Alexander Evans

June 9th, 2025

How to strengthen UK business and public sector against cyber-threats

*Cyber risk is increasing in the UK – costing companies and citizens billions. Notwithstanding robust efforts by the government, **Alexander Evans** argues another step is needed to bolster individual responsibility at company Board level.*

Enjoyed this post? Sign up to our newsletter and receive a weekly roundup of all our articles.

Britain's digital defences are being battered in 2025. A wave of cyber assaults are hitting the country's public and private sectors, exposing systemic vulnerabilities and rattling consumer trust. Household names have been affected, including Marks & Spencer, Harrods, and Co-Op UK all falling victim to coordinated attacks, disrupting operations and compromising millions of customers. The scale and sophistication of these attacks, including AI-driven phishing, underscore a grim reality: Britain's cyber hygiene is faltering.

The challenge is both retail and wholesale. Cyber-crime is increasing, now an estimated 43 per cent of all crime in 2024 according to the UK Crime Survey, targeting citizens and companies. The current threat environment sees state and non-state actors converging to exploit digital vulnerabilities with increasing sophistication. Ransomware attacks alone have cost UK businesses billions, with the average global incident requiring 287 days to identify and contain. Yet these figures capture only the immediate financial impact, not the longer-term erosion of trust, competitive advantage, and strategic capability. Meanwhile organisations are struggling to keep up.

The UK Government's *Cyber Security Breaches Survey 2025* reveals concerning gaps in cyber risk management across different business sizes. Only 31 per cent of businesses and 26 per cent of charities reported having undertaken a cybersecurity risk assessment in the past year although this rises to 63 per cent of medium-sized businesses and 72 per cent of large businesses.

Meanwhile, 43 per cent of businesses and 30 per cent of charities reported experiencing some form of cybersecurity breach or attack in the last 12 months.

> *Cyber risk has evolved into a strategic imperative that demands board-level attention. This calls for a new approach to corporate governance on cyber.*

Since sweeping into power in 2024, Labour has moved swiftly to shore up Britain's digital defences. A landmark Cyber Security and Resilience Bill, unveiled in 2025, promises to tighten oversight of digital supply chains and expand mandatory breach reporting, while granting regulators sharper teeth. Over £1 billion has been earmarked for cyber and digital defence. Complementing this is the Digital Information and Smart Data Bill, which lays the groundwork for secure digital identities and smarter data sharing. The National Cyber Security Centre, part of GCHQ, continues to track and advise on the evolving threat, supported by tech companies.

A new approach to cyber risk?

Cyber risk has evolved into a strategic imperative that demands board-level attention. This calls for a new approach to corporate governance on cyber. Across many boards – including those I sit on – Chief Technology Officers are rarely board members or on Executive Committees. This makes little sense given the scale of risk: financial, operational and reputational that organisations carry. But simply demanding that all boards include a Chief Technology Officer probably misses the point – the issue is board grip and accountability, not expertise alone. The time has come to change tack.

Is there another step that could be taken? Should the UK mandate a new board-level obligation for all medium and large firms in the form of a Chief Cyber Risk Officer (CCRO)? This would take the form of a nominated, named individual on private and public boards in the UK with an obligation to lead and report on cyber risk, foregrounding this at board level. Individual accountability tends to focus attention – as anyone who has shared a bathroom, kitchen or home knows well. Garrett Hardin's classic warning about the "tragedy of the commons" underscores how shared resources, when left to individual discretion without accountability, are prone to neglect.

> *Should the UK mandate a new board-level obligation for all medium and large firms in the form of a Chief Cyber Risk Officer?*

And boards struggle to ensure that they have sufficient talent and technical knowledge to oversee technology and cyber risk. Headhunters I interview are persistently chasing capability at board level to bridge this gap. There is also a generational challenge: tech and data evolves at pace, while the average age of decision-makers in the UK private and public sector tends to veer towards the 50s (or more). In UK public companies, the average age of appointment for the role of CEO is 49 years. The average age of appointment for non-executive directors in the UK is 56 years, and 59 years for Chairs. Only three per cent of non-executive directors (NEDs) in the UK are under the age of 45, according to Spencer Stuart in 2024. This is not to be ageist: but recognising that much of the talent engaged with digital and data tends to be younger – as is the operational familiarity with potential compromises.

Making cybersecurity a C-suite priority

Traditional governance structures are inadequate. Most boards treat cybersecurity as a technical function delegated to Chief Information Officers or external consultants. This approach fundamentally misunderstands the strategic nature of cyber risk. The complexity requires dedicated expertise at the C-suite level – someone who can translate technical vulnerabilities into business language while ensuring that cyber considerations inform strategic decision-making.

Mandating CCROs could help forge greater board focus and investment to improve cyber defences. Unlike traditional CISOs who focus primarily on technical controls, a CCRO would operate at the intersection of risk, strategy, and regulatory compliance. The role would partner closely with the CTO and CEO, and make sure that at board level there would be a named, responsible individual. The most effective cyber governance structures embed risk assessment into core business processes.

Accountability is crucial. Recent incidents demonstrate that when failures occur, boards often struggle to explain their oversight responsibilities to regulators, shareholders, and the public. The Post Office Horizon scandal – while not a cybersecurity case – speaks to this. From an investment perspective, the CCRO role addresses a persistent challenge in corporate cybersecurity: the difficulty of securing appropriate capital and operational expenditure.

Technical teams often struggle to articulate business cases for cyber investments in language that resonates with apex decision-makers. A CCRO can translate threat landscapes into investment priorities while ensuring that security considerations influence broader business decisions. This enhances the quality and quantum of cyber-related investments. It's a better model than delegation to technology committees.

For a government serious about boosting growth, blunting the cyber threat is key. An overdose of regulation and compliance will just add costs for small and medium sized businesses already struggling with margins. But the CCRO model, without mandated additional reporting or personal legal liability, could focus minds – a named individual notified to Companies house in the annual return puts a premium on accountability. The broader implications extend to national resilience. A network of experienced CCROs across major UK firms and public sector bodies would create a community of practice that could enhance investment, information sharing and coordinated response. In the difficult age we live in, CCROs could boost cybersecurity and resilience.

All articles posted on this blog give the views of the author(s), and not the position of LSE British Politics and Policy, nor of the London School of Economics and Political Science.

Image credit: AlBooth on Shutterstock

Enjoyed this post? Sign up to our newsletter and receive a weekly roundup of all our articles.

About the author

Alexander Evans

Professor Alexander Evans is Associate Dean of the LSE School of Public Policy. He leads an LSE initiative on regulatory diplomacy and serves on various boards as a non-executive director. He is a former adviser in 10 Downing Street, Director Cyber in the Foreign Office and served on the Cabinet Office Executive Committee.

Posted In: Global Politics | Government | LSE Comment

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

© LSE 2025