Cybersecurity Business Network (CBN) – Autumn Budget 2026 representation

Introduction

The Cybersecurity Business Network (CBN) is a coalition of over 80 cybersecurity organisations and provides a vehicle for industry to collaborate and inform the development of UK cyber policy[1], with the shared aim of a more secure, resilient and prosperous economy and society. CBN acts as the secretariat to the All-Party Parliamentary Group (APPG) on Cyber Innovation, chaired by Dan Aldridge MP, with an active group of officers & members drawn from across Parliament[2]. Through the APPG and our own policy work, we connect Parliamentarians, officials and industry so that cyber security policy keeps pace with a fast-changing threat and a fast-growing UK sector.

CBN welcomes the opportunity to make this representation ahead of the Autumn Budget on 28 October 2026. Our membership spans certification and assurance bodies, managed security and DDoS protection providers, threat-intelligence specialists, cyber law firms, and OT security and data-protection vendors, among others. Collectively, our members protect organisations of every size and sector – from FTSE-listed companies and critical national infrastructure operators to the SMEs, charities and public bodies that make up most of the UK economy – and the millions of consumers who rely on those organisations to keep their data safe.

The threat landscape those organisations face is intensifying. The NCSC addressed 429 cyber incidents in the year to August 2025, of which 204 (48%) were nationally significant – more than double the 89 the year before – and 18 highly significant, up around 50% for the third year running[3]. Government has responded with a growing policy focus: a Cyber Security and Resilience Bill to widen statutory duties, a Cyber Growth Action Plan, the forthcoming National Cyber Action Plan to grow the sector, and an Industrial Strategy naming cyber security a priority growth area. CBN supports this direction; our ask is that the Treasury backs it with the fiscal tools – on tax, funding, awareness, skills and procurement – needed to turn ambition into adoption, resilience and growth across the nation. As AI lowers the barriers to hostile actors and enhances threats to significant economic impact, there has never been a more pressing time to invest in strengthening cyber security across the economy.

Key asks

[1] About CBN, Cybersecurity Business Network

[2] Register of All-Party Parliamentary Groups: Cyber Innovation, UK Parliament

[3] NCSC Annual Review 2025, Chapter 01: Incident management, National Cyber Security Centre

In this document we will outline the current state of UK cyber security, business vulnerability, the economic opportunity from stimulating growth, the barriers to strengthening resilience, all of which culminate in these specific asks:

1. Tax relief to lower the cost of purchasing cyber security from UK providers
2. Funding for cyber awareness, skills and training
3. Reduce the bureaucracy and cost of procurement for UK cyber security companies
4. Support for organisations newly in scope of the Cyber Security and Resilience Bill
5. Support cyber security growth in the regions
6. Strengthen the environment for UK cyber exports and scale-ups

---

Overview

The threat landscape is changing, and the stakes are rising

The NCSC's 2025 Annual Review describes ransomware as "one of the most acute and pervasive cyber threats to UK organisations" and warns that the gap between the threat to critical infrastructure and the UK's collective defensive capability is widening[4]. State and state-aligned actors from China, Russia, Iran and North Korea are increasingly active against UK targets, and criminal ransomware groups continue to exploit unpatched, legacy systems.

The impact on UK business and society is real – and growing

This is no longer a theoretical risk. The Cyber Monitoring Centre – the UK's independent assessor of systemic cyber events – rates the autumn 2025 ransomware attack on Jaguar Land Rover as "the most economically damaging cyber event to hit the UK": a five-week production halt and a modelled £1.9 billion economic cost, cascading through more than 5,000 organisations, including nearly 1,000 tier-one suppliers[5]. Government had to step in with a £1.5 billion loan guarantee to keep hundreds of exposed suppliers afloat[6]. The fallout still hasn't stopped, as recently as 7th September 2026, JLR has announced over 4000 job cuts to its UK based workforce from a culmination of factors, including the attack.

---

[4] It's time to act – NCSC Annual Review 2025, National Cyber Security Centre
[5] Cyber Monitoring Centre statement on the Jaguar Land Rover cyber incident (October 2025)
[6] Government backs £1.5bn loan guarantee for suppliers as JLR recovers from cyber attack, AM-Online

Marks & Spencer's own attack is expected to cost around £300 million[7], and the Co-op's cost an estimated £206 million[8] and exposed the data of all 6.5 million of its members[9]. More broadly, the government's Cyber Security Breaches Survey 2025/2026 estimates that 43% of businesses and 28% of charities – around 612,000 businesses and 57,000 charities – experienced a breach or attack in the past 12 months[10].

AI is set to intensify this threat on three fronts. It is already lowering the cost and skill needed to mount a sophisticated attack: Anthropic's November 2025 disclosure of a Chinese state-sponsored espionage campaign found AI systems executing 80–90% of the operation with minimal human input, and concluded that "the barriers to performing sophisticated cyberattacks have dropped substantially - and we predict that they'll continue to do so."[11] It is accelerating the exploitation of legacy, unpatched systems: the NCSC has warned of an AI-driven "vulnerability patch wave,"[12] with AI now able to exploit accumulated technical debt "at scale and at pace across the technology ecosystem." And the frontier models driving this progress are becoming harder to fully constrain: independent safety evaluations of leading models have found them attempting to disable their own oversight mechanisms and copy themselves onto other servers to avoid being replaced, when tested under adversarial conditions.[13] Together, these trends point to a threat growing faster than most UK businesses' capacity to defend against it, and posing a serious risk to economic disruption.

Adoption and resilience are not keeping pace

Government and industry broadly agree on what good looks like; the challenge is adoption. CBN identifies eight connected barriers the Budget can help address:

SME take-up: only 5% of UK businesses hold Cyber Essentials certification (up from 3%), and just 14% of micro-businesses are even aware the scheme exists[14]. Only 52% of smaller businesses undertake any cyber risk identification, against 91% of large businesses[15] – and SMEs make up the overwhelming majority of the supply chains larger organisations depend on.

Cyber skills and awareness: the annual UK cyber workforce gap has narrowed to around 3,800 roles, but 49% of businesses lack the confidence for basic tasks such as firewall configuration, and 30% lack advanced skills such as forensic analysis[16].

---

[7] Marks & Spencer says cyber attack to cost business £300 million, Bloomberg (21 May 2025)
[8] Co-op declares cyber attack damage cost it £206m, Computer Weekly
[9] Data of all 6.5 million Co-op members stolen – CEO says she is 'incredibly sorry', TechRadar Pro
[10] Cyber Security Breaches Survey 2025/2026, Department for Science, Innovation and Technology (GOV.UK)
[11] Disrupting the first reported AI-orchestrated cyber espionage campaign, Anthropic
[12] Preparing for a 'vulnerability patch wave', NCSC
[13] Frontier Models are Capable of In-Context Scheming, Apollo Research
[14] DSIT, Cyber Security Breaches Survey 2025/2026 (GOV.UK)
[15] DSIT, Cyber Security Breaches Survey 2025/2026 (GOV.UK)
[16] Cyber Security Skills in the UK Labour Market 2025, DSIT (technical report)

Only 19% ran any staff cyber training in the past year[17], and women make up only 17% of the cyber workforce[18].

Senior-level awareness and responsibility: only 31% of businesses and 30% of charities have a board member with explicit responsibility for cyber security, rising to 68% among large businesses but just 29% among micro-businesses[19]. As the NCSC puts it: "For too long, cyber security has been regarded as an issue predominantly for technical staff. This must change."[20]

Funding and resources for cyber security adoption: self-reported breach costs are typically modest, masking the tail risk JLR, M&S and Co-op made visible. When resilience funding is not there upfront, the bill often lands on the taxpayer, as the £1.5 billion JLR supplier loan guarantee showed[21]. Proactive investment is far cheaper than reactive bailouts, but many businesses, especially SMEs, lack the resources to invest before a breach forces their hand.

Funding for innovative UK cyber scale-ups and sector growth: investment into UK cyber scale-ups fell 11% in 2025, to £184 million across 47 deals, from £206 million across 59 deals the year before[22], making it harder for the innovative firms best placed to help the rest of the economy adopt new protection to scale, invest and stay UK-based.

Procurement systems: the APPG on Cyber Innovation's own SME roundtable found that cyber responsibility is too often assigned informally to "the most tech-savvy person" rather than built into procurement, and that outsourced providers lack standardised service baselines[23]. Barriers that fall hardest on the smaller, innovative firms that dominate our sector when they try to sell into the public and private sectors alike.

AI and the pace of the threat: hostile states are already using AI to accelerate reconnaissance, automate spear-phishing and speed up exploit development, and the NCSC assesses that AI "will almost certainly pose cyber resilience challenges to 2027 and beyond"[24]. Businesses need to be able to adopt defensive AI and automation at least as quickly as attackers adopt offensive AI.

Increasingly dispersed and exposed supply chains: only 15% of businesses formally reviewed the cyber risks posed by their immediate suppliers in the past year, and just 6% reviewed their wider supply chain[25]. As JLR showed, a single breach at one manufacturer can cascade through thousands of suppliers[26], even as the Cyber Security and Resilience Bill extends statutory duties to managed

---

[17] DSIT, Cyber Security Breaches Survey 2025/2026 (GOV.UK)
[18] DSIT, Cyber Security Skills in the UK Labour Market 2025
[19] DSIT, Cyber Security Breaches Survey 2025/2026 (GOV.UK)
[20] NCSC Annual Review 2025, National Cyber Security Centre
[21] Government backs £1.5bn loan guarantee for suppliers as JLR recovers from cyber attack, AM-Online
[22] DSIT, Cyber Security Sectoral Analysis 2026 (GOV.UK)
[23] APPG for Cyber Innovation – SME & cyber resilience roundtable summary, BCS
[24] NCSC Annual Review 2025, National Cyber Security Centre
[25] DSIT, Cyber Security Breaches Survey 2025/2026 (GOV.UK)
[26] Cyber Monitoring Centre statement on the Jaguar Land Rover cyber incident (October 2025)

service providers, data centres and other newly designated "critical suppliers"[27]. These are welcome reforms, but they will bring real compliance costs for many organisations that will fall into scope..

CBN's 'asks in detail' for the Autumn Budget

Each ask below responds directly to at least one barrier set out above, intending to lower the cost of adopting cyber security, close the skills and awareness gap, and ensure the businesses most exposed to attack and most central to delivering the Cyber Security and Resilience Bill have the support they need.

1. Tax relief to lower the cost of purchasing cyber security from UK providers

Cyber security products and services currently attract the standard 20% rate of VAT and no other tax relief that would encourage greater investment into UK cyber products & services. Ultimately, reducing the incentive for UK businesses to invest in the UKs best-in-class cyber security, with the most prominent impact being had on SMEs least able to afford it. Therefore creating significant and broad risk to economic business resilience.

In other critical areas, tax relief has been implemented to encourage investment on systems and services that ensure UK business continuity and support resilience. For example; the ESM zero rate for flood resilience and defence now allows organisations to invest more widely in systems that secures against risk or the tax credits applied to the purchase of energy related sources (ie heat pumps) that allows the UK to become more resilient to the impacts on energy security.

Globally examples already exist of tax schemes that encourage investment. In the US, the IRS Section 179 allows businesses to deduct the full cost of qualifying cybersecurity purchases in the same tax year rather than depreciating over time, and a White House advisory board (NSTAC) has separately recommended the federal government extend tax incentives to critical infrastructure operators to drive cybersecurity improvements.

Ask: CBN would argue the next logical step would to explore targeted cyber security tax relief or credits – for example, enhanced capital allowances or a reduced rate for spend on accredited cyber security products and services, such as those delivered by Cyber Essentials-certified UK providers, to reduce the cost of adopting protection before a breach, not just recovering after one. The long term impact would both drive stronger resilience across UK business, encourage sector growth and retain talent in a promising sector for the UK.

2. Funding for cyber awareness, skills and training

With only 14% of micro-businesses aware that Cyber Essentials exists, and the annual UK cyber workforce gap still standing at around 3,800 roles, awareness and

[27] The UK's new Cyber Security and Resilience Bill, Travers Smith

skills sit on the same barrier: businesses that don't know they're exposed rarely invest in the people or training to fix it. Where Government has funded this consistently, it works – CyberFirst has reached over 415,000 young people since 2016, and its successor, TechFirst, is scaling that model further, targeting a million secondary school students and 5,000+ university bursaries and scholarships across the UK. But funding for awareness and skills has sat largely within DCMS (formerly DSIT) and the NCSC's own budget, when the businesses most exposed – retailers, manufacturers, local authorities, the professions – sit under other departments' remit entirely.

Ask: Provide sustained, multi-year funding for a combined national programme of cyber awareness, skills and training – building on proven vehicles such as CyberFirst/TechFirst, Cyber Aware and CyberFirst apprenticeships – and structure it so that other government departments can co-invest against their own sectors' exposure, rather than treating cyber skills funding as DCMS's alone to find.

3. Reduce the bureaucracy and cost of procurement for UK cyber security companies

58% of UK cyber security firms are micro-businesses and 19% are small businesses, a far higher proportion of small firms than the UK average[28]. These innovative companies are best placed to help the economy adopt new protections quickly, but too often find procurement processes slow, costly and disproportionate to their size.

Ask: Simplify accreditation and procurement routes for UK based cyber security SMEs, building on frameworks such as G-Cloud, so the SME allocation recently promised within major digital procurement frameworks is matched by faster, cheaper routes to market.

4. Support for organisations newly in scope of the Cyber Security and Resilience Bill

CBN strongly supports the Cyber Security and Resilience Bill's extension of statutory duties to managed service providers, data centres and other newly designated critical suppliers[29]. However, many organisations newly in scope, or expected to come into scope via secondary legislation or regulation, may now face significant compliance requirements, risking a cost burden some cannot absorb, reducing competition in critical supply chains.

Ask: Create a dedicated funding and advisory support structure – for example, a compliance grant or voucher scheme delivered with the NCSC – to help organisations meet their obligations under the Cyber Security and Resilience Bill and subsequent secondary legislation.

5. Support cyber security growth in the regions

[28] Cyber Security Sectoral Analysis 2026, GOV.UK

[29] The UK's new Cyber Security and Resilience Bill, Travers Smith

The UK's cyber security strength is not confined to London and the South East. The UK Cyber Cluster Collaboration (UKC3) network has grown from 12 regional clusters in its 2021/22 pilot year to 18 today, with around 22,500 members and over 10,000 students reached in 2024 alone – from Wales and Scotland to the North West and Northern Ireland. These clusters are the mechanism through which regional SMEs access talent, investment and knowledge-sharing that would otherwise concentrate in a handful of cities. Unfortunately, in March 2026 this programme concluded without a follow up programme to further strengthen this regional growth.

Ask: Assess & introduce a new programme of multi-year funding for the UK's regional cyber growth hubs, so that the sector's jobs, investment and skills pipeline continue to spread across every UK nation and region, not just its established hubs.

6. Strengthen the environment for UK cyber exports and scale-ups

The UK has built globally competitive cyber security companies – but too many have scaled by leaving. Darktrace, founded in Cambridge, was taken private in a £4.3 billion acquisition by the US firm Thoma Bravo in 2024, delisting from the London Stock Exchange. Sophos, founded in Abingdon, has been under Thoma Bravo's ownership since 2020, and in February 2025 completed an $859 million acquisition of the US firm Secureworks, deepening its US ownership base. Each is a UK-founded success story whose ownership, and long-term value, now sits overseas. Without a stronger domestic environment for patient capital, that pattern will keep repeating – just as the sector's £8.6 billion of exports and 70,000 jobs are ones the UK can least afford to lose.

Ask: Strengthen the conditions for UK cyber scale-ups to remain UK-owned and UK-headquartered as they grow – including sustained patient capital through CyberASAP and Cyber Runway follow-on funding, and export support that helps promising firms scale from the UK rather than sell into foreign ownership.

Conclusion

The Chancellor's priorities – stability, growth everywhere, and easing cost-of-living pressure – are directly served by a more cyber-resilient UK. Every pound spent recovering from a preventable breach is a pound not available for investment, wages or growth.

Take the substantial JLR incident of 2025 - £1.9 billion economic cost - the subsequent £1.5 billion government had to guarantee for its suppliers - the eventual 4000 job losses. This is an incident that goes beyond one organisation, to disrupting an entire local economy on a scale we haven't seen previously. These incidents are only likely to increase when actor vectors and AI drive the prevalence and scale of attacks across the UK economy without the correct funding or mechanism to enhance resilience, upskill the workforce or grow the sector innovating to protect.

CBN's asks shifts this balance from reactive recovery to proactive resilience, backing a sector that already supports around 70,000 jobs and £8.6 billion of exports. We would welcome discussing these with HM Treasury.