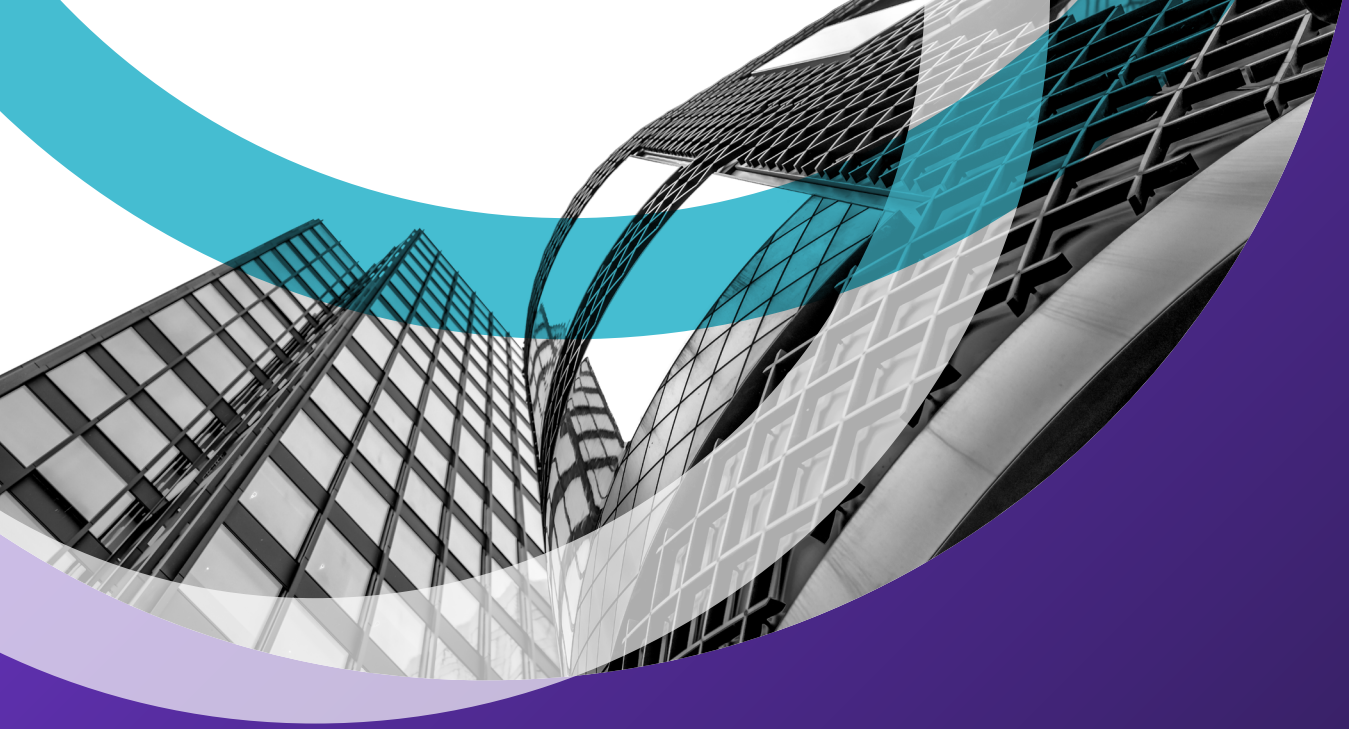


RESEARCH REPORT 2026

# Cyber Security in Financial Services

Learn about the top cyber threats, trends and challenges facing financial services organisations in 2026.

Bridewell

Cyber Security. Where it Matters.

# Foreword

Financial services organisations have long operated under intense regulatory scrutiny. High-profile cyber incidents over the past year, combined with growing geopolitical and economic uncertainty, have forced many institutions to reassess their security posture as well as their operational resilience to withstanding cyber threats and resulting disruption.

What sets financial services apart is the convergence of high-value assets, complex digital ecosystems, and stringent regulatory requirements. While organisations in this sector tend to be more mature than those in others, they are also more frequently targeted due to the sensitive data and financial transactions they manage. Attackers are highly motivated, and response processes tend to be layered and cautious; however, the consequences of failure, whether financial, operational, or reputational, are significant.

This year's findings show a sector that understands the risks it faces but is still grappling with how to respond quickly enough in a fast-moving threat landscape. From managing AI risk to improving response times and strengthening trust in security tooling, the challenge now is evolving from awareness to execution.

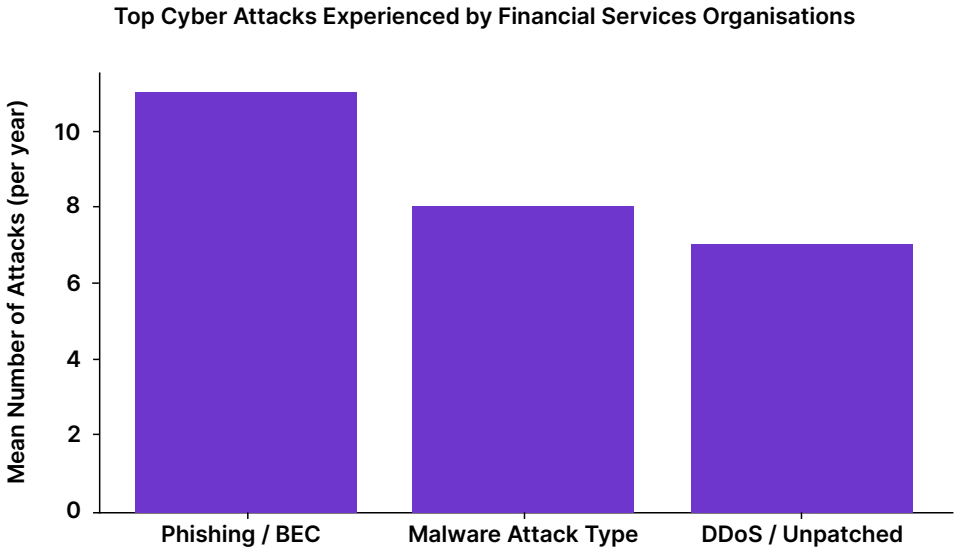
# Executive Summary

**The financial services sector remains one of the most targeted and highest-impact areas within UK Critical National Infrastructure (CNI). While broadly aligned with cross-sector trends, including the near-universal experience of cyber attacks, the continued dominance of phishing and business email compromise and the growing importance of data protection and AI-related risks, financial organisations face distinct pressures driven by regulatory oversight, high-value transactions and complex operating environments.**

### Key findings include:

- Cyber attacks remain near-universal, with 93% of financial services organisations experiencing a cyber incident involving ransomware, supply chain attacks, employee sabotage, data theft/leakage, physical security breach, malware, phishing/ BEC, unauthorised system access, social engineering, DDoS or outdated software/unavailable patches for legacy equipment.
- Financial services organisations demonstrate cyber security maturity, including strong adoption of formal incident response processes, sustained investment following incidents and a greater focus on governance-driven risks such as data protection and AI.
- Phishing and BEC attacks are especially prevalent, reflecting financially motivated threat activity.
- Response times are the slowest across all sectors, with data theft incidents taking nearly 24 hours on average to respond to.
- AI cyber risk (42%) and data protection (40%) are top concerns, closely aligned with regulatory and operational risk.
- Trust in cyber security tools is the highest challenge for financial services out of all CNI sectors (36%), indicating some scepticism around tooling effectiveness.

**Approximately how many, if any, of the following [cyber attacks] have you suffered from in the past 12 months?**



# Top Cyber Security Concerns by Sector

**What, if anything, are your biggest cyber security challenges at present? (Select up to 5)**

| Concern | Government | Finance / Insurance | Utilities | Transport | Manufacturing | Healthcare |
|---|---|---|---|---|---|---|
| Data protection & privacy | **45%** | 40% | **45%** | 43% | **45%** | **51%** |
| Managing AI cyber risk | 41% | **42%** | 27% | **55%** | 37% | 35% |
| Improving cyber resilience | 41% | 21% | 37% | 34% | 34% | 40% |
| Managing cloud cyber security | 28% | 23% | 30% | 32% | 36% | 29% |
| Trust in cyber security tools | 27% | 36% | 25% | 25% | 33% | 26% |
| Complying with regulations | 23% | 28% | 31% | 30% | 25% | 28% |

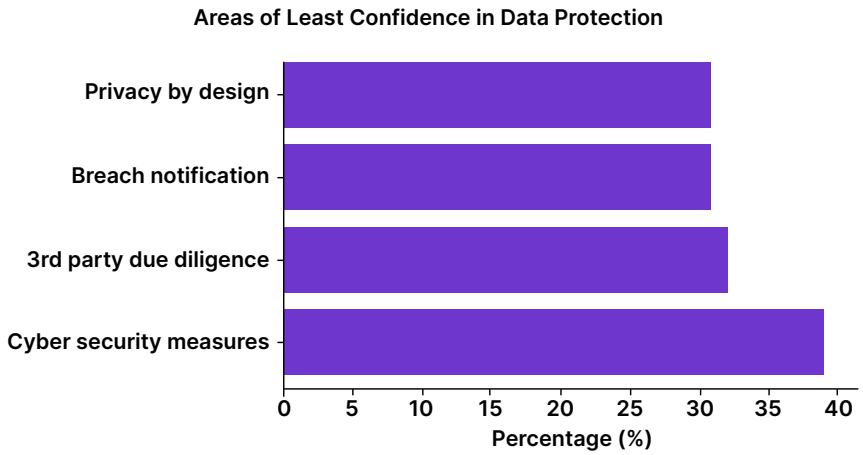
Overall, financial services organisations are among the most mature in cyber security terms, however, this maturity is accompanied by structural complexity, with slower response times indicating that highly controlled environments can introduce operational friction during incidents.

# Data Protection, AI Risk and Regulatory Pressure

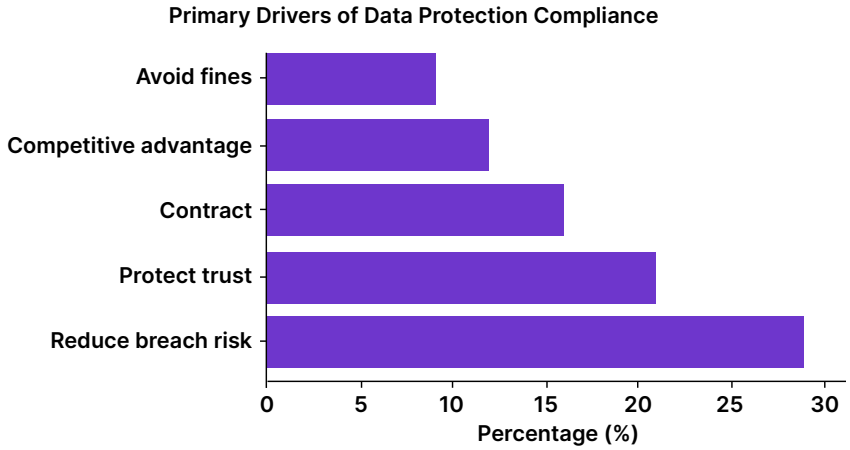
Data protection remains one of the most pressing cyber security challenges for financial services organisations, with 40% citing it as a top concern, closely aligned with the CNI average of 43%. However, within financial services, this concern is amplified by the sheer volume and sensitivity of the data being handled. Financial institutions manage vast amounts of personal and transactional data, making them prime targets for attackers and placing them under intense regulatory scrutiny. Frameworks such as GDPR, DORA and ongoing oversight from bodies like the FCA and PRA mean that data protection failures carry significant legal and financial repercussions, not to mention operational consequences.

Alongside this, managing AI cyber risk has emerged as an equally urgent priority, cited by 42% of financial respondents, which is higher than the cross-sector average of 39%. This reflects the rapid integration of AI into core financial operations, from fraud detection and credit scoring to customer service automation. While these technologies offer efficiency and competitive advantage, they also introduce new risks around data exposure, model integrity and access control. As organisations expand the use of AI and agentic AI, the challenge extends further than simply controlling human access to sensitive data, to governing how AI systems and agents interact with it as well. This shift is forcing financial institutions to rethink traditional security models and places greater emphasis on identity (both human and non-human), access governance and data visibility across environments which are growing in complexity all the time.

**Which aspects of UK data protection requirements does your organisation feel least confident in complying with, if any? (Select up to 3).**




**What is the primary driver for your organisation to achieve compliance with UK data protection regulations, if any?**



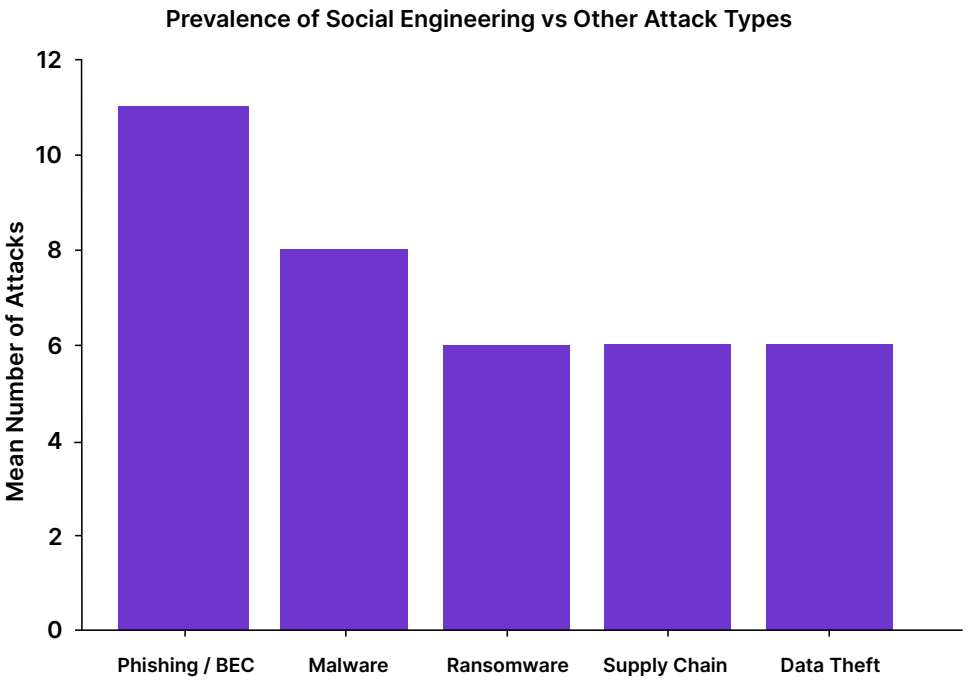
# Email Threats and Financially Motivated Attacks

Phishing and business email compromise (BEC) continue to dominate the threat landscape for financial services, reflecting the sector's attractiveness to financially motivated attackers. Across CNI, organisations experience an average of 11 phishing or BEC attacks per year, but in financial services, the potential payoff from even a single successful attack is significantly higher. This has led to more targeted and sophisticated campaigns, often focused on high-value individuals or systems involved in payments and financial decision-making.

What distinguishes the current threat landscape is the growing use of AI by attackers to enhance social engineering techniques. Emails are more convincing, impersonation is more accurate, and attacks are more scalable than ever before. In many cases, attackers no longer rely on crude phishing attempts, but instead compromise legitimate accounts and insert themselves into existing conversations. This makes detection significantly more difficult, as traditional security controls, designed to identify anomalies in email structure or origin, are less effective when the communication appears entirely legitimate.

As a result, the human layer remains the most consistently exploited entry point. While awareness training remains important, it is no longer sufficient on its own. Financial services organisations must rely on behavioural analysis, anomaly detection and AI-driven defence mechanisms to identify subtle deviations in user behaviour and communication patterns.

**Approximately how many, if any, of the following have you suffered from in the past 12 months?**



# The High Cost of Cyber Attacks in Financial Services

For financial sector organisations, the consequences of cyber attacks are felt most acutely in operational disruption and financial loss. IT outages and service disruption are the most common impacts, closely followed by direct revenue loss and increased cyber security investment. Notably, the psychological impact on employees also ranks among the top consequences, highlighting the growing human cost of cyber incidents.

Additionally, financial institutions face heightened regulatory obligations following an incident, including reporting requirements, investigations and potential penalties. This adds further complexity and cost to the recovery process. In many cases, the indirect costs, such as increased insurance premiums, long-term reputational damage and loss of customer confidence, can exceed the immediate financial impact of the attack itself.

**What have been the main consequences of a ransomware attack on your business? (Select up to 5).**

**Top 5 Consequences of Cyber Attacks in Financial Services:**

1. **IT disruption or outages** (49%)
2. **Loss of revenue from downtime** (36%)
3. **Increased cyber security budgets** (32%)
4. **Psychological impact on employees** (31%)
5. **Operational disruption to services** (30%)

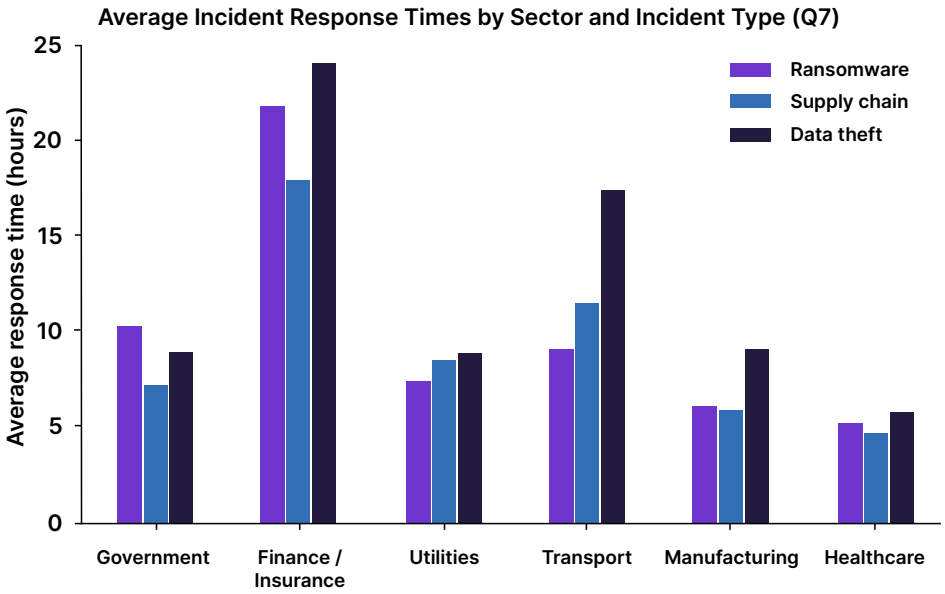
# The Response Time Problem

Despite relatively mature security capabilities, financial services organisations report the slowest incident response times across all sectors. On average, it takes nearly 24 hours to respond to data theft incidents, with ransomware and supply chain incidents also taking significantly longer than in other industries. This stands in stark contrast to the speed at which modern attackers operate, with data exfiltration often occurring within minutes of initial access.

The root of this challenge lies not in a lack of capability, but in the structural complexity of financial organisations. Decision-making processes are often layered, requiring validation, escalation and approval before action can be taken. Regulatory considerations further complicate this, as organisations must ensure that any response aligns with compliance obligations and reporting requirements. While these controls are necessary, they can significantly delay containment efforts during a live incident.

This creates too much space between detection and response. Even when threats are identified quickly, the time taken to act allows attackers to establish persistence, escalate privileges or exfiltrate data. Closing this gap will require financial institutions to rethink how incident response is governed, enabling faster, more decisive action while still maintaining appropriate oversight and control.

**What is the average time taken to respond to a cyber event?**



# Trust in Cyber Security Tools

Trust in cyber security tools has emerged as a particularly significant concern within financial services, with 36% of organisations highlighting it as a key challenge, higher than any other sector. This reflects growing unease around the effectiveness, transparency and reliability of the tools that organisations depend on to detect and respond to threats.

Several factors contribute to this lack of trust. Many organisations operate complex security stacks composed of multiple overlapping tools, making it difficult to achieve a clear and unified view of risk. At the same time, the increasing use of AI-driven security solutions introduces new challenges around explainability and auditability. Financial institutions, in particular, require a high degree of assurance that security decisions can be understood, validated and justified, both internally and to regulators.

As a result, there is a growing recognition that simply deploying more tools is not the answer. Instead, organisations are focusing on improving integration, reducing complexity and ensuring that the tools they use provide meaningful, actionable insights. Building trust in security tooling will be critical as organisations continue

# Conclusion: From Maturity to Agility

Financial services organisations are among the most advanced in terms of cyber security maturity, but this maturity does not necessarily translate into resilience. The findings highlight a sector that understands the risks it faces and has invested heavily in controls, but is still constrained by complexity, process and the pace of change.

The most significant challenge for 2026 is not identifying risk, but responding to it quickly and effectively. As attackers become faster and more sophisticated, the ability to detect, decide and act in real time will define resilience. This requires a shift away from traditional, compliance-driven approaches towards more agile, operationally embedded security models.

At the same time, emerging risks such as AI and expanding cloud environments are increasing the attack surface and introducing new layers of complexity. Addressing these challenges will require organisations to strengthen governance, improve visibility and build greater confidence in the tools and technologies they rely on.

Ultimately, the financial services sector is at a turning point. The foundations of cyber maturity are in place, but the next phase will be defined by execution and how effectively organisations can translate strategy into action, as well as how quickly they can adapt and recover from changing cyber threats.


+44 (0)3303 110 940 hello@bridewell.com bridewell.com