RISK LEDGER

Every Link Matters: The State of Supply Chain Security in Financial Services - UK Edition

A Risk Ledger Data Insights Report

About this report

This report, "Every Link Matters: The State of Supply Chain Security in Financial Services — UK Edition" provides a comprehensive analysis of supply chain security risks in UK financial services, based on a survey of cyber security and risk management professionals across the industry, open source data and proprietary risk intelligence.

About Risk Ledger

Risk Ledger was founded in 2018 by Haydn Brooks and Daniel Saul with a mission to shift the way organisations approach cyber security and risk management in the supply chain by building a global network of connected organisations. Today, Risk Ledger is the cutting-edge Third-Party Risk Management (TPRM) platform, dedicated to transforming supply chain security. We empower security and procurement teams to Defend-as-One, visualising their entire supply chain in real-time and providing unmatched transparency and collaboration. Our platform offers comprehensive, continuously updated risk assessments that reduce compliance burdens and enhance your organisation's cyber defences. By visualising and managing every link in your supply chain, Risk Ledger ensures you are always one step ahead of emerging threats.

Our commitment to asking the right questions and working closely with industry experts allows us to build a more secure, resilient future for all. With our Defend-as-One approach, we strengthen your organisation's ability to detect, respond to, and prevent cyber attacks. Risk Ledger isn't just about managing risk — it's about fortifying your entire supply chain because every link matters in cyber security.

We're here to help you secure today's operations and safeguard tomorrow's reputation, creating a safer digital landscape for all.

Risk Ledger Ltd.
Adam House
7-10 Adam Street
London WC2N 6AA
United Kingdom

Company registration number (England & Wales): 10831970

Contact: www.riskledger.com I marketing@riskledger.com I +44 1234 567890

Contents

Executive Summary: The State of Supply Chain Cyber Security in UK Financial Services

This executive summary distills the key findings from the new, comprehensive report "Every Link Matters: The State of Supply Chain Cyber Security in Financial Services – UK Edition". It provides C-suite executives, Chief Risk Officers (CROs), Chief Cyber Security Officers (CISOs) and regulatory leads with a high-level overview of the systemic vulnerabilities currently facing the supply chain ecosystem supporting financial sector organisations' critical business functions. For the full analysis, detailed survey data, regulatory context, and suggested solutions for transforming TPRM from a mainly reactive and increasingly ill-suited approach for managing supply chain risk into an active cyber defence discipline, please refer to the complete report.

The Architecture of Financial Fragility

The UK financial services sector enters 2026 at a critical juncture. The transition toward cloud-native architectures and wholesale digitalisation has created a "visibility crisis" where the distinction between internal systems and external vendors has effectively vanished. Supply chain cyber attacks affected 82% of surveyed firms in the last 12 months, demonstrating that the traditional approach to third-party risk management has reached its functional limit.

The Visibility Paradox

While 91% of sector leaders prioritise supply chain risk as a top-tier concern, only 28% of institutions possess "Excellent" visibility into their Nth-party dependencies, where many of today's risks reside. This opacity constitutes a systemic vulnerability that regulators are no longer willing to tolerate. Following the implementation of the FCA's and PRA's Operational Resilience rules, including the Critical Third Party (CTP) regime, and DORA, the focus has shifted from individual firm resilience to the stability of the entire financial sector's supply chain ecosystem.

Closing the Regulatory Gap: Compliance vs. Resilience

A primary objective of the new operational resilience regime is to allow regulators to obtain exhaustive data on firms' wider supply chain dependencies—extending deep into the layers of subcontractors and lower-tier suppliers. The implicit goal is to map the wider ecosystem and identify concentration risks and systemic single points of failure before they can be exploited.

However, the industry cannot afford to wait for regulators to achieve this birds-eye view. As demonstrated by a collaborative project of 6 financial institutions with Risk Ledger, firms can take a more proactive approach today. By collaborating with peers and overlaying supply chain maps, institutions can not only achieve real-time visibility and identify shared risks to stay far ahead of the regulatory curve, transforming TPRM from a reactive compliance exercise into a dynamic, proactive defence, they can also reduce resource spend and scale their TPRM programmes.

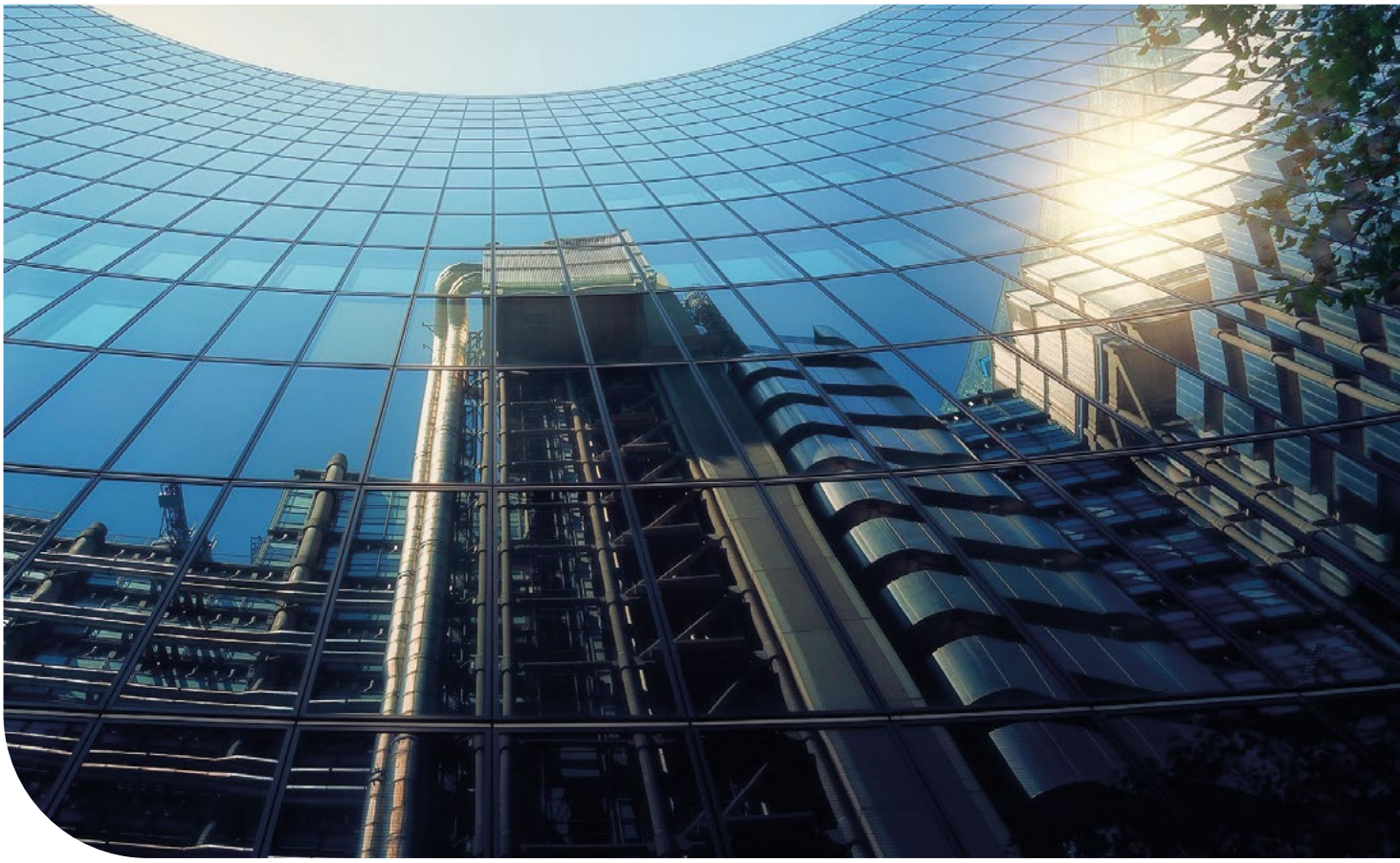
Key Takeaways

- **The Scale of Failure:** With 82% of firms impacted by supply chain breaches, traditional TPRM is increasingly found wanting.
- **The Visibility Deficit:** 72% of the sector are lacking the Nth-party visibility required to map dependencies supporting Important Business Services (IBS).
- **Regulatory Imperative:** New UK legislation mandates a move toward continuous monitoring and deep-tier supply chain mapping.
- **Collective Defence:** Collaboration and collective defence with peers is the only mechanism to reveal hidden concentration risks before they cause national disruptions.

Next Steps for Resilience

To meet the 2026 regulatory standards and secure the UK financial frontier, the report recommends three immediate actions:

1. **Prioritise Security Team Integration:** Move beyond procurement-led questionnaires by establishing direct, recurring touchpoints between your internal security operations and the security leads at critical suppliers, treating suppliers not as potential risk factors but as an extension of your own security teams. This "fast-track" relationship is the only way to ensure rapid triage and effective remediation when an incident occurs.
2. **Proactive Ecosystem Mapping:** Do not wait for regulatory mandates; utilise collaborative platforms to overlay supply chain maps with peers and identify systemic single points of failure.
3. **Adopt a "Defend-as-One" Strategy:** Engage in cross-industry data sharing between TPRM, security, compliance and threat intelligence functions to transform TPRM into an active cyber defence discipline.



Introduction

The UK financial sector serves as the indispensable backbone of the national economy, with the City of London, a global financial powerhouse that processes trillions in transactions and serves as a critical hub for international capital, at its strategic heart. However, this global prominence has placed the sector directly in the crosshairs of increasingly sophisticated adversaries. In 2026, the threat landscape is no longer shaped solely by opportunistic cyber criminals; it is defined by deepening geopolitical crises and the systemic fragility of a hyper-connected supply chain ecosystem.

For financial institutions, the continuing shift toward cloud-based services and a heavy reliance on Information and Communication Technology (ICT) as well as a few critical financial infrastructure providers has created a complex and interconnected web of dependencies and rendered traditional "moat-and-wall" defence models obsolete. Attackers now recognise that the most effective route to a well-defended target is through its less-visible suppliers, exploiting a single breach to potentially reach multiple high-value victims.

The SolarWinds attack has driven home the inherent dangers in our interconnected modern supply chains. As a direct result of the attack, the New York State Department of Financial Services (NY DFS) saw a potentially major threat to the financial system at large and thus immediately required all New York financial institutions to report any impacts the attack had on them. While this attack drew a lot of attention because of its massive "blast radius", there are hundreds of other attacks against the financial services industry through their supply chains each year that receive far less attention. For instance, the 2024 ransomware attack against ION Trading Technologies' cleared derivatives unit. The attack forced ION to take its systems offline, resulting in financial institutions suddenly having to manually confirm trades, causing ripple effects and reporting delays across the sector.

The stakes have been raised further by a stringent new regulatory environment. The UK's Operational Resilience Rules (PS21/3, SS1/21, SS2/21 and most recently PS7/26) and the EU's Digital Operational Resilience Act (DORA) have moved expectations from high-level guidance to rigorous mandates. As of 31 March 2025, firms are required to have mapped their "important business services" and the chain of third and nth-party dependencies necessary to deliver them, ensuring they can remain within tolerable impact levels during severe disruptions. Moreover, these regulations are no longer just aimed at strengthening the operational resilience of individual firms, but of the entire financial sector.

This report thus sets out to examine the state of supply chain cyber security in financial services in the UK, investigating whether traditional risk management practices are evolving fast enough to secure every link in the sector's intricate supply chain ecosystem, or if a fundamental shift in approach is required to safeguard the City of London's and wider financial services sector's continued role as an engine of growth and global financial stability.

Section 1: The Rise of Supply Chain Attacks

1.1. Section Overview

While financial services firms commonly have strong cyber defences in place, not least because of the stringent compliance and regulatory requirements the industry has to meet, there remains a clear weak spot: their extended supply chain dependencies.

The integration of more and more new technologies and external partners and vendors has created a web of dependencies that are both opaque and vulnerable to exploitation by threat actors. Supply chain attacks represent an indirect but highly effective pathway to compromising critical economic infrastructure. Rather than attacking a well-defended tier-1 bank or major insurer directly, threat actors increasingly opt to compromise their critical suppliers—such as a fintech startup, a software vendor, or an IT managed service provider—to gain access to their ultimate target's network or data. Supply chain attacks have thus become a defining feature of the modern threat environment, and are aimed at not only direct suppliers but also the extended network of service providers and subcontractors that underpin the financial services industry.

This section evaluates the scale of the threat facing the industry today, analysing the prevalence of supply chain incidents and the structural vulnerabilities and headwinds the sector is facing.

1.2. The Scale of the Threat Facing the UK Financial Sector

According to the European Union Institute for Network and Information Security's (ENISA) latest finance-sector threat-landscape report (2025), supply-chain attacks are a "key and growing vector" for the sector, as attackers increasingly abuse third-party providers and integrators to reach multiple institutions at once. ENISA's research found that most commonly, supply chain attacks impact financial institutions in the form of exposure and sale of sensitive data (63%), followed by operational disruption (26%), and trailed by financial loss (11%).

In parallel, the World Economic Forum's Global Cybersecurity Outlook 2026 highlights third-party and supply-chain compromises as one of the fastest-rising sources of cyber risk globally, with financial services among the most exposed sectors.

82%

of surveyed financial services firms have experienced 1 or more supply chain incidents in the past year while 56% experienced 2 or more.

According to our own research, involving cyber security and TPRM leaders across UK financial institutions, 82% of surveyed firms experienced at least one supply chain incident in the past 12 months, with 56% suffering two or more incidents, and nearly one in ten (9%) experiencing three or more. The scale of the challenge has fundamentally altered the perceived threat landscape. Today, 91% of respondents rank supply chain cyber incidents among their top three cyber security concerns.

The risks appear concentrated in specific categories of suppliers. Our survey findings point to IT service providers (44%), such as MSPs and software vendors, as the most vulnerable parts in the supply chain. This is followed by operational technology (18%) and cloud/SaaS providers (12%), reflecting a deep-seated concern that the very tools used for digital transformation are becoming the primary vectors for enterprise cyber risk.

1.3. The Threat Is No Longer Limited to Critical Third Parties

Moreover, the problem with supply chain incidents goes well beyond direct third-parties. As attacks such as Solarwinds, MOVEit Transfer and many others have demonstrated, in many cases, the initial breach that impacted firms and their customers did often not even originate in a direct third-party, but in a 4th party that a critical third-party relied on.

When threat actors, for example, exploited a zero-day vulnerability that was discovered in the file transfer software, they also exfiltrated large amounts of data handled by a company called PBI Research Services, a leading research service provider used by many financial institutions to determine whether their account holders are still alive, or to find beneficiaries. This research provider had used MOVEit Transfer to process its clients' customer data, hence also directly impacting the financial services firms it served as well.

Another example of fourth-party impacts during the MOVEit attack is the case of Zellis, a UK payroll services provider. Only days after Progress Software had published its notice about the discovery of a zero-day vulnerability in its MOVEit Transfer software, it began to emerge that Zellis had confirmed a data breach through their use of the software. Zellis also announced that eight of their clients had been impacted as well. The affected parties included the BBC, British Airways, Boots and DHL, among others.

These examples demonstrate that without greater awareness of what is happening further down the supply chain, it becomes almost impossible to anticipate potential threats that might suddenly surface at 4th, 5th or 6th parties and beyond, but then ripple up and come to affect a financial services firm directly.

1.4. Geopolitics as a Strategic Driver

The situation is further complicated by a rapidly worsening geopolitical situation and is inextricably linked to the broader fracturing of the global order. The National Cyber Security Centre (NCSC) and other bodies have noted that the wars in Ukraine and shifting alliances have emboldened threat actors to explicitly target Western financial systems. The emergence of groups such as the 'DarknetParliament'—a coalition involving KillNet, REvil, and Anonymous Sudan—signalled a new era of cyber aggression. Their coordinated campaigns in 2023, such as those announced under 'Decision No. 0191,' specifically aimed to attack the foundational pillars of international finance, including SWIFT, IBAN, and SEPA messaging protocols. For the UK financial sector, these tensions translate into a "live-fire" test of operational resilience.

While ransomware gangs motivated by financial gain remain a persistent nuisance, the primary concern for the UK financial sector is increasingly becoming the rise of sophisticated, state-sponsored adversaries. For these actors, the motive shifts from simple extortion to strategic sabotage, disruption, and pre-positioning within the global financial architecture.

1.5 Key Takeaways

The shift from static perimeter defence to a geopolitically charged era of supply chain threats represents a definitive turning point for the UK financial sector. As institutions move toward cloud-native architectures and explore more sovereign digital alternatives, they aren't just upgrading technology; they are fundamentally expanding their attack surface into a sprawling, ecosystem of third-party providers. The industrialisation of supply chain attacks—where a single software flaw can paralyse multiple systemic institutions—means that individual resilience is now entirely dependent on the security of the wider supply chain network.

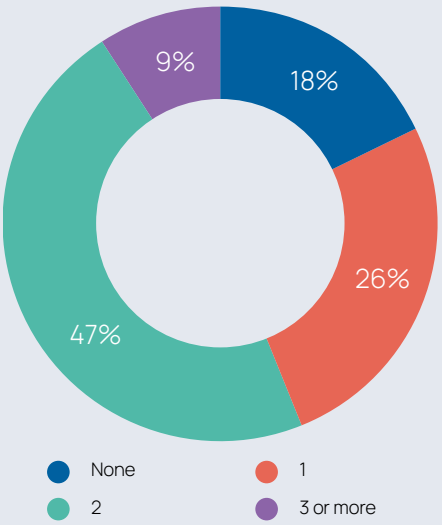
Furthermore, the drive for digital sovereignty and international conflicts such as in Ukraine or Iran introduce significant "transition risk." Decoupling from global dependencies in favour of domestic or at least alternative "friend-shored" infrastructure creates new and largely unknown threats. In this environment, supply chain security is becoming a battleground for national resilience. With nation-state threat actors shifting their focus from financial gain to strategic sabotage, the UK financial grid has become a Tier-1 target for those seeking to degrade public trust and economic stability.

91%

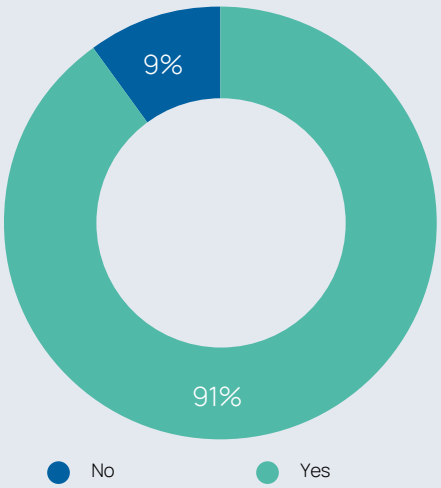
of respondents-rank supply chain cyber incidents among their top three cyber security concerns.

Survey Results

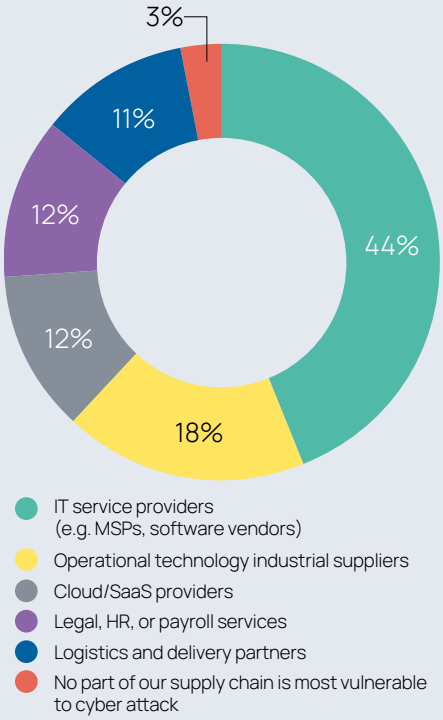
Q1. In the past 12 months, how many cyber security incidents have you experienced in your supply chain?



Q2. Do supply chain cyber incidents rank among your top three areas of concern for 2025?



Q3. Which part of your supply chain do you consider the most vulnerable to cyber attack, if any?



Section 2: Is Third-Party Risk Management Fit for a New Era of Supply Chain Threats?

2.1. Section Overview

The escalation of supply chain attacks amidst an increasingly complex geopolitical environment raises a fundamental question: is the prevailing methodology of Third-Party Risk Management (TPRM) still an effective bulwark against modern cyber threats emanating from organisations' supply chain dependencies? The persistent rise in organisations and entire industries being impacted by supply chain incidents suggests that there might be inherent, structural flaws with the traditional TPRM model.

The core paradox lies in the scope of the task: while organisations rightly prioritise the security of their own internal applications, people, and governance, TPRM effectively requires them to apply the same level of rigour to their hundreds or even thousands of external suppliers and partners as well. Using current methodologies, this has become a seemingly impossible mandate. Traditional TPRM, whether using manual spreadsheets or digital tools, remains, in essence, a point-in-time compliance-driven, one-to-one assurance exercise that is siloed and can't be easily scaled.

As firms pivot to meet the "non-delegable" accountability standards of the Bank of England's (BoEs), Financial Conduct Authority's (FCAs) and Prudential Regulation Authority's (PRAs) Operational Resilience rules, and the EU's Digital Operational Resilience Act (DORA), the gap between what traditional TPRM can deliver and the requirement to achieve genuine operational resilience has become wider and wider.

The second section of this report will investigate whether there are inherent flaws with traditional TPRM that prevent it from producing better security outcomes.

2.2. Third-Party Risk Management Under Scrutiny

56%

of surveyed professionals described TPRM as only somewhat effective in reducing supply chain risks.

Our survey data reveals a sector that is increasingly skeptical of its existing risk management toolkit. When asked about the effectiveness of traditional TPRM in mitigating modern supply chain cyber risk, professional confidence is lukewarm at best. While 42% of respondents consider their TPRM programme as "very effective", 56% described TPRM as only somewhat effective, with 2% rating it as "not very effective". The core dilemma is that TPRM, while meeting compliance requirements, often fails to translate into stronger security or resilience against supply chain attacks because occasional supplier assessments are detached from real-time operational risks.

One of the leading technical deficiencies identified by industry professionals is the pervasive "Monitoring Gap". The survey insights reveal the stark inadequacy of point-in-time risk assessments, with currently only 40% of organisations performing continuous monitoring of their critical suppliers, with the remainder relying on quarterly (28%), biannual (18%), or even just annual (12%) review cycles.

There is also a strong likelihood that the fairly high number of respondents claiming to have the ability to continuously monitor their critical suppliers might have based this assessment on their organisations utilisation of external scanning tools. While external scanning tools can assess a vendor's public-facing perimeter, they remain blind to internal hygiene factors—such as network segmentation, privileged access management, and employee training—that are critical for preventing lateral movement during an attack. This is why 38% of practitioners pointed to the inability to continuously monitor a supplier's internal security controls as a key shortcoming of traditional TPRM. This "Point-in-Time" problem creates extensive windows of invisibility, during which a new vulnerability, new shadow IT or a configuration error can remain undetected until they are exploited.

Another key weakness, as identified by 40% of respondents, is the lack of collaboration and information sharing with industry peers. This suggests that the tradition of siloed defence is now rightly viewed as a barrier to identifying sector-wide threats and achieving enhanced resilience.

Perhaps most crucially, however, 35% of the sector identified a lack of visibility into deeper supply chain dependencies (Nth-parties) as a key shortcoming, leaving firms exposed to risks buried deep within their digital dependencies.

2.3 Key Takeaways

As the frequency and impact of supply chain attacks continue to escalate, it has become evident that traditional Third-Party Risk Management (TPRM) frameworks are structurally ill-suited to defend against the modern threat landscape. Historically built as a one-to-one, compliance-driven exercise, legacy TPRM fundamentally struggles to scale to the reality of today's deeply interconnected digital ecosystems. The core dilemma is that standard TPRM practices prioritise checking regulatory boxes over establishing genuine operational resilience. Because these assessments are generally static and detached from real-time operational risks, they create a false sense of security.

Industry practitioners recognise that these foundational flaws cannot be resolved simply by throwing more headcount or budget at the problem. The methodology itself is restricted by severe monitoring gaps, a lack of deep-tier visibility, and an over-reliance on siloed defences. As regulatory bodies introduce stricter mandates—such as DORA and the new UK operational resilience rules—requiring continuous, automated, and comprehensive assurance, it is clear that TPRM must evolve from a reactive compliance function into a dynamic, continuous, and collaborative cyber defence discipline.

- **The Compliance Illusion:** Traditional TPRM is predominantly a compliance-focused exercise that often fails to translate into stronger security outcomes, as annual or periodic questionnaires do not reflect real-time operational risks.
- **The Dangerous Monitoring Gap:** Relying on point-in-time assessments creates extensive windows of invisibility. With only 40% of the sector performing continuous monitoring on critical suppliers, the majority of firms are essentially blind to vulnerabilities, shadow IT, or configuration errors that emerge between review cycles.
- **Internal Control Blindspots:** Current methodologies struggle to evaluate a supplier's internal security hygiene. While external scans can view the public perimeter, they miss critical internal controls—like network segmentation and privileged access management or shadow IT—that are vital for preventing an attacker's lateral movement.
- **Lack of Collaboration:** Traditional risk management is a siloed, localised effort. A lack of collaboration and information sharing with industry peers prevents organisations from seeing the broader threat picture and identifying systemic vulnerabilities.

Key TPRM Shortcomings:

58%

of surveyed organisations don't continuously monitor the security of their critical suppliers.

40%

of respondents identified the lack of collaboration and information sharing with industry peers as a major shortcoming.

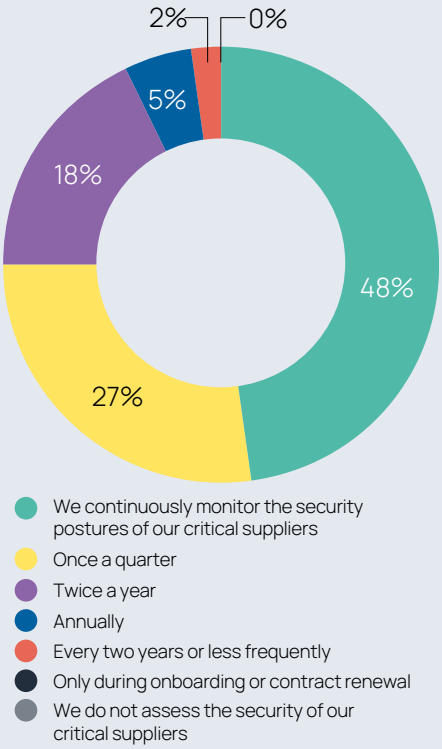
35%

of the sector identified a lack of visibility into deeper supply chain dependencies (Nth-parties) as a key shortcoming.

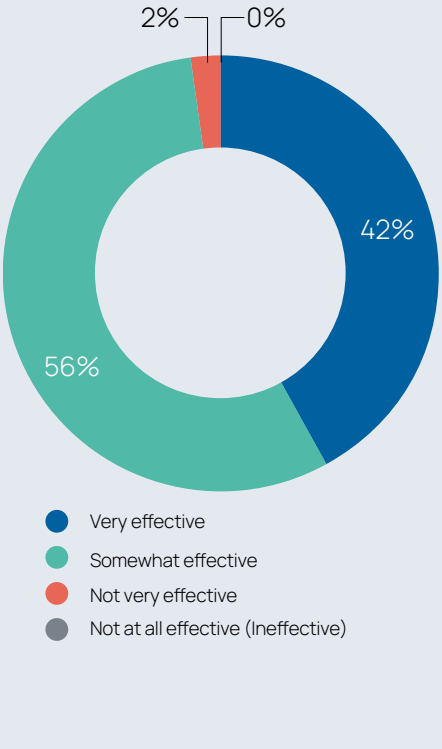
- **An Unscalable Approach:** The inherent limitations of static, one-to-one assessment models cannot be fixed simply by increasing financial resources or human capital.

Survey Results

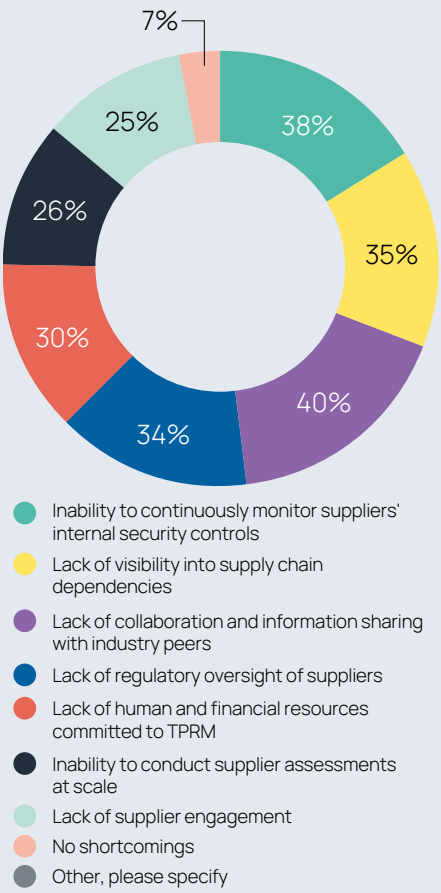
Q4. How often do you conduct security assessments of your critical suppliers?



Q5. How effective, if at all, do you believe traditional third-party risk management (TPRM) is in reducing supply chain cyber risks in 2025?



Q6. What, if anything, are the biggest shortcomings of your current TPRM programme? (Select up to 3)



Section 3:
Supply Chain Visibility, Important Business Services and Concentration Risks in the Financial Services Industry

3.1. Section Overview

The findings of the previous chapters indicate that while the worsening threat landscape and the structural limitations of legacy TPRM are well-documented, the persistent opacity of the extended supply chain represents the sector's primary systemic risk exposure.

As financial institutions transition from managing contracts and direct suppliers' security postures to grappling with the complexity of today's intricate and interconnected digital ecosystems, the risk has effectively migrated into the opaque layers of 4th, 5th, and Nth-party environments.

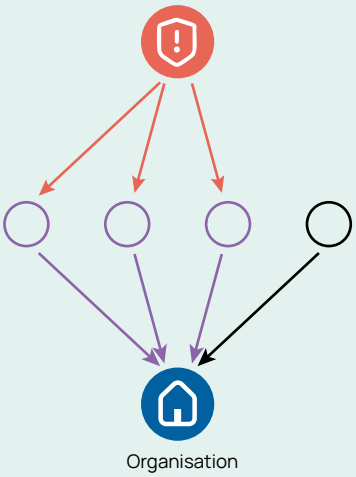
This section argues that the sector has reached a visibility plateau: as a result of this lack of visibility into their extended supply chains, firms are unable to identify concentration and systemic risks, or even to fully map all the nth-tier dependencies that support their Important Business Services, although this is something that regulators now expect.

3.2. What are Concentration Risks

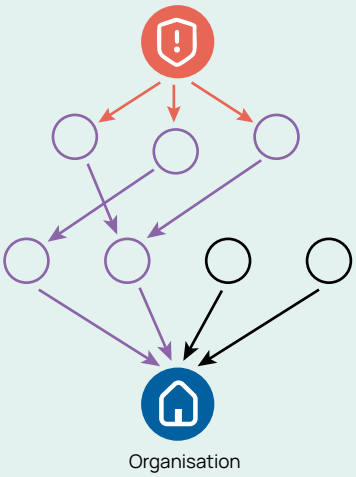
There are different types of concentration risks. Concentration risks can arise when a single organisation relies too heavily on one particular supplier for several business critical services, or when several critical direct suppliers of an organisation all depend on the same fourth-party provider for a critical service or function. It is these dependencies that can introduce single points of failure, i.e. when a disruption at this supplier could cascade rapidly, impacting operations far beyond the immediate contractual relationship. Systemic concentration risks, meanwhile, are an extension of concentration risks facing individual organisations. They stem from shared suppliers, whose disruption would have a cascading impact across multiple organisations within the financial services industry.

The industry's reliance on a relatively small number of key technology providers, data processors, and service partners amplifies the impact of such concentration risks.

Individual Concentration Risks

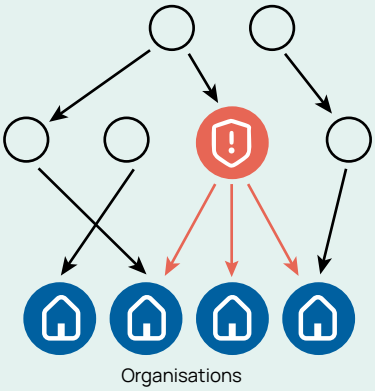


4th-party concentration risk

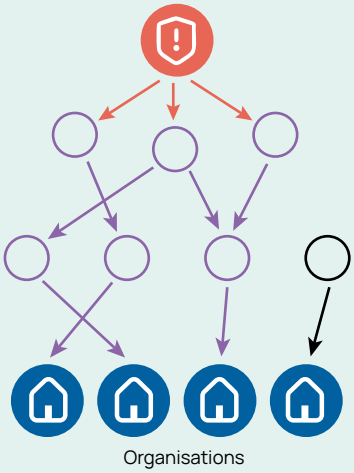


5th-party concentration risk

Systemic Concentration Risks



3rd-party systemic risk



5th-party systemic risk

3.3. Regulators focus on systemic resilience

While 81% of industry respondents confidently assert their ability to identify these risks, the reality is that such risks are often obscured within deeper-tiers in organisations supply chains, where such concentration risks often reside.

Regulators increasingly recognise how suppliers can also represent systemic risks, especially for sectors like finance and critical national infrastructure, where an incident at a widely shared supplier could lead to a domino effect impacting an entire sector. For instance, the FCA's FG 16/5 explicitly requires firms to "monitor concentration risk and consider what action it would take if the outsource provider failed." Similarly, the EU's Digital Operational Resilience Act (DORA), under Article 25(5), expects entities to assess whether contractual arrangements might "reinforce ICT concentration risk," while the Prudential Regulatory Authority (PRA) demands comprehensive documentation to enable authorities to supervise these aggregate systemic risks.

3.4. The Importance of Supply Chain Visibility

In order to be able to identify concentration and systemic risks, however, enhanced visibility into extended supply chain dependencies is key. As the UK Government Cyber Security Strategy (GCSS) correctly observed, "visibility is the foundation from which an accurate assessment of risk can be derived". Without this foundation, the "central mapping" required to understand dependencies on critical and shared suppliers remains incomplete, leaving the sector vulnerable to incidents that could simultaneously paralyse the nation's ability to conduct real-time settlements or manage liquidity.

The foundational importance of enhanced visibility is thus a core pillar of modern resilience. Despite a high awareness of this necessity, a significant "Reality Gap" persists: only 28% of survey respondents claim to have "Excellent" or full visibility across all tiers of their extended supply chain. The majority (63%) possess visibility only into their most critical 4th parties, while 9% operate with limited insight that does not extend beyond their direct contractual partners. This is a critical shortcoming because, as the GCSS highlights, only an "improved understanding of suppliers and their dependencies will… enable [entire sectors of the economy] better respond to cyber security incidents that emanate from the supply chain."

Moreover, to move from individual risk awareness to enhanced sectoral resilience, the UK financial sector must embrace the spirit of the new operational resilience rules in the UK and EU, which treat critical third parties as well as their critical suppliers all as an extension of the institution's own infrastructure. This requires shifting the focus from "who we contract with" to "who is touching our Important Business Services" regardless of their position in the supply chain. By adopting the "central mapping" approach advocated by the UK government, the industry can identify the systemic and aggregate supply chain risks that individual firms, acting in isolation, simply cannot see.

72%

of surveyed organisation don't have sufficient visibility beyond their critical third parties.

Concentration Risks - A View from the Industry

In this interview with Risk Ledger, Yohann Le Grand, Senior Security & Resilience Manager at Schroders Personal Wealth (SPW) provides an industry perspective and elaborates on the importance of uncovering concentration risks in the supply chain for financial services firms, and offers his thoughts on the role collaboration with peers can play in addressing this challenge collaboratively.

1. **How important do you think is the ability to identify individual concentration risks for organisations to achieve better supply chain security and operational resilience?**

   Identifying concentration risks is key to evaluating and preparing for the potential impacts of a disruption at a critical 4th party.

2. **How important is it in your opinion to identify shared systemic risks facing your wider industry, and who should be responsible for identifying and addressing them, e.g. individual organisations, regulators or others?**

   Identifying the systemic risk is really important as all organisations, both within and outside the industry, are interlinked through banking services at the very least. Individual organisations should already have identified, evaluated, and prepared for risks from individual third parties as part of their supply chain management activities. Maintaining good resilience at an individual level plays a major part in minimising systemic risk. However in most cases, only industry-level associations have enough combined resources and adequate information sharing guardrails in place to efficiently identify actual systemic risks, agree actions and, with the help of regulators, influence large players in the supply chain.

3. **Do you think current regulatory frameworks adequately address concentration and systemic risks in supply chain cybersecurity? What improvements would you suggest?**

   In the UK, current regulatory guidance (e.g. CQUEST) is focussed on the responsibilities of individual financial services companies. In the EU, DORA is going some way to improve supply chain resilience. Industry associations should leverage this to develop a common response to systemic risks.

4. **What actions do you currently take on the back of any concentration risks you can identify in your extended supply chains, i.e. do you work with your critical suppliers to better understand the role and importance of concentration risk suppliers to them, and learn more about specific risks that might emanate from them?**

   We routinely ask our critical suppliers to confirm who their critical suppliers are with a view to both identify concentration risks and perform some due diligence on these subcontractors where necessary. This allows us to understand potential impacts more accurately and refine our operational resilience accordingly.

5. **What additional contextual information on potential concentration risks would be useful to make information more actionable for you in the future?**

   There are two things we need: 1) information about who the subcontractors/Nth parties are, and 2) information about what their resilience/security posture is like.

6. **Can you think of ways for how, in the future, it might be possible to identify potential attack paths based on the criticality of services provided down the chain from a possible concentration risk at a 5th degree level or higher into 4th parties, 3rd parties and organisations themselves?**

   Absolutely, as long as we can get the visibility of the deep supply chain. Inadequate contractual limitations can unfortunately hinder that process which is where regulation such as DORA is beginning to help, but more needs to be done from both a regulatory and industry angle.

7. **Which role do you envision enhanced collaboration with industry peers to play in order to better identify and mitigate concentration risks and achieve better supply chain security and operational resilience more generally, and how could you envision such enhanced collaboration to look like?**

   Proactive information sharing about supply chains, contracts and regulation allowing, is the key to enabling the industry to better and more easily identify and manage its concentration risks. The work that Risk Ledger and FS-ISAC are doing is a start. However, industry peers need to continue to work much more closely to assert greater influence over third and Nth parties so we are able to obtain and share information about their security and resilience.

8. **Does the TPRM team or role in your organisation regularly collaborate with your threat intelligence and operational resilience teams?**

   Absolutely, our information security and TPRM functions are in constant communication.

9. **How often does your TPRM team or function collaborate with industry peers or participate in information-sharing initiatives with industry peers related to supply chain security?**

   We are part of several information sharing organisations within our industry and we interact with them daily

10. **Could you give us 3 ideas for how organisations could more effectively identify and address concentration risks in their supply chains in the future?**

    1. Adequate contractual clauses so information about subcontractors can be obtained.
    2. An adequate system to capture this information.
    3. Industry collaboration, particularly in terms of threat intelligence/information sharing, but also lobbying organisations in the shared supply chain who may not engage with peers on an individual basis.

3.5 Key Takeaways

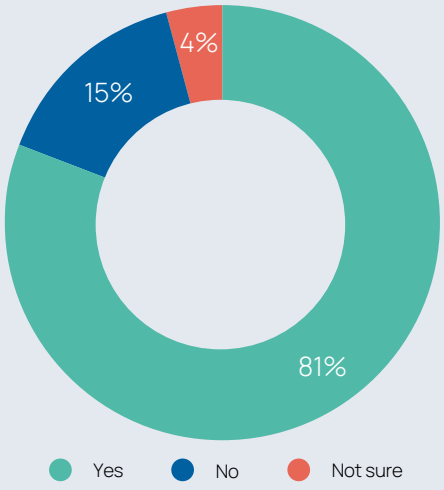
The modern financial threat landscape has fundamentally shifted. Cyber risks are no longer confined to direct, critical third-party providers, but have migrated deep into the opaque layers of fourth, fifth, and nth-party extended supply chains. Regulators have recognised this escalating complexity and are recalibrating their approach to focus on the continuity of Important Business Services. Under new operational resilience frameworks, regulated entities bear the responsibility for securing not just their direct suppliers, but the entire underlying chain of dependencies that support these critical functions. This includes the critical mandate to identify hidden concentration risks—such as a primary and backup supplier relying on the exact same fourth party—which could trigger simultaneous, cascading failures across an organisation's operations.

However, a severe "visibility gap" prevents most organisations from achieving this; traditional risk management leaves firms blind to the complex dependencies residing at the fourth-party level and beyond. Recognising this systemic fragility, regulators are now expanding their mandate from individual corporate resilience to the stability of the entire financial sector. By demanding exhaustive data on deep-tier dependencies from regulated entities, regulatory bodies aim to centrally map the wider supply chain ecosystem. This macro-level visibility is designed to expose shared systemic risks and single points of failure that individual firms, acting in isolation, cannot see, ultimately shifting the industry toward collective resilience.

- **The Nth-Party Threat Landscape:** Cyber risk has effectively migrated beyond direct third-party relationships into the deeper, less visible tiers (4th, 5th, and Nth parties) of the extended supply chain ecosystem.
- **Service-Led Accountability:** Compliance is no longer just about assessing direct vendors; firms must map and secure the entire chain of third and nth-party dependencies necessary to deliver their Important Business Services.
- **Concentration Risks:** Organisations must actively identify potential single points of failure hidden deep within their supply chains, such as instances where both primary and backup suppliers rely on the same fourth party, rendering traditional incident response plans ineffective.
- **The Visibility Deficit:** A significant operational gap exists, as most organisations currently lack the comprehensive visibility required to map dependencies and evaluate the security postures of entities beyond their direct third parties.
- **The Shift to Sectoral Defence:** Regulators are transitioning from focusing on the resilience of individual firms to the stability of the entire financial sector. To achieve this, regulators are using new operational resilience rules to extract exhaustive supply chain data, with the ultimate goal of mapping the wider ecosystem and neutralising systemic single points of failure.

Survey Findings

Q7. Concentration risks occur when several of your critical suppliers rely heavily on a specific 4th party (this dependency could also appear further down the supply chain). Can you currently identify such risks in your supply chain?

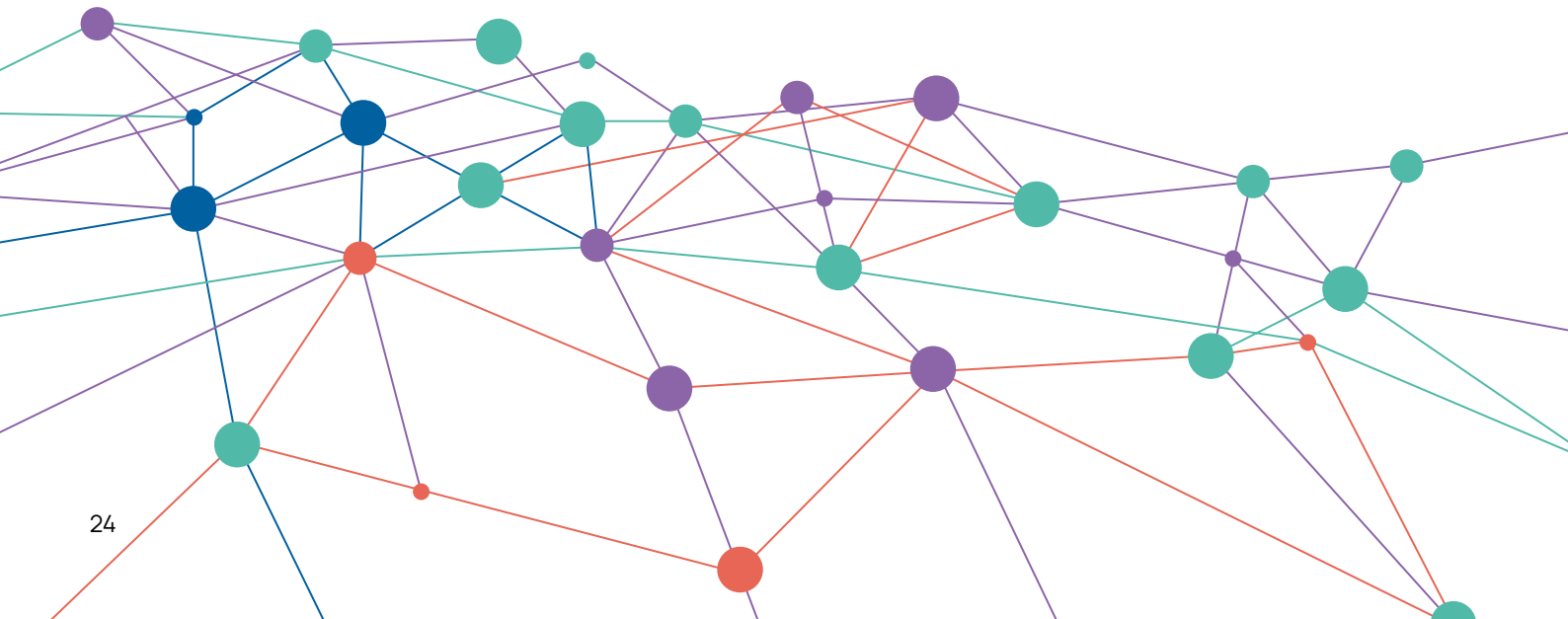


Q8. Which of the following best describes your visibility into supply chain dependencies, beyond your immediate third-parties?

Section 4: How Collaboration Can Transform Supply Chain Resilience

4.1. Section Overview: Moving Toward a "Defend-as-One" Strategy

The systemic nature of the supply chain threat implies that individual resilience is no longer a sufficient defence for the UK financial sector. If a multitude of banks, insurers, and payment providers rely on the same critical technology suppliers, they are essentially sharing the same risks. This section argues that enhanced collaboration is the only viable mechanism to solve the systemic visibility crisis inflicting the financial sector. By moving towards a "Defend-as-One" model, however, the sector can leverage shared platforms to turn isolated, repetitive risk assessments into collective, real-time risk intelligence. This approach recognises that in a highly interconnected Critical National Infrastructure (CNI) environment, a vulnerability in one link in the extended and interlocking supply chain is a vulnerability for all.



4.2. The Current State of Collaboration: Bridging the Frequency and Data Gaps

Collaboration between industry peers is increasingly recognised as becoming essential to effectively manage cyber security risks and enhance sectoral resilience. No single financial services company, regardless of size or sophistication, can address these challenges in isolation.

By sharing insights, threat intelligence, and best practices, organisations can gain greater visibility into potential vulnerabilities and identify systemic concentration risks, build collective resilience, and respond faster and more effectively to evolving cyber threats. Fostering stronger partnerships and open communication across the industry can help transform supply chain security from a fragmented challenge into a unified defence strategy.

The transition to utilising collaborative supply chain security platforms allows for the secure aggregation of supply chain data, which can automatically generate a deep-tier map of the UK financial ecosystem's dependencies. This collective mapping instantly reveals concentration and systemic risks that would otherwise remain invisible to individual firms working in isolation. When a new weakness emerges in the defences of a specific specialised software provider, a collaborative defence platform also allows the entire sector to instantly identify shared exposure and coordinate a unified, rapid response.

Despite the clear benefits, current collaborative efforts within the UK financial sector remain inconsistent and primarily reactive. Our survey data reveals a significant "Collaboration Gap": only 43% of organisations engage regularly with their peers on systemic risk identification, while a vast 55% do so only occasionally and 2% rarely or never collaborate with their TPRM colleagues beyond their own institutional boundaries. While the exchange of threat intelligence with peers is maturing in many industries, the sharing of supplier risk intelligence—the technical assessment of whether a shared supplier is actually secure and insights into security control weaknesses—remains stagnant due to perceived competition concerns as well as technological and potential legal barriers.

55%
of respondents do not regularly collaborate with industry peers.

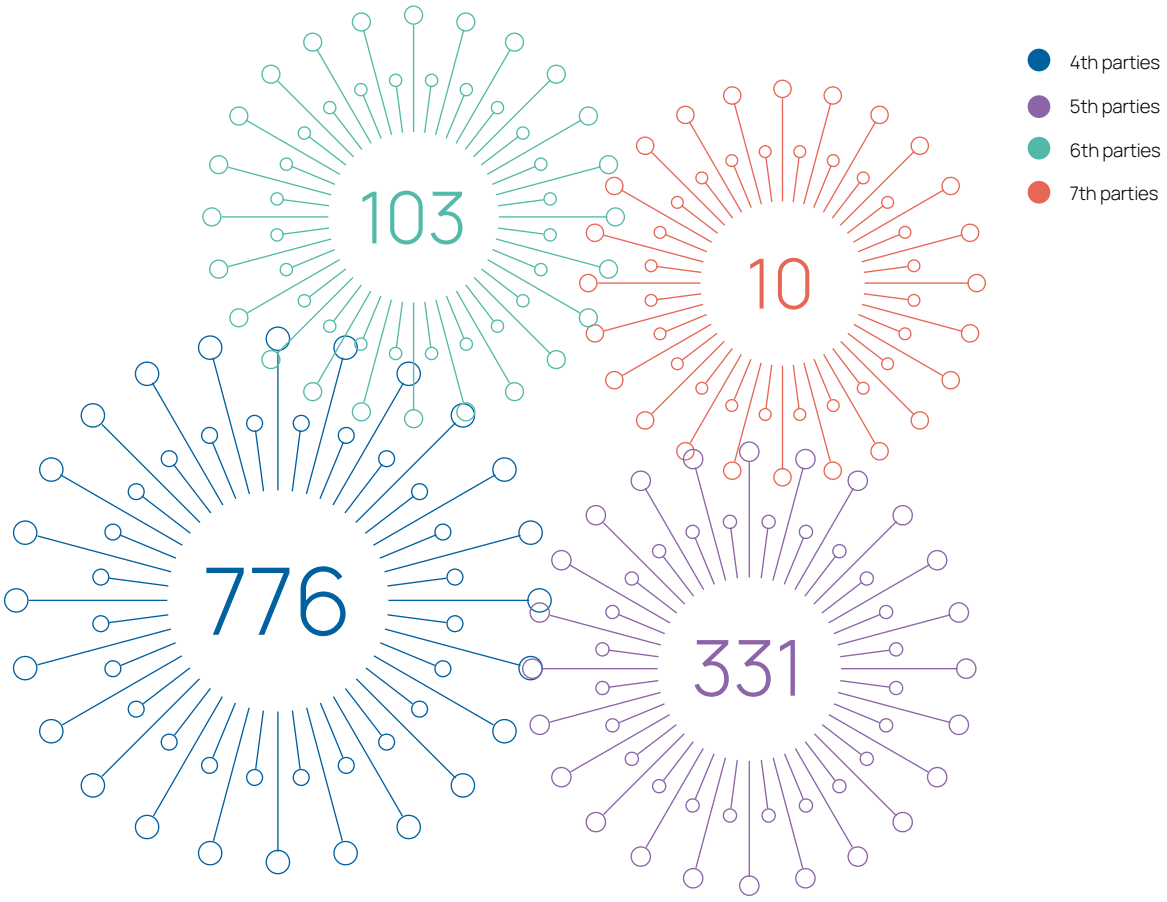
The industry itself is signaling a desire for change, with 42% of respondents advocating for the upcoming Cyber Security and Resilience Bill to provide greater incentives or even mandates for cross-industry collaboration and information sharing. This aligns with the legislative intent to recognise that a collective failure poses a stark national security risk, necessitating a coordinated response across CNI sectors.

4.3. Mapping Dependencies and Uncovering Concentration Risks in the Financial Sector

Across the UK's most critical sectors, some organisations are already embracing this new model of collective defence, working together to identify supply chain risks that no single entity could identify on its own. By leveraging Risk Ledger's collaborative supply chain security platform, organisations can now join forces with their industry peers to securely share their respective supply chain maps, best practices, and risk intelligence. This new ethos to Defend-as-One yields tangible results, as the following data from the Risk Ledger platform demonstrates.

In one such instance, Risk Ledger brought together a group of 8 of its financial services clients to form a community of peers on its platform to help them identify shared concentration risks and respond faster to emerging threats when they appear. By utilising Risk Ledger and overlaying their respective supply chain maps, the institutions gained unprecedented visibility into their extended supply chains, identifying not just shared direct suppliers but also 4th, 5th, and nth-party dependencies.

Based on an aggregate total of only 98 direct third-party supplier connections of these financial services clients, the platform was able to identify 1,220 further dependencies in their overlapping extended supply chains:



Most importantly, by overlaying their respective network maps on Risk Ledger, community members discovered:

92 potential concentration risks

62 of these were identified as potential risks at 4th parties and beyond.

14 of these were direct 3rd parties connected to at least 50% of all community members.

4.4. Key Takeaways

It is still common for organisations to assess each individual supplier on their own, so there remains a vast amount of duplicated effort across organisations when performing these reviews. By sharing information on their suppliers' security practices and controls, and then collaborating with peers across the industry on making the weakest nodes in the system stronger collectively, we can save a lot of time and resources. Even more importantly, it enhances the security of the entire ecosystem.

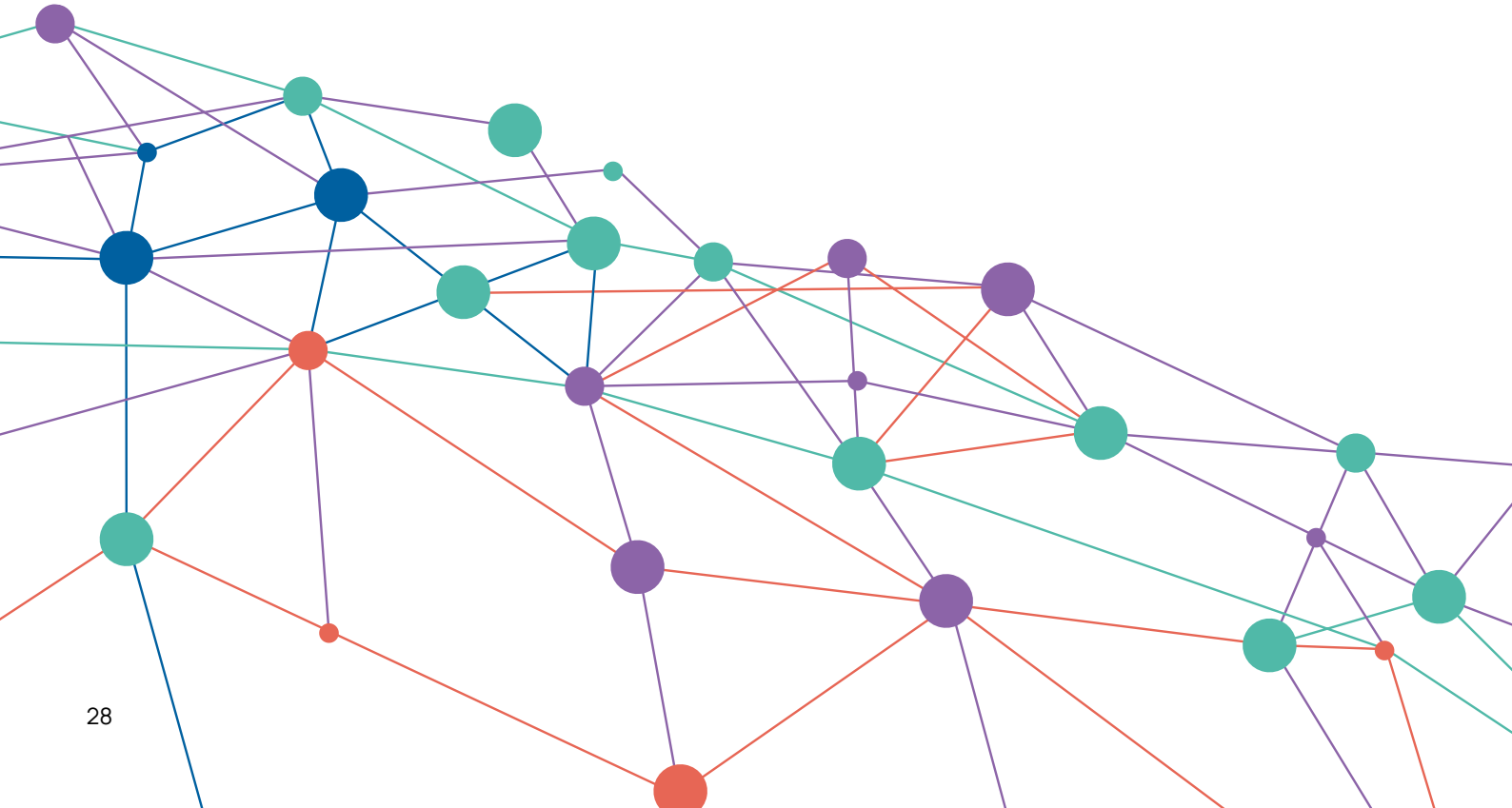
Also, with most Third-Party Risk Management programmes focusing on direct supplier relationships only, they miss the extended web of dependencies and shared vulnerabilities that exist across the industry and could become single points of failure. Greater collaboration with industry peers that often share substantially overlapping supply chains can overcome many of the current shortcomings with TPRM. Specifically, collaboration enables organisations to:

Share supplier assessments and risk data: reducing duplication and assessment fatigue, while improving the quality and consistency of risk information.

Map extended supply chain dependencies: visualising not just direct suppliers, but also fourth- and nth-party relationships, and identifying shared dependencies and single points of failure.

Identify and mitigate systemic risks: by aggregating data across multiple organisations, collaborating with peers can highlight emerging threats and vulnerabilities that have the potential to impact entire sectors.

Support regulatory compliance: by providing industry-wide visibility and audit trails, Risk Ledger's collaborative approach helps organisations and regulators meet the requirements of new operational resilience and cyber regulations.



Conclusions: Forging a Resilient Future for the UK Financial Sector

The UK financial services sector stands at a critical juncture, as traditional security paradigms are being outpaced by a new era of digital supply chain complexity and risk. As established throughout this report, the transition toward a hyper-connected digital ecosystem has coincided with intensifying geopolitical instability and a professionalisation of supply chain attacks. For many organisations, these external pressures, compounded as they have been by an increasing drive toward digital sovereignty, including in the UK and Europe, represent potentially existential challenges to sectoral resilience. Despite the sector possessing some of the most mature cyber security functions in the world, the results remain sobering; the continued prevalence and high frequency of successful supply chain incidents suggests that there are inherent flaws with traditional, questionnaire-driven Third-Party Risk Management (TPRM) approaches that cannot be resolved through the mere injection of additional capital or manpower.

As this report has found, the fundamental weakness plaguing the industry is a widespread lack of visibility amidst the exponential rise in the complexity of the sector's supply chain ecosystem. This "visibility gap" is particularly perilous because the threats to Important Business Services and the stability of the UK financial infrastructure do not respect contractual tiers; a vulnerability in a deep-tier subcontractor can propagate through the system with the same lethality as a direct supplier compromise. Regulators, including the Bank of England, the FCA, or the ECB have recognised this structural fragility, shifting their focus toward system-level resilience through frameworks like the Critical Third Party (CTP) regime and the wider Operational Resilience rules. These regulations aim to map the wider ecosystem and identify the single points of failure that could trigger a cascade of operational paralysis.

However, the industry cannot afford to remain reactive while regulators build this capacity. Enhanced collaboration and the proactive sharing of supply chain intelligence offer the most effective path forward, as demonstrated by the successful application of the Risk Ledger network model within a group of financial services clients and within other CNI sectors. This new approach transforms TPRM from a reactive, point-in-time compliance exercise into an active cyber defence discipline. By collaborating with peers and overlaying supply chain maps, the UK financial sector can move beyond the "Compliance Trap" and build a proactive, coordinated defence capable of safeguarding not only individual organisations' resilience, but sectoral resilience and national economic stability in an increasingly hostile threat environment.

RISK LEDGER

Risk Ledger Ltd.
Adam House
7-10 Adam Street
London WC2N 6AA
United Kingdom

Company registration number (England & Wales): 10831970

Contact: www.riskledger.com | marketing@riskledger.com | +44 1234 567890