FMBusinessDaily

# Report: UK's Cyber Security & Resilience Bill May Not Meet its Goals Unless Skills Gaps Are Addressed

3 hours ago


The UK's Cyber Security & Resilience Bill may fail to achieve its goals unless the Government fundamentally shifts how it addresses the country's cyber skills crisis, an authoritative new report warns.

Published this week by The CSBR, the report – The UK Cyber Skills Gap: Building Capability and Resilience – reveals that, while the UK has built a solid foundation of cyber initiatives, an unstable "hourglass" labour market structure combined with expanding regulatory burdens threaten to undermine genuine digital resilience across critical national infrastructure.

Following royal assent, the Cyber Security & Resilience Bill is expected to expand regulatory powers to managed service providers and introduce strict 24-hour incident reporting.

But the report highlights that this will trigger an unprecedented surge in demand for compliance and assurance skills, inadvertently creating the new risk of the UK trapping scarce technical talent in a cycle of bureaucratic box-ticking.

Drawing on official evidence including the Government Cyber Action Plan, the NCSC Annual Review 2025, the Cyber Security Breaches Survey 2025 and the Cyber Security

Skills in the UK Labour Market 2025 report, the report identifies:

- 49% of UK businesses and 58% of government organisations already suffering from a basic cyber skills gap. Without systemic reform, critical personnel will be diverted into compliance management rather than

practical threat defence, resulting in legal contestation instead of security.

- a structural crisis in the UK cyber workforce, which resembles an hourglass: high demand for experienced mid-to-senior level practitioners, but a severe bottleneck at the bottom. In 2024, 65% of core cyber job postings required mid-level experience, whereas entry-level opportunities fell to just 17%.

- a 'leaky bucket' dynamic, in which trained public sector staff continuously exit to better-paid private sector roles due to rigid pay constraints, recycling the shortage rather than solving it.

James Morris, founder of The CSBR, observed: "No-one wants a scenario in which the Cyber Security & Resilience Bill becomes a paper tiger. Unless policy makers systematically connect our fragmented training programs and create viable entry routes for new talent, regulations will overwhelm the very sectors they are meant to protect. We could easily end up with compliance 'contestation' instead of genuine resilience."

The CSBR's report calls on UK policy makers to urgently execute four targeted interventions:

- 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. Consider drawing on leading international examples such as Singapore's Skills Framework.

- Strengthen pathways into work and progression in work: 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.

- Make leadership and shared responsibility a core part of cyber policy: While this shift has begun through the Cyber Governance Code of Practice and Board-facing NCSC guidance, the next step should be to embed those expectations more systematically so that cyber literacy becomes part of mainstream governance, management and organisational practice.

- 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.

"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." concluded The CSBR's Morris.

Production of the CSBR's report was sponsored by global recruitment and workforce optimisation company RGH Global. Justin Madgwick, Global CEO from RGH, commented: "The CSBR report rightly highlights that the UK's cyber challenge is not simply a shortage of people; it's a shortage of visibility into capability, potential and workforce readiness. Organisations often know who holds cyber qualifications, but they have far less insight into the behavioural, cognitive and transferable skills that determine whether someone can succeed, adapt and progress in increasingly complex cyber environments.

“Through our recruitment and workforce optimisation platform, powered by Epitome, we see significant opportunities to widen talent pools, identify hidden capability and create more effective pathways into cyber careers. Closing the skills gap is not just about attracting more people into the profession; it’s about understanding the capability that already exists within organisations and developing it more intelligently.

“The recommendations outlined by The CSBR provide an important framework for doing exactly that, and we welcome the focus on building sustainable capability rather than simply increasing compliance.”

The full report is available for immediate download from The CSBR’s official website, thecsbr.com.