that cannot be addressed through specialist hiring alone. The Government Cyber Action Plan, meanwhile, identifies fragmented accountability and inconsistent leadership as core drivers of public-sector vulnerability. These findings point in the same direction: the skills deficit in the UK is as much a cultural and governance problem as it is a labour market problem. Policy that treats it primarily as a recruitment challenge will fall short.[1,2,3]

Defining baseline capability

A central policy question is what should count as a reasonable baseline of cyber capability. The discussion suggests that the UK would benefit from a clearer distinction between minimum competence for the wider workforce and more advanced competence for specialist roles. This matters because a system cannot close a “skills gap” effectively unless it is also clear about the different levels of capability it expects people and organisations to hold.

In practical terms, a tiered model might distinguish between three levels: a minimum cyber awareness standard expected of all employees and organisations regardless of sector; an operational competence level for those working directly with digital systems, data or security tools; and an advanced specialist level for security architecture, penetration testing, incident response and governance leadership. The absence of a clear national statement of these tiers creates compounding problems: employers cannot hire to a standard, training providers cannot align curricula, and learners cannot see where they are on a progression path. Addressing this is the single most important structural reform the UK could make.

Entry routes and the missing middle

The labour market evidence points to a well-recognised but still unresolved pathway challenge. There is strong demand for experienced people, but too few genuine entry routes and too little support for progression into the middle of the profession. This is one reason the market can feel tight even when awareness of cyber careers is growing.

The labour market data is instructive here. In 2024, only 17% of core cyber job postings were at entry level, while almost two thirds were concentrated at mid-level requiring two to six years of experience. The result is a structural mismatch: organisations say they cannot find people, yet graduates report they cannot get started. This “hourglass” shape — too few genuine entry opportunities at the bottom, too much competition for experienced hires in the middle — does not resolve itself through awareness campaigns. It requires deliberate investment in genuine entry-level roles, supervised pathways, and structured progression from early career into mid-career seniority.[4]

Awareness, culture and shared responsibility

The discussion repeatedly returns to the limits of treating cyber as one person's job. Stronger resilience is more likely where responsibility is shared across leadership, management and the wider workforce, with clear expectations built into roles, routines and accountability structures. In practice, this means moving from awareness as a one-off message towards a more embedded culture of everyday cyber responsibility.

Creating shared responsibility in practice requires more than training. It depends on clear role definitions that specify what cyber awareness or action is expected of each function, performance frameworks that include cyber conduct as a dimension of professional behaviour, and leadership that models good practice visibly. The Cyber Governance Code of Practice provides a useful starting point for boards. The next challenge is to extend similar clarity downwards through management structures and into operational teams, so that cyber responsibility does not stop at the boardroom door.[5,6]

The organisational missing middle

The pathway challenge remains one of the clearest themes. There is still a mismatch between repeated concern about shortages and the limited availability of genuine entry-level opportunities. At the same time, there appears to be a thinner middle layer than the system needs, both within the profession itself and between technical teams and senior decision-makers. This helps explain why the labour market can feel constrained even as interest in cyber careers continues to grow.

The missing middle is also visible in organisational terms. Many organisations — particularly in the public sector and among SMEs — may lack a layer of technically informed middle management capable of translating cyber risk between specialist teams and executive decision-makers. This creates two problems simultaneously: specialist staff operating without effective escalation routes, and boards receiving advice that is either too technical or too thin to act on. Strengthening the middle of the profession, both through progression support and through management-level cyber literacy programmes, is therefore likely to be as important as expanding the entry pipeline.

Retention, progression and the public sector

Retention deserves more attention alongside recruitment. Where organisations train staff only to lose them quickly to better-paid employers, shortages are recycled rather than resolved. This appears especially significant for the public sector, where pay, progression and recruitment flexibility remain part of the wider resilience picture. A stronger capability strategy would therefore place greater weight on progression, development and long-term retention as well as pipeline expansion.

Broadening the idea of cyber work

Another strong theme is that cyber is often still understood too narrowly. The discussion points instead to a broader conception of cyber work that includes governance, risk, crisis leadership, operational technology, business continuity, supply chains and behavioural insight alongside highly technical roles. This wider definition is useful because it reflects more accurately how resilience is built in practice and opens the door to a wider range of skills and career pathways.

This broader conception has direct implications for how vacancies are written and how candidates are assessed. An employer who defines a "cyber role" as requiring primarily technical or coding skills will systematically miss candidates with strong analytical, communication or governance backgrounds who could contribute significantly to risk management, business continuity or board-level cyber leadership. Widening role definitions in job specifications, rewriting person specifications to reflect the actual work rather than assumed technical prerequisites, and building assessment processes that value diverse experience could together expand the effective talent pool without requiring any new training infrastructure.

Stronger resilience is more likely where responsibility is shared across leadership, management and the wider workforce, with clear expectations built into roles, routines and accountability structures.

Supply chains and practical demand signals.

One of the clearest practical levers identified is the role of supply chains in driving adoption. Many organisations, particularly SMEs, respond most readily when cyber expectations are tied to contracts, procurement requirements and customer pressure rather than advice alone. This suggests that baseline schemes can become more effective when they operate as part of a wider demand signal, helping to create both stronger market incentives and clearer employment pathways.[10,11]

The Cyber Essentials scheme already demonstrates this dynamic. When tied to government procurement requirements through Procurement Policy Note 014, it creates a demand signal that many SMEs respond to precisely because the cost of non-compliance has become concrete. Extending this logic further — into private-sector supply chain requirements, insurance conditions, and sector-specific regulatory thresholds — would widen the effective reach of baseline cyber standards without requiring SMEs to engage with government guidance on its own terms. The policy lever is commercial rather than advisory, and the evidence suggests it is significantly more effective.[10,11]

SMEs, usability and real-world adoption

A recurring point is that smaller organisations often face a problem of usability as much as one of awareness. Time constraints, limited internal capacity and mobile-first working habits all affect whether guidance is acted on. This suggests that the format, presentation and delivery of support matter alongside the content itself. A more effective SME strategy would therefore focus not only on what guidance says, but on whether it is practical to absorb and use.

This has implications for the format and delivery model of cyber support, not only its content. Evidence from digital adoption programmes in other policy areas suggests that guidance delivered through trusted intermediaries — trade associations, accountants, local enterprise partnerships — can reach small businesses more reliably than direct government communication. The Cyber Resilience Centre model, which connects regional policing, universities and local business communities, offers one practical illustration of how this joined-up delivery can work. Scaling models of this kind, rather than investing primarily in new digital guidance platforms, may have a stronger effect on actual SME behaviour.[29]

Board literacy and the translation challenge

The discussion also highlights a persistent gap between cyber language and board-level decision-making. Where cyber risk is presented in technical terms alone, boards may struggle to engage with it confidently. The implication is that stronger resilience depends partly on translation: turning cyber into language that connects with finance, operations, assurance and strategic risk. This is less about simplifying the issue than about making it governable.

The tools for this translation already exist in part. The NCSC's Cyber Security Toolkit for Boards frames cyber risk in terms of financial exposure, operational disruption and reputational consequence — language that connects directly with standard board responsibilities. The challenge is that uptake of this kind of resource remains uneven. Regulators and professional bodies have a role to play in normalising board-level cyber literacy as a governance expectation, in the same way that financial literacy and health-and-safety awareness have become standard board competencies over time.6

Alternative talent pools

The workforce discussion points to valuable opportunities beyond conventional recruitment routes. Neurodivergent candidates, mid-career entrants and people from adjacent analytical professions may all represent important sources of capability if pathways are more accessible and employers recruit more flexibly. The broader point is that workforce expansion does not depend only on producing more traditional entrants. It also depends on widening the routes through which existing talent can contribute.

Some of the most promising underexplored routes include professionals from adjacent analytical disciplines such as data science, intelligence analysis, financial crime and fraud investigation, who often possess risk-reasoning and adversarial-thinking skills that translate well into cyber security roles. Mid-career professionals in law, audit, project management and operations represent a further pool, particularly for roles in governance, risk management and business continuity. Neurodivergent candidates, who are disproportionately represented in technically strong problem-solving roles, also benefit from more accessible recruitment and onboarding practices that remove unnecessary credentials barriers.

UK cyber capability and diversity indicators (%)

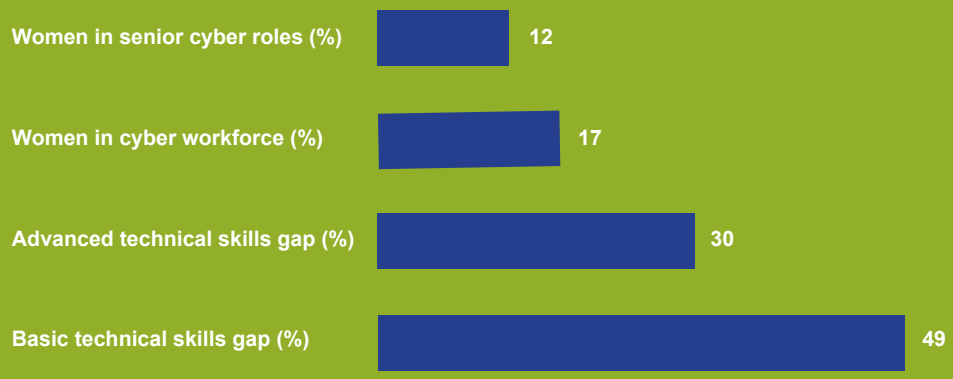


Figure 4

Selected UK cyber capability indicators suggest that skills pressures and representation challenges remain unevenly distributed across the workforce and leadership pipeline.

Education, teacher capacity and labour market alignment

There is also a strong concern that parts of the education system are not yet keeping pace with employer needs. Curriculum relevance matters, but so too does teacher capacity, especially where pay and recruitment pressures make it difficult to sustain high-quality computing and cyber education. This suggests that stronger links between education and practice, including more regular exposure to industry, could help improve readiness for work over time.

Teacher capacity is the most acute constraint in this area. Computing and cyber education requires educators who are both pedagogically skilled and technically current — a combination that is difficult to recruit and retain at state school pay rates when industry demand for the same skills is high. Short-term industry placements for teachers, subsidised by government or sector bodies, could help maintain currency without requiring permanent salary competition. In parallel, stronger links between schools and local Cyber Resilience Centres or university departments could expose students to applied cyber work earlier, creating more realistic entry pathways than a curriculum alone can provide.

AI as an enabler and pressure point

AI is presented as both an opportunity and a pressure point for cyber capability. It can support training, analysis and productivity, but it can also widen the attack surface, lower barriers for attackers and encourage overreliance if used poorly. This means the AI question is not only technical. It is also educational and organisational, requiring stronger judgement, clearer adoption practices and more deliberate capability planning.

One specific risk deserves particular attention. If AI tools automate a growing share of the tasks currently performed by junior analysts — log analysis, alert triage, initial reporting — the demand for entry-level cyber roles may fall further, compounding an already thin bottom of the pipeline. This possibility is not hypothetical: employer demand for AI-related skills in cyber roles rose sharply in 2024. Policy that treats AI as purely an enabler for cyber upskilling, without also assessing how it reshapes what is being hired for, risks planning for a workforce structure that is already changing.[4]

Standardisation, assurance and reduced duplication

The discussion suggests that fragmentation across standards, regulators and audit processes can absorb scarce time and talent that might otherwise be directed towards practical resilience work. A more aligned assurance environment could therefore support capability by reducing duplication and making expectations easier to navigate. This points to the value of greater coherence, common evidence standards and more proportionate oversight.

The Cyber Security and Resilience Bill provides an opportunity to address this directly. If incident reporting, regulatory standards and audit requirements are designed with coherence in mind — drawing on the NCSC's Cyber Assessment Framework as a common baseline rather than allowing sector-specific frameworks to proliferate independently — the compliance burden on organisations with scarce cyber teams could be reduced. The financial services sector, which operates under some of the most demanding cyber expectations, offers a model of how proportionate but rigorous requirements can drive consistent practice without creating paralysing audit overhead.[26,28]

Incentives, enforcement and public communication

A further theme is that stronger cyber outcomes are likely to depend on a mix of incentives, minimum expectations and better public communication. Regulation alone may not keep pace with threats, but neither can the system rely on awareness alone. This discussion points to the importance of clearer public messaging, better role models and broader social understanding of cyber as part of everyday safety and resilience, including for parents, schools and communities.

There is a specific gap in public communication around cyber careers. Survey evidence consistently shows that awareness of cyber as a career option remains lower than awareness of it as a threat. Parents, school advisers and careers counsellors play a disproportionate role in shaping young people's occupational choices, yet they are rarely the direct target of pipeline-development investment. Campaigns that build the social legitimacy and perceived accessibility of cyber careers — particularly among groups currently underrepresented in the sector — could have a longer-term impact on diversity and pipeline breadth that specialist recruitment schemes alone cannot achieve.[4]

Partnerships and collaborative delivery

A final theme is that capability is more likely to grow where institutions work together rather than in isolation. Collaborative models involving policing, universities, enterprise networks and SMEs appear especially promising because they connect prevention, skills development and local economic support. This reinforces a broader point running through the discussion: cyber capability is built most effectively when it is treated as a shared endeavour across public, private and civic actors.

The regional dimension of this is under appreciated. Cyber resilience and cyber skills capacity vary across the UK, with London and the South East accounting for a disproportionate share of sector employment and specialist infrastructure. Regional partnerships that connect local universities, policing, local enterprise networks, employers could help distribute capability more evenly — both by developing local talent and by making cyber careers and cyber support more accessible to organisations outside the major urban centres. The Cyber Resilience Centre model, where it is well-resourced, already demonstrates the potential of this approach.[4,29]

Policy Recommendations

The government ought now to build on existing momentum with a smaller number of focused interventions which strengthen capability, improve coherence and support implementation across the economy.

1. Publish a national cyber capability framework

The UK would benefit from a clearer national framework which distinguishes between baseline capability for all staff and leaders, practitioner capability for operational roles, and advanced specialist capability for higher-risk functions. This would support a more consistent language across education, recruitment, workforce planning and professional development.

> Align public-sector role design, training pathways and professional standards around a shared framework.

> Use that framework to make careers, transitions and progression routes more visible to employers, educators and learners.

> Draw selectively on the role-mapping approach used in the NICE Framework and Singapore's Skills Framework for ICT.[13,24]

2. Strengthen pathways into work and progression in work

The next phase of policy should focus more directly on transition points: from school into further study, from education into employment, and from adjacent professions into cyber roles. This is also where public-sector capability can be strengthened most, by using government's own hiring, training and procurement levers to create more real entry routes and better progression opportunities.

> Expand high-quality placements, apprenticeships, conversion routes and early-career hiring tied to genuine operational roles.

> Support progression at mid-level through modular training, mentoring and clearer career ladders.

> Treat retention and progression data as part of resilience planning, especially across government and critical sectors.[1]

The public sector presents the most acute version of this problem. The Cyber Security Breaches Survey 2025 found that 58% of government organisations reported a basic cyber skills gap, while the Government Cyber Action Plan identifies pay, career development and recruitment flexibility as structural constraints. Training staff only to lose them to better-resourced private-sector employers is, as the evidence suggests, recycling the problem rather than resolving it. A credible public sector cyber strategy must therefore include realistic career ladders, pay structures that can compete at least partially with private markets, and succession planning that treats cyber capability as a long-term institutional asset rather than a short-term resourcing question.[1,3]

3. Make leadership and shared responsibility a core part of cyber policy

The UK has already begun this shift through the Cyber Governance Code of Practice and board-facing NCSC guidance. The next step is to embed those expectations more systematically so that cyber literacy becomes part of mainstream governance, management and organisational practice.

> Promote wider uptake of the Cyber Governance Code of Practice through regulators, public bodies and sector leadership groups.[5]

> Support board-level and executive-level training that helps leaders understand cyber risk in operational and financial terms.

> Pair specialist skills investment with a stronger baseline expectation of cyber awareness across the wider workforce.

4. Use demand-side levers to raise capability across SMEs and supply chains

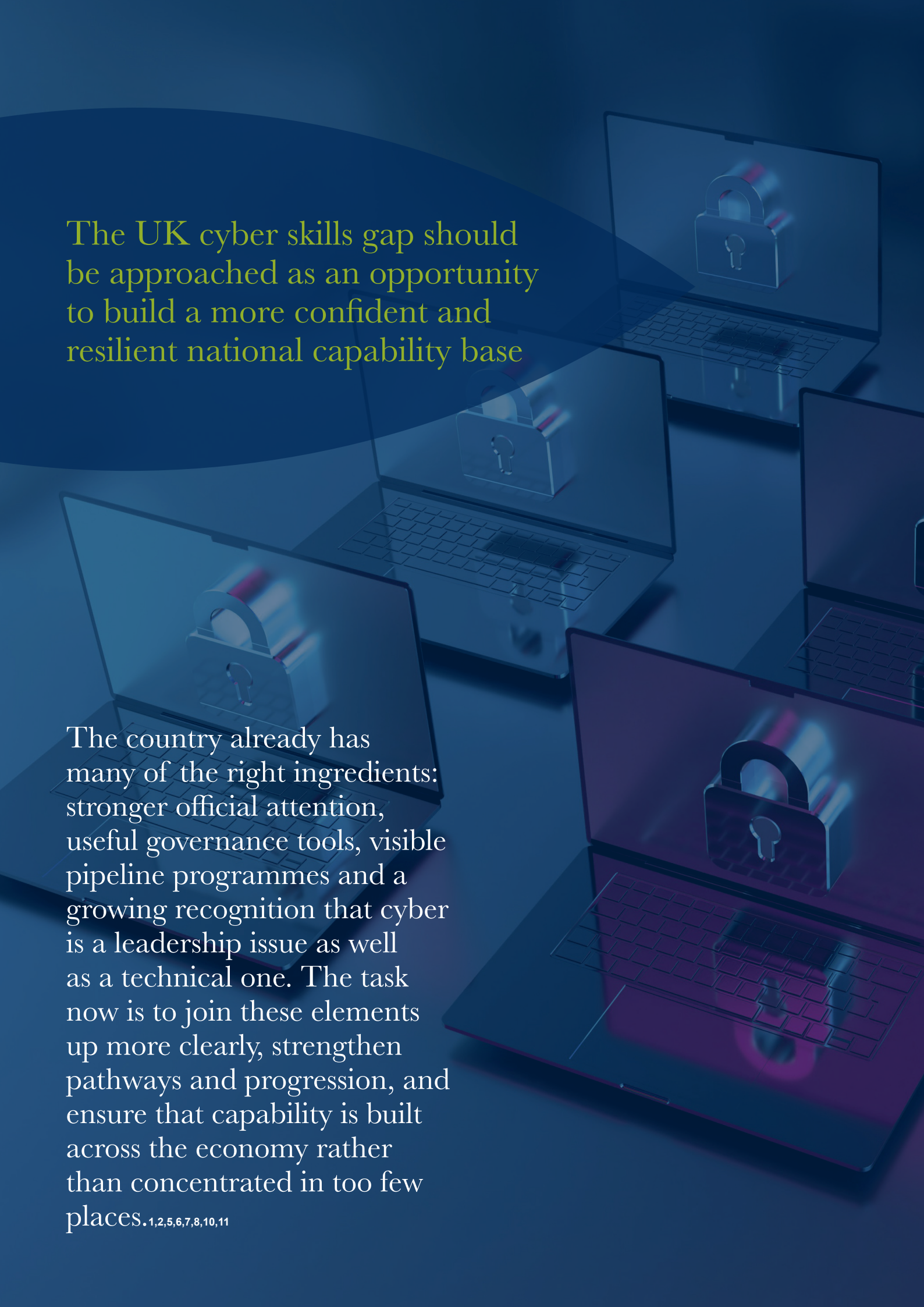
For many smaller organisations, the most effective incentives are practical rather than rhetorical. Policy should therefore make greater use of procurement, customer standards and light-touch support to strengthen baseline cyber capability where it is most needed.

> Expand the use of Cyber Essentials and related baseline requirements in public procurement and encourage wider adoption across supply chains.[10,11]

> Link standards with trusted guidance and regional support so that compliance becomes a route into resilience rather than a stand-alone exercise.

> Use local partnerships, sector networks and Cyber Resilience Centre models to help SMEs access advice, training and talent.[29]

The UK cyber skills gap should be approached as an opportunity to build a more confident and resilient national capability base



The country already has many of the right ingredients: stronger official attention, useful governance tools, visible pipeline programmes and a growing recognition that cyber is a leadership issue as well as a technical one. The task now is to join these elements up more clearly, strengthen pathways and progression, and ensure that capability is built across the economy rather than concentrated in too few places.[1,2,5,6,7,8,10,11]

References

1 Department for Science, Innovation and Technology. Government Cyber Action Plan. 2026. https://assets.publishing.service.gov.uk/media/695cfb1534c664251c38a0f9/E03515734_-_Government_Cyber_Action_Plan_ACCESSIBLE.pdf

2 National Cyber Security Centre. NCSC Annual Review 2025: It's time to act. 2025. https://www.ncsc.gov.uk/files/ncsc-annual-review-2025.pdf

3 Department for Science, Innovation and Technology. Cyber Security Breaches Survey 2025. 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

4 Department for Science, Innovation and Technology; Ipsos; Perspective Economics. Cyber Security Skills in the UK Labour Market 2025. 2026. https://assets.publishing.service.gov.uk/media/68be9b4c11b4ded2da19ff1b/Cyber_security_skills_in_the_UK_labour_market_2025-_findings_report.pdf

5 Department for Science, Innovation and Technology. Cyber Governance Code of Practice. 2025. https://www.gov.uk/government/publications/cyber-governance-code-of-practice

6 National Cyber Security Centre. Cyber Security Toolkit for Boards. 2025 update. https://www.ncsc.gov.uk/collection/board-toolkit

7 National Cyber Security Centre. CyberFirst. 2026. https://www.ncsc.gov.uk/section/advice-guidance/all-topics/cyberfirst

8 UK Cyber Security Council. Cyber Career Framework. 2026. https://www.ukcybersecuritycouncil.org.uk/for-individuals/about-the-cyber-security-sector/cyber-career-framework

9 UK Government Security. Government Cyber Security Academy. 2026. https://www.security.gov.uk/careers-and-learning/careers/government-cyber-security-academy/

10 National Cyber Security Centre. Cyber Essentials. Updated 2026. https://www.ncsc.gov.uk/cyberessentials/overview

11 Cabinet Office. Procurement Policy Note 014: Cyber Essentials scheme. 2025. https://www.gov.uk/government/publications/ppn-014-cyber-essentials-scheme

12 Cyber Security Agency of Singapore. Singapore Cybersecurity Strategy 2021. https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021/

13 Infocomm Media Development Authority. Skills Framework for Infocomm Technology. https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa/skills-framework-for-infocomm-technology-sfw-for-ict

14 Cyber Security Agency of Singapore. SG Cyber Talent. 2026. https://www.csa.gov.sg/our-programmes/talent-and-skills-development/sg-cyber-talent/

15 Cyber Security Agency of Singapore. SG Cyber Associates. https://www.csa.gov.sg/our-programmes/talent-and-skills-development/sg-cyber-talent/sg-cyber-associates/

16 Cyber Security Agency of Singapore. New Cyber Talent Programme to Provide Foundational and Targeted Cybersecurity Training for Non-Cybersecurity Professionals. 2023. https://www.csa.gov.sg/news-events/press-releases/new-cyber-talent-programme-to-provide-foundational-and-targeted-cybersecurity-training-for-non-cybersecurity-professionals/

17 Infocomm Media Development Authority. TechSkills Accelerator (TeSA). https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa

18 Infocomm Media Development Authority. Career Conversion Programmes. Updated 2024. https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa/career-conversion-programmes

19 Infocomm Media Development Authority. Tech Immersion and Placement Programme. https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa/tech-immersion-and-placement-programme-tipp

20 Infocomm Media Development Authority. Company-Led Training Programme. https://www.imda.gov.sg/how-we-can-help/techskills-accelerator-tesa/company-led-training-programme-clt

21 Cyber Security Agency of Singapore. SG Cyber Educators. https://www.csa.gov.sg/our-programmes/talent-and-skills-development/sg-cyber-talent/sg-cyber-educators/

22 Cyber Security Agency of Singapore. SG Cyber Leaders. https://www.csa.gov.sg/our-programmes/talent-and-skills-development/sg-cyber-talent/sg-cyber-leaders/

23 Cyber Security Agency of Singapore. Operational Technology Cybersecurity Competency Framework. 2021. https://www.csa.gov.sg/resources/publications/operational-technology-cybersecurity-competency-framework--otccf-/

24 National Institute of Standards and Technology. NICE Framework Resource Center. 2026. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

25 European Commission. Communication on the Cybersecurity Skills Academy. 2023. https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy

26 Department for Science, Innovation and Technology. Cyber Security and Resilience Bill: policy statement. 2025. https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement

27 Prime Minister's Office, 10 Downing Street. The King's Speech 2024 background briefing notes. 2024. https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pdf

28 European Parliament and the Council of the European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

29 Department for Science, Innovation and Technology. Cyber resilience. Updated 2024. https://www.gov.uk/government/collections/cyber-resilience

Workforce Optimisation

powered by