Thrive Or Die – Cyber Security

UK Cyber Security And Regulation Edition — Why Cyber Is Becoming The Core, Not The Perimeter

A Charterhouse Consultants white paper by Bridget Convey, November 2025

Executive Summary

This paper asks a direct question. Does cyber need to sit at the core of every organisation now, rather than as a perimeter function bolted onto IT? The evidence says yes, and it says so with unusual precision, because this is the one paper in the series where the capability to governance gap is not an analogy, it is the literal, current state of UK regulation. In April and May 2025, a loosely organised group of young UK-based attackers, using off-the-shelf tooling and a single phone call to a third-party helpdesk, caused between £270 million and £440 million of combined damage to Marks & Spencer, Co-op and Harrods. No nation-state resources were required. Meanwhile, the regulation meant to close this gap is still arriving in stages: DORA enforcement only became genuinely active in 2026, the UK's own Cyber Security and Resilience Bill will not be fully in force until 2028, and the National Cyber Security Centre's own roadmap for quantum-safe encryption does not complete until 2035. Attacker capability is compounding faster than the calendar regulators are working to.

The Premise: The Gap Is The Danger, Not The AI

In October 2023, a group including Turing Award winners Yoshua Bengio and Geoffrey Hinton, alongside Stuart Russell, Daniel Kahneman and more than twenty other senior AI researchers, published a consensus paper in the journal Science on the risks of advanced AI. Their argument was precise. AI capability and autonomy are increasing rapidly. Systems are shifting toward acting and pursuing goals with reduced human oversight. Governance is not keeping pace with that shift. In every other paper in this series, that mechanism has been used to explain organisational or institutional risk. In cyber security, it is not a borrowed mechanism. It is the field's own native description of what is happening. The UK's National Cyber Security Centre has stated plainly that AI will almost certainly increase the volume and impact of cyber attacks, specifically because it lowers the skill barrier for attackers who previously lacked the capability to cause serious harm.

This paper's core claim follows directly from that. If attacker capability and defender governance are both racing, and one is compounding through AI faster than the other is legislating, then cyber cannot remain a bolted-on IT function governed by an annual audit. It has to become as central to strategy as the financial controls, the customer product, or the AI governance this entire paper series has been arguing for. Cyber, in other words, is not a separate risk category any more. It is the same core versus shell question this whole series has been asking, applied to the infrastructure everything else in the organisation now depends on.

Thrive Or Die: When The Gap Is A Phone Call, Not A Decade

Kodak invented the first digital camera in 1975 and its own internal research predicted by 1981 that digital would eventually replace film. It took thirty seven years for the governance gap it left open to become fatal. Blockbuster was offered the chance to buy Netflix outright for fifty million dollars in 2000, declined, and filed for bankruptcy a decade later. Both prove the same point at a commercial timescale measured in years. Cyber security proves it at a timescale measured in minutes.

In April 2025, attackers linked to a loosely affiliated group known as Scattered Spider phoned M&S's outsourced IT helpdesk, impersonated an employee, and persuaded the agent to reset multi-factor authentication on a privileged account. From that single call, they gained domain administrator access, the customer database, and the ability to deploy ransomware across the business. Weeks later the same group struck Co-op and Harrods, using similar methods. The UK's Cyber Monitoring Centre, an independent body set up by the insurance industry to assess major cyber events, classified the combined M&S and Co-op incidents as a single Category 2 systemic event, with total financial impact estimated between £270 million and £440 million. M&S alone absorbed roughly £300 million off its operating profit, saw more than £700 million wiped from its market value, and suspended online clothing orders for 46 consecutive days. Four individuals were later arrested in the West Midlands and London, several of them young enough that press coverage repeatedly noted how unusual it was for attackers of this profile to cause damage of this scale. That is the point. The skill and capital required to inflict a £440 million loss on three major UK brands has collapsed, because attack tooling, social engineering scripts and ransomware infrastructure are now available off the shelf. Kodak and Blockbuster show what happens when a governance gap is left open for decades. M&S and Co-op show what happens when it is left open for the length of a single phone call.

The Evidence: A Widening Gap On Both Sides At Once

Two bodies of evidence anchor this paper. One shows attacker capability accelerating, driven substantially by AI. The other shows the regulation meant to close that gap arriving in careful, multi-year phases, by design, because rushed regulation of critical financial infrastructure carries its own risks. Both things are true at once, and the distance between them is the subject of this paper.

Attacker Capability Is Compounding, And AI Is The Accelerant

The NCSC's own assessment is that AI is already being used in malicious activity today, reducing the barrier to entry for novice criminals, mercenary hackers and hacktivists, enabling people with relatively basic skills to conduct far more effective intrusions. Fortinet's 2026 Global Threat Landscape Report recorded a 389 percent year-on-year increase in ransomware victims, and describes attackers now using AI-driven shadow agents that compress the entire attack lifecycle, reconnaissance, payload generation, lateral movement and exfiltration, into a fraction of the time it previously required. Armis's head of threat intelligence has made a specific, dated prediction that a major global enterprise will suffer a breach caused or significantly advanced by a fully autonomous agentic AI system by mid-2026. Palo Alto Networks has described the emerging risk in financial services terms directly, warning that a single well-crafted prompt injection or tool-misuse vulnerability can turn a trusted AI agent with privileged

access into what it calls an AI insider threat, capable of executing trades, deleting backups or exfiltrating entire customer databases autonomously.

Regulation Is Closing The Gap Deliberately, In Stages, By Design

DORA, the EU's Digital Operational Resilience Act, became fully applicable on 17 January 2025, and 2026 is the year enforcement moved from reviewing frameworks to active supervision, with national regulators now cross-checking registers of ICT third-party arrangements and beginning to issue penalties. It does not apply directly to UK-only firms, though the FCA and PRA built a parallel operational resilience framework, mandatory since March 2025, that mirrors its principles. The UK's own Cyber Security and Resilience Bill, introduced to Parliament in November 2025, is expected to receive Royal Assent in late 2026, but full implementation is not expected until 2028, and it diverges from the EU's NIS2 in enough specific respects that firms operating across both jurisdictions will need to run two similar, but not identical, compliance programmes. The most concrete long-dated deadline in this entire space is the NCSC's own post-quantum cryptography migration roadmap, published in March 2025: a full cryptographic inventory and migration plan by 2028, priority systems migrated by 2031, and complete migration across all systems by 2035. The NCSC has been explicit about why the urgency starts now rather than in 2033, adversaries are already engaged in harvest now, decrypt later collection, gathering encrypted financial and government data today specifically to decrypt it once quantum computing matures.

UK Cyber Security In Three Horizons: The Gap Closes Or It Does Not

This is the one paper in the series where the horizons below are not constructed from general trend analysis. Two of the three dates are taken directly from published NCSC and Parliamentary timelines. What is genuinely uncertain is not when the deadlines fall, but whether attacker capability, and the AI accelerating it, arrives faster than organisations close the gap in time.

Two Years: 2026 To 2028 — Regulation Arrives While Attacker Capability Is Already Ahead

What happens on the calendar: DORA enforcement continues to mature through active supervision, the UK Cyber Security and Resilience Bill receives Royal Assent and begins phased implementation, and the NCSC's 2028 deadline for a complete cryptographic inventory and migration plan falls due.

- Thrive path. Firms treat the 2028 NCSC cryptographic inventory deadline and the Cyber Security and Resilience Bill's phased implementation as one combined governance programme, not two separate compliance projects, and build third-party identity verification controls, of the kind that failed at M&S, as a board-level priority now rather than waiting for the Bill to force the issue.
- Die path. Firms treat 2026 to 2028 as a grace period because full enforcement of the UK Bill is not expected until 2028, while attacker capability, already assessed by the NCSC as accelerating through AI, does not wait for a commencement date, and the next Category 2 systemic event arrives before the regulation meant to prevent it is even fully in force.

Five Years: 2028 To 2031 — Priority Systems Migrate While Agentic Attacks Become Routine

What happens on the calendar: the NCSC's second PQC milestone falls due, with the highest-priority systems required to have completed quantum-safe migration, and the UK Cyber Security and Resilience Bill is expected to be fully in force.

- Thrive path. Organisations that began cryptographic discovery in the first horizon complete priority migration on schedule, and the same governance muscle built for quantum-safe migration is reused for AI agent oversight, since both are fundamentally the same problem, verifying that a system with real autonomy is doing only what it is authorised to do.
- Die path. Organisations that treated the 2028 deadline as the finish line rather than the starting gate arrive at this horizon with an incomplete cryptographic inventory, no priority migration plan, and by this point agentic AI-driven attacks are, per Armis's own prediction, no longer a novel risk but a routine one, arriving faster than a firm starting from zero can credibly catch up.

Ten Years: 2031 To 2036 — Quantum Migration Completes, And Cyber Is No Longer A Separate Discipline

What happens on the calendar: the NCSC's full migration deadline of 2035 falls within this horizon, meaning every system, service and product still relying on classical encryption is expected to be fully quantum-safe.

- Thrive path. By this point, cyber governance and AI governance have converged into a single discipline, because the organisations that thrived through the two prior horizons will have already built one governance function that treats system autonomy, whether it is an AI agent or a cryptographic protocol, as the same underlying question. Cyber is no longer a department. It is the core the rest of the organisation is built on.
- Die path. Organisations that kept cyber and AI governance as two separate reporting lines, run by two separate teams, with two separate boards' sub-committees, discover that the seams between them, exactly where an AI agent's access intersects with a cryptographic control, are where the next Category 2 systemic event originates, because nobody owned the whole picture.

What I Am Recommending To Boards Across Every Sector In This Series

- Treat the NCSC's 2028, 2031 and 2035 post-quantum cryptography deadlines as fixed, board-level dates now, not future IT planning items, since the harvest now, decrypt later threat means data volumes exposed grow every year action is delayed.
- Audit third-party helpdesk and identity verification procedures specifically, since the M&S, Co-op and Harrods attacks did not begin with a technical vulnerability, they began with a phone call, and the same social engineering playbook has already been used against MGM, Caesars, ICBC and multiple other major brands.
- Stop governing cyber security and AI governance as two separate programmes. The mechanism behind both is identical, capability with real autonomy needs oversight that scales at the same pace, and organisations that build one governance function for both will close the gap faster than organisations running two.
- Assume attacker capability will continue compounding through AI faster than statutory deadlines require, and build ahead of the compliance calendar rather than to it, since the Cyber Monitoring Centre's own post-incident guidance for the M&S and Co-op attacks stressed exactly this, testing continuity plans against realistic scenarios before regulation demands it.

Conclusion: Does Cyber Need To Be At The Core Of Everything Now?

Yes, and this paper series has, without initially intending to, already been building the argument for why. Every prior paper in this series has described the same mechanism, capability accelerating faster than governance, playing out differently across insurance, banking, asset management, fintech, professional services, defence, healthcare, energy, telecoms and real estate. Cyber security is not a new addition to that list. It is the substrate all of them run on. The NCSC's own quantum migration roadmap already spans a decade, structured almost exactly like the horizons this series has used throughout. The M&S, Co-op and Harrods attacks already show what a governance gap costs when it is left open for the length of a phone call rather than a generation. Every board this series has been written for is already running the cyber version of this argument, whether or not it has been named that way internally. The organisations that close the gap will be the ones that stop treating cyber as a perimeter around the business, and start treating it, and the AI governance this whole series has argued for, as one and the same core.

Sources: Computer Weekly, The Hacker News, Silicon UK, BlackFog, Storm Guidance, atthacked.com, Cyber Monitoring Centre assessments, NCSC published guidance and Annual Review 2025, techUK, Mayer Brown, Trowers & Hamlins, Macfarlanes, TLT, Taylor Wessing, Naq Cyber, Kiteworks, PwC UK, Fortinet 2026 Global Threat Landscape Report, SecurityWeek, Panorays, Trend Micro, CybersecurityNews.com. All figures and regulatory dates current as of mid-2026, verified at time of writing. This is a first draft prepared for internal discussion.