BCLP. Client Intelligent

**Insights**

# CYBER RESILIENCE IN FINANCIAL SERVICES: NAVIGATING RISING RISKS AND THE 2026 REGULATORY SHIFT

Apr 07, 2026


SUMMARY

UK regulators have not yet fully exercised the breadth of their powers to address shortcomings in organisational cyber-security measures—but that restraint is unlikely to continue. The policy statements published on 18 March 2026 by the FCA, PRA and Bank of England, introducing a new single regime for operational incident and third-party reporting, signal the direction of travel. The framework—under which firms must report serious cyber and operational incidents through a unified portal and provide structured information on their critical third party (CTP) dependencies—reflects the UK regulators' sharpened focus on digital risk, system resilience, and their recognition of the vulnerabilities inherent in complex technological supply chains.

This shift sits alongside the UK government's broader agenda. As the Cyber Security and Resilience (Network and Information Systems) Bill (NIS Bill) progresses and HM Treasury (HMT) prepares to designate major technology providers as CTPs using its FSMA powers, firms can expect a step-change in supervisory expectations. Cyber-security, data protection and operational resilience disciplines must now operate as a single, evidence-based ecosystem capable of withstanding assertive regulatory challenge. The coming year will require firms not only to demonstrate alignment on paper, but to evidence—consistently and credibly—that controls work in practice.

This article is the first in our three part Emerging Themes in Financial Regulation & Disputes 2026 series. We examine the evolving regulatory and risk landscape shaping cyber and operational resilience expectations for the year ahead—and set out practical priorities for financial services firms seeking to respond proactively. Our accompanying articles will examine (i) the evolving cyber litigation risks facing financial services firms and (ii) operational resilience and the growing influence of CTP designations.


## WHY 2026 REPRESENTS A REGULATORY TURNING POINT

The regulatory backdrop is now unmistakable. As the FCA highlighted when announcing the new unified operational-incident and third-party reporting framework, cyber attacks are increasing in frequency and sophistication, and more than 40% of all cyber incidents reported to the FCA in 2025 involved a third-party provider—a reminder that technology-supply-chain fragility has become a structural vulnerability for the sector. The outages referenced by the FCA underline the risk that a single service provider failure can have system-wide consequences. This context explains why regulators have converged around a single, cross-authority reporting regime: clear, consistent and timely reporting is now viewed as essential to identifying risks early and enabling coordinated intervention.

2025 did not deliver a single, sector defining "mega incident" in UK financial services. But it did see significant attacks on two well-known high street retailers and a major automotive manufacturer, with supply chain disruption that underscored the economy wide consequences of cyber shocks. The year also saw a series of more targeted attacks affecting financial services customers, including a ransomware related incident in which insiders at a global crypto platform were bribed to access internal systems and extract user data—an event that impacted UK based account holders.

ICO incident-trend reporting shows that financial services remained one of the most consistently affected sectors, with ransomware and malware dominating reported incidents. The exposure is persistent and structural, and the ICO also reinforces that firms must reflect on lessons learned across ICO cases more broadly—not just those arising within the sector.

The NCSC's 2025 Annual Review reinforces this urgency, positioning cyber as a strategic board level risk. With "an average of four nationally significant cyber attacks every week", the message to firms is unmistakable: prepare now, not after an attack. As the NCSC puts it, "It is time to act." The messaging also has to be seen in the context of the Bank of England's repeated warnings in its Financial Stability Reports, including the December 2025 report, highlighting elevated cyber and geopolitical risk.

At the same time, 2026 marks the first full year in which firms must meet the FCA and PRA's "steady-state" operational-resilience expectations, embedding tested impact tolerances across important business services. Add to this the continued rise of fraud – UK Finance's published annual fraud data for 2025 reports £1.17bn of annual losses – and the rapid expansion of AI-enabled threat vectors, and the result is a sector facing a genuine regulatory inflection point.

Taken together, these pillars reinforce a central theme for regulators: the absence of a single catastrophic failure does not imply systemic resilience. Instead, persistent sector adjacent disruption, coupled with targeted attacks on financial consumers, has sharpened the supervisory view that 2026 must be the year in which firms demonstrate not only sophisticated organisation-wide awareness of cyber risk, but credible, embedded resilience in practice.

## REGULATORY EXPECTATIONS AND LESSONS LEARNED

The ICO, under Commissioner John Edwards, has emphasised a proactive regulatory approach—using guidance and published reprimands to drive change. As Edwards wrote in November 2025: "reprimands drive change and publishing them creates strong reputational incentives for compliance, while also offering other organisations valuable lessons from the mistakes of others." This shift towards visible, preventive signalling is notable even if fewer monetary penalties are imposed.

Several high profile enforcement actions continue to underscore the importance of fundamental cyber hygiene. The ICO's £14m penalty against Capita in October 2025 for failures in security measures and breach response capability demonstrates the consequences of inadequate controls across complex data environments. Similarly, two years before, the FCA's £11m fine against Equifax reflects longstanding concerns around intra group oversight, particularly where UK customer data is processed by overseas affiliates. These cases highlight a common regulatory theme: failures of oversight, whether third party or intra group, remain a critical risk vector.

Alongside this, the FCA's August 2025 insights from its Cyber Coordination Group underline five points of broad relevance to firms:

1. Threat-led testing exposes what conventional assurance misses. CBEST (Critical National Infrastructure Banking Supervision and Evaluation Testing) and STAR-FS (Simulated Targeted Attack and Response for Financial Services) continue to be the most effective means of identifying previously unknown vulnerabilities.

2. Minor weaknesses can combine into major risk. The FCA highlights that clusters of "non-critical" vulnerabilities can cause as much harm as a single critical flaw.

3. Legacy technology still requires active governance. End-of-life systems must be subject to the same risk management expectations as modern infrastructure.

4. Information-sharing materially strengthens sector response. Forums such as the UK's CMORG (Cross Market Operational Resilience Group) and the global FS-ISAC (Financial Services Information Sharing and Analysis Center) play an important role during significant third-party outages.

5. AI introduces opportunity and new exposure. Without proper understanding and controls, AI adoption in cyber domains can create novel or unidentified risks.

What troubles the FCA most is the persistent disconnect between documented controls and operational reality. Common issues include misconfigured access, phishing susceptibility, inherited scoring models that no longer reflect the business and over reliance on third party assurances that

fail to reflect real world usage. Supervisors continue to probe whether firms do what they say they do—particularly in relation to privileged access, testing cadence and intra group outsourcing.

The CTP regime further shapes this landscape. CTP oversight by regulators does not dilute firms' existing outsourcing and operational resilience obligations; it heightens the need for accurate dependency mapping and credible assurance.

## MODERNISING THE UK'S CYBER LEGISLATION AND RESILIENCE FRAMEWORK

Sector regulators already have enforcement powers under the Network and Information Systems (NIS) Regulations 2018, which are designed to strengthen the resilience of essential services and the digital economy. The NIS Regulations apply both to operators of essential services and to digital service providers, capturing any incident, cyber or non cyber, with a significant disruptive effect (including physical failures such as power loss or system outages). Historically, however, regulators have used their enforcement powers pursuant to the NIS Regulations sparingly. Although significant incident notifications rose sharply between 2022 and 2024, no formal sanctions were imposed during that period.

The NIS Bill introduced in late 2025 is the most substantial overhaul of the UK's NIS framework to date. For a deeper dive, see our BCLP analysis. For financial services firms, we highlight three significant developments:

1. Expansion of scope: Managed service providers (MSPs), data centres and other key supply chain actors can now be brought into the regulatory perimeter. Government will have the power to designate suppliers whose disruption could pose systemic risk. This targets concentration risk and the "single point of failure" problem that has surfaced in several large outages.

2. Accelerated incident reporting: A new two-stage reporting model—initial notification within 24 hours and a full report by 72 hours—will require seamless coordination between legal, cyber, data protection, and communications teams, especially where the Article 33 thresholds under the UK General Data Protection Regulation (UK GDPR) are also triggered. The practical takeaway: incident playbooks must be time-bound, role-clear, and evidence-ready.

3. Strengthened regulatory powers and cost recovery: Regulators will gain enhanced powers to demand information, direct remediation, and recover supervisory costs. This not only raises the stakes for cloud and other data hosting vendors, but also for the firms that depend on them. In practice, firms should expect sharper due diligence requirements and more intrusive oversight.

The EU's approach provides a useful contrast, highlighting how major jurisdictions are converging on similar themes while diverging in execution. While the UK is pursuing a targeted, criticality-driven model—combining NIS reform, the emerging CTP regime and steady-state operational resilience—the EU is already operating under the Digital Operational Resilience Act

(**DORA)** and preparing for updated cybersecurity directive known as **NIS2**. The regimes share broad objectives: faster incident reporting, strengthened ICT risk governance, threat-led testing, and tighter supply-chain oversight. But they diverge materially in design. Where the EU favours harmonisation and prescriptive, centralised oversight, particularly for critical ICT providers, the UK's framework emphasises proportionality, system criticality and alignment with national-security-led prioritisation. For firms operating across both jurisdictions, the practical takeaway is clear: align programmes where sensible, but do not presume equivalence—reporting triggers, supervisory expectations, and enforcement architectures will continue to differ in material ways.

## WHAT SHOULD FINANCIAL SERVICES FIRMS PRIORITISE NOW?

### Elevate cyber to a core business risk

Firms should treat cyber resilience as a strategic business risk by maintaining clear visibility of service dependencies and defined incident triggers, including 24- and 72-hour NIS and UK GDPR duties. Governance artefacts should evidence informed challenge and accountability, ensuring boards understand how disruption could propagate across the organisation and its supply chain, and that mitigations are properly resourced and embedded.

### Refresh dependency and CTP mapping

Organisations should update end-to-end service maps across third- and fourth-party chains, identify providers likely to fall within the future CTP perimeter, and document failure modes and realistic fallback arrangements, validating exit, contingency and substitution strategies to ensure clarity on what fails over, where, and with what operational friction.

### Strengthen simulation and threat-led testing

Firms should continue CBEST/STAR-FS and high-fidelity simulations that test technical, procedural and human decision-making under pressure, including coordination between cyber, legal and privacy teams, while rehearsing dual-track NIS and UK GDPR reporting and ensuring remediation is tracked through to closure and verified by re-testing.

### Coordinate data protection and cyber response

Organisations need a pre-agreed triage model aligned with NIS 24/72-hour triggers and UK GDPR thresholds, supported by structured coordination across legal, cyber, privacy and communications teams, with all regulatory and stakeholder outputs drawn from a single "golden source" of verified incident information.

### Reassess payments and critical infrastructure dependencies

Firms should re-evaluate operational dependencies on payment systems—especially in the context of the New Payments Architecture—by reviewing exposure across interbank retail payments and

internal reconciliation processes and ensuring playbooks reflect the practical realities of outages, settlement delays and customer communication obligations.

### Upgrade contracts, diligence and supplier monitoring

Supplier oversight should be strengthened through enhanced diligence and contractual controls—including audit rights, testing access, telemetry standards, breach cooperation and subcontractor flow-downs—and supported by continuous, telemetry-driven monitoring, with intra-group arrangements subjected to the same scrutiny as external outsourcing.

### Pressure-test cyber insurance coverage

Firms should validate cyber insurance limits, business interruption triggers and vendor failure cover, assess exclusions relating to war, terrorism and sanctions, and ensure incident response processes—from forensics to claims notification—are fully aligned with policy terms to avoid disputes during a live event.

### Evidence culture—not just controls

Organisations should use the NCSC CAF to demonstrate embedded governance, secure-by-design principles, and control-owner-level resilience, supported by meaningful metrics such as detection and containment times, patch latency, backup immutability tests and achieved RTOs/RPOs (Recovery Time & Point Objectives), ensuring regulators see evidence of lived practice rather than static policy.

## CONCLUDING THOUGHTS

The UK is raising the regulatory floor through the NIS Bill, widening supervisory visibility via the emerging CTP regime, and consolidating expectations under steady state operational resilience rules. Across the EU, DORA and NIS2 already apply, signalling a parallel shift toward more assertive oversight. Against a backdrop of AI enabled fraud, increasingly fragile supply chain dependencies and heightened reliance on payments infrastructure, the question for 2026 is no longer whether cyber posture is documented—it is whether it works in production, and whether third party providers can evidence that resilience with equal clarity.

For financial services firms, the winners in 2026 will be those that treat resilience as an engineered, measurable capability: understanding and mapping dependencies with precision, tightening contractual levers and supplier oversight, conducting threat led tests early and often, and ensuring boards can not only see but prove that the organisation can absorb shocks and recover at pace. In a year defined by regulatory convergence, rising threat sophistication and enhanced supervisory expectations, credible operational resilience strategies will distinguish those prepared for disruption from those merely hoping to avoid it.

## RELATED CAPABILITIES

- Financial Regulation Compliance & Investigations

## MEET THE TEAM


**Geraldine Scali**

Partner and EMEA Lead of Data Privacy and Security, London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483



**Samantha Paul**

Knowledge & Innovation Counsel, London

samantha.paul@bclplaw.com
+44 (0) 20 3400 3194



**Anna Blest**

Knowledge & Innovation Counsel, London

anna.blest@bclplaw.com

+44 (0) 20 3400 4475

---