RISK LEDGER

Every Link Matters: The State of Supply Chain Security in Insurance — UK Edition

A Risk Ledger Data Insights Report

About this report

This report, "Every Link Matters: The State of Supply Chain Security in Insurance — UK Edition" provides a comprehensive analysis of supply chain security risks in the UK insurance industry, 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 | marketing@riskledger.com | +44 1234 567890

Foreword: Industry Perspective

Recent cyber attacks have sent a clear message throughout society — no organisation is immune from business disruption, and even established industry leaders can be brought to a standstill overnight. For insurers, these attacks represented a live-test of operational resilience, the state of regulatory preparedness, and the inherent trust model within third-party ecosystems.

As a CISO operating within the insurance industry, I have seen first-hand how emerging technologies, such as Cloud migrations, outsourcing, and GenAI can transform organisations. But these opportunities bring with them an expanding web of third-party relationships, each one posing a potential point of vulnerability, and even more so, silent aggregation points considered as concentrated entities which serve multiple organisations. Understanding where risks reside in this web is no longer optional, as demonstrated by the impacts following cyber attacks with software and vendor supply chains (e.g. Kaseya, MoveIT, Blue Yonder and many others). Regulatory imperatives have helped: under FCA and PRA operational resilience, in-scope organisations are required to identify their important business services and map the chain of dependencies that could cause severe disruptions.

However, this challenge extends beyond internal operations. When we consider the risk transferred to cyber insurance as a portfolio, understanding the external supply chain ecosystem becomes critical. Aggregation risk is no longer a theoretical concern — it is an under-examined exposure. A systemic supply chain event could trigger cascading losses across portfolios, highlighting the need for underwriting to incorporate supply chain visibility as a key data point.

Organisations have matured their third-party risk management processes to manage known entities, but few have taken the time to identify and contextualise who matters. To move forward, we must shift our mindset. Operational resilience in today's threat landscape requires greater collaboration, transparency, and information sharing. We need better processes to map the unknown, stronger signals to detect concentrated risk points, and a shared commitment to manage exposed visibility gaps. This report offers a timely and important perspective, and a call to action: only through collective insight can the insurance industry rise to meet the systemic challenges posed by supply chain risks.

Jay Vinda, Global CISO and Cyber Risk Engineering Lead, Mosaic Insurance

Preface:

The operations and functions of the UK insurance sector are increasingly dependent on third-party technology and services providers and other external partners that operate outside the industry's own confines. No longer simply a matter of policy wordings or actuarial precision, cyber risk has become a test of trust, resilience, and adaptability at every tier of the market.

A single supply chain attack has the potential to reverberate across the entire insurance ecosystem. The sector's deep interconnectivity — through Insurers, Delegated Authorities, Managing Agents, Coverholders, Brokers and service providers — means a compromise in any part of this vast supply chain ecosystem can quickly cascade, threatening not just clients but the operational resilience of the industry as a whole. The stability of the market is as dependent on its operational infrastructure as on its financial position; it's about the risk of core systems, underwriting platforms, or Delegated Authority networks being disrupted, with consequences that could undermine the sector's ability to function as the backbone of the UK economy.

Drawing on a survey of senior cyber security and third-party risk management professionals from across the UK insurance industry, it takes a hard look at the scale of the supply chain cyber risk in 2026 and the state of its defences. With the UK insurance sector representing such a significant pillar of the national economy, driving growth and stability even amid global uncertainty, the stakes could hardly be higher. The insights generated by this report are not just relevant — they are essential reading for anyone serious about safeguarding the future of the industry.

Ben Francis, Insurance Lead,
Risk Ledger

Contents

Introduction **6**

Section 1: The Rise of Supply Chain Attacks **7**

1.1. Section Overview 7

1.2. The Scale of the Threat Facing the UK Insurance Sector 7

1.3. Key Takeaways 8

Section 2: Is Third-Party Risk Management Fit for a New Era of Supply Chain Threats? **9**

2.1. Section Overview 9

2.2. Third-Party Risk Management Under Scrutiny 9

2.3. Key Takeaways 10

Section 3: Supply Chain Visibility, Important Business Services and Concentration Risks in the Insurance Industry **11**

3.1. Section Overview 11

3.2. What are Concentration Risks? 12

3.3. The Importance of Supply Chain Visibility 12

3.4. Key Takeaways 14

Section 4: How Collaboration Can Transform Supply Chain Resilience **15**

4.1. Section Overview 15

4.2. The Current State of Collaboration 15

4.3. Sharing Supply Chain Data Can Uncover Systemic Risks 17

4.4. Mapping Dependencies and Uncovering Concentration Risks in the Financial Sector 17

4.5. Key Takeaways 19

Conclusions **20**

Appendix: Survey Methodology **22**

Introduction

The insurance sector is undergoing a profound transformation as it navigates an era of unprecedented cyber complexity. In recent years, the convergence of digitalisation, heightened regulatory scrutiny, and the proliferation of third-party relationships has dramatically expanded the sector's attack surface. As the insurance community races to leverage new technologies and optimise their operations through external partnerships, they are simultaneously contending with an evolving threat landscape — one in which supply chain attacks are not only more frequent, but also more sophisticated and systemic in their potential impact.

This report, drawing on open-source intelligence and a dedicated survey of senior cyber security and third-party risk management professionals from across the UK insurance industry, explores the current state of supply chain cyber security in the sector. It examines the scale and nature of the threat, assesses the fitness of traditional third-party risk management (TPRM) practices, and considers the urgent need for enhanced collaboration and visibility to build sector-wide resilience. The findings reflect a sector at a crossroads: aware of the risks, yet still grappling with the complexity and inter-dependencies that define the modern supply chain ecosystem.

Section 1: The Rise of Supply Chain Attacks

1.1. Section Overview

The global cyber landscape has entered an era marked by escalating risk, not least due to heightened geopolitical conflicts and global realignments. For the global insurance industry, this complexity is acutely felt in their rapidly growing corporate and technology supply chains, where the integration of new technologies and external partners and vendors have created a web of dependencies that are both opaque and vulnerable to exploitation by threat actors. Supply chain attacks have become a defining feature of the modern threat environment, targeting not only direct suppliers but also the extended network of service providers, software vendors, and subcontractors that underpin insurance operations and portfolios.

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

90%

of respondents reported experiencing at least one supply chain cyber incident in the past year

The insurance sector's exposure to supply chain cyber risk is both significant and growing. In our survey, 90% of respondents reported experiencing at least one supply chain cyber incident in the past year, with 50% suffering two incident and 12% suffering three or more incidents — an alarming statistic that highlights the scale and persistence of the threat. This is consistent with broader industry research, which finds that 59% of breaches in the insurance sector originate from third-party vectors,[1] the highest rate across all sectors and more than double the global average.

The drivers behind this heightened risk are multifaceted. The insurance sector is characterised by extensive outsourcing, reliance on IT service providers, cloud and SaaS platforms, and a diverse array of legal, HR, and logistics partners as well as thousands of Coverholders for Lloyd's specifically. According to survey respondents, IT service providers (26%) and cloud/SaaS vendors (22%) are widely perceived as the most vulnerable points in the supply chain, closely followed by legal, HR, and

1 Security Scorecard, "Insurance Carriers Face Unprecedented Supply Chain Cyber Threats", https://securityscorecard.com/company/press/securityscorecard-report-59-of-breaches-impacting-insurance-sector-caused-by-third-party-attack-vectors/

payroll services (20%). The sector's interconnectedness, while enabling operational efficiency, also creates potential single points of failure that can be exploited by increasingly sophisticated threat actors.

94%

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

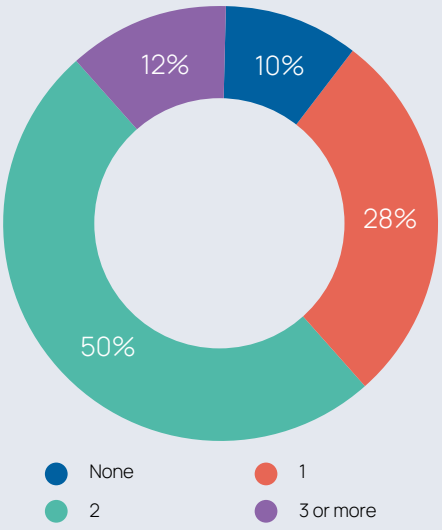
The perception of risk is also heightened among the sector's cyber security and risk management leaders: 94% of survey respondents rank supply chain incidents among their top three cyber security concerns for 2026. The convergence of geopolitical tensions, rapid technology adoption, and regulatory change is further amplifying the sector's vulnerability, creating a risk environment that is both dynamic and unpredictable.

1.3. Key Takeaways

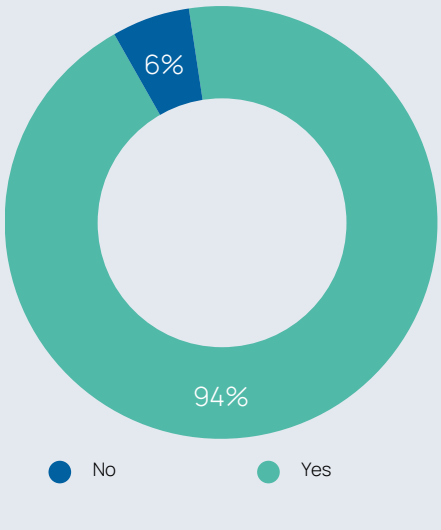
The research findings demonstrate that supply chain attacks are now a central concern for the insurance industry. The sector's reliance on complex, interdependent networks of third and fourth parties has created new vectors for attack and amplified the potential for systemic disruption. As the threat landscape evolves further, the sector must confront the reality that their own cyber security increasingly also depends on the security of all their external partners and services providers that they work with and rely on for their daily operations.

Survey Results

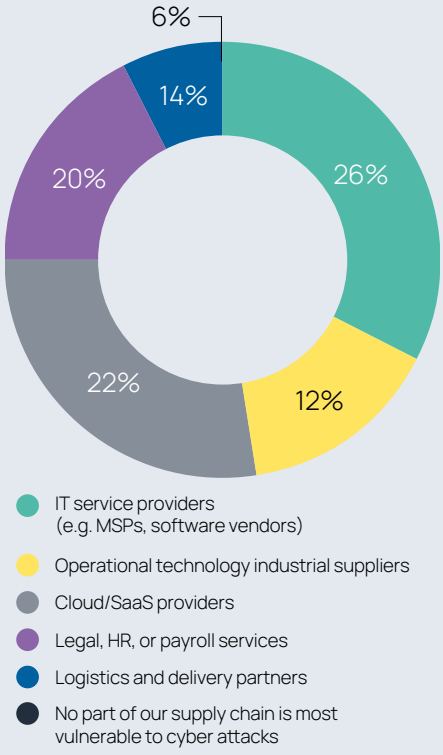
Q1. In the past 12 months, how many cyber security incidents have you experienced in your supply chain?



Q2. Do supply chain cyber incidents rank among your top three areas of concern for 2026?



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

In the face of such mounting supply chain threats, the effectiveness of traditional Third-Party Risk Management (TPRM) has to be put under intense scrutiny. Historically, TPRM has relied on periodic assessments, static questionnaires, and contractual assurances. While these are often complemented today by external scanning tools for additional validation, these tools are beset with similar problems: they are still point-in-time, are prone to many false negatives, and only provide data insights on suppliers' external perimeters. Crucially, they don't provide assurance of the effectiveness of suppliers' internal security controls for assumed breach scenarios.

46%

of respondents still rely on quarterly, biannual, annual or even less frequent re-assessments

The question is therefore whether these methods are still sufficient in the face of the dynamic, real-time nature of modern cyber threats? The stakes for the insurance industry are especially high: regulatory compliance with the Prudential Regulation Authority's and Financial Conduct Authority's latest Operational Resilience Rules such as PRA SS2/21, and market confidence, all hinge on the ability to anticipate, detect, and respond to risks across the entire supply chain.

2.2. Third-Party Risk Management Under Scrutiny

Our survey found that more than half (54%) of respondents argue they conduct continuous monitoring of their critical suppliers, while a substantial minority (46%) still rely on quarterly, biannual, annual or even less frequent re-assessments. This periodic approach leaves significant gaps in risk visibility, particularly as threat actors exploit vulnerabilities that can emerge and escalate rapidly between assessment cycles.

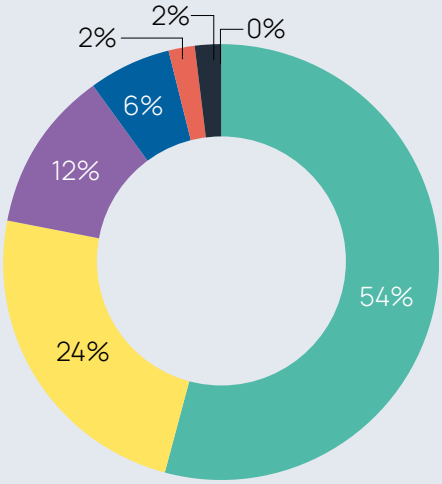
Despite a degree of confidence in existing TPRM methods — with 44% rating them as "very effective" and 56% as "somewhat effective" — no respondents considered them ineffective. However, this apparent optimism is tempered by widespread recognition of persistent shortcomings. The most frequently cited challenges with TPRM in its current state remain the inability to genuinely continuously monitor suppliers' internal security controls (36%) beyond external scanning, lack of visibility into supply chain dependencies (26%), and insufficient collaboration and information sharing with industry peers (36%). Other concerns that were raised include insufficient regulatory oversight over suppliers (34%) and difficulties in scaling supplier assessments (36%).

2.3. Key Takeaways

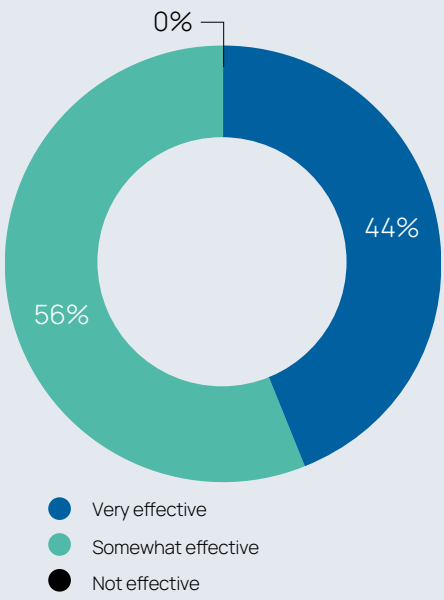
The insurance sector's experience with TPRM reflects a wider industry challenge: legacy frameworks are struggling to keep pace with the scale and complexity of modern supply chain threats. Gaps in continuous monitoring, limited visibility into extended supply chain dependencies, and insufficient collaboration are leaving the Insurance industry exposed to a plethora of supply chain cyber risks. Addressing these challenges will require a fundamental shift in mindset, a new approach to TPRM, and a commitment to greater collective defence and burden sharing.

Survey Results

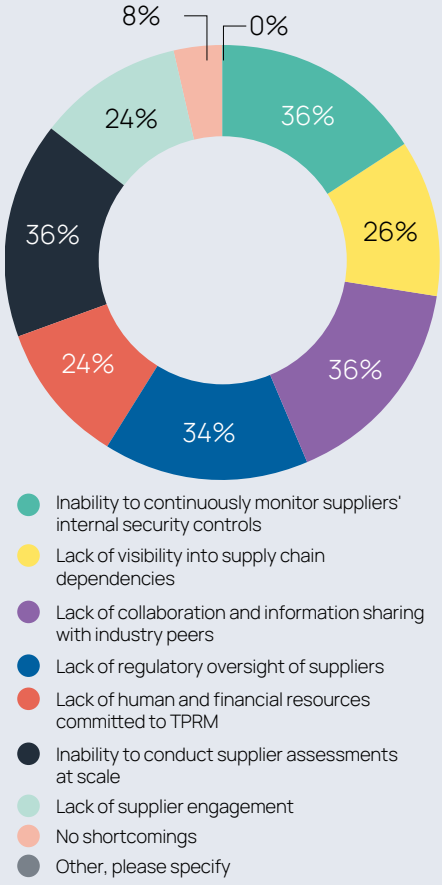
Q4. How often do you conduct security assessments of your critical suppliers?



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



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 Insurance Industry

3.1. Section Overview

UK regulators, including the Prudential Regulation Authority (PRA), the Bank of England (BoE) and the Financial Conduct Authority (FCA), are prioritising enhanced supply chain visibility, systemic risk identification, and collaboration in their latest operational resilience and cyber security measures. The Operational Resilience Framework, developed by the BoE, FCA, and PRA through rules such as PS21/3, SS1/21, and SS2/21, directly mandates firms to map important business services, identify deep supply chain dependencies, and rigorously test for systemic risks that could disrupt entire sectors. This framework explicitly includes requirements for firms to understand and manage their "critical third parties" (CTPs), whose failure could impact the stability of the wider UK financial system. The new CTP regime (PS16/24 and SS6/24), meanwhile, also grants regulators direct oversight into these essential service providers, including their own supply chain dependencies.

In the insurance sector, concentration risks — or potential single points of failures — are rarely confined to immediate partners. Instead, they can hide deeper within the extended network of supply chain relationships that underpin the market's daily operations. A single software platform, cloud provider, or analytics firm, sitting anywhere in this vast ecosystem of dependencies, can quietly serve dozens of Insurers, Brokers, and Coverholders, even indirectly, potentially amplifying the impact of any disruption. This section investigates how well equipped the sector currently is to identify these potential systemic risks.

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. A recent example is the Blue Yonder ransomware attack, which caused widespread disruption across supply chains and resulted in the compromise of potentially sensitive information, illustrating how a failure at one critical supplier can have far-reaching industry impacts.

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 insurance industry.

Similar to the financial services industry as a whole, the insurance sector's reliance on a relatively small number of technology providers, data processors, and service partners amplifies the impact of such concentration risks.

3.3. The Importance of Supply Chain Visibility

Today's supply chains are highly complex and interdependent, with organisations no longer just exposed to third-party risks. As suppliers also rely on their own suppliers, and so on, this creates the need to understand risks beyond direct third parties, extending to fourth, fifth, and nth parties. Every link is important and it is important to gain visibility and context of all the links to understand the potential cascading impact an incident may have on the industry's and individual market participants' operations. Regulators increasingly recognise how any supplier in this complex web of supply chain dependencies can represent systemic risks, especially for sectors like finance, critical national infrastructure and the public sector.

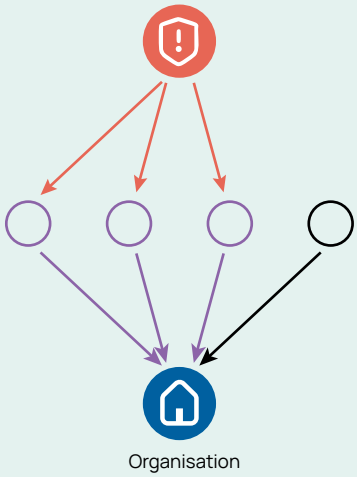
Supply chain visibility is foundational to effective risk management and the identification of concentration risks, yet remains elusive for many organisations in the wider insurance industry. Only 36% of survey respondents report full visibility into all tiers of their extended supply chain, while the majority (56%) have good visibility into most critical fourth parties but limited insight beyond. A further 8% have only limited visibility into fourth parties.

This lack of comprehensive visibility is a significant vulnerability. Without a clear understanding of dependencies and interconnections, insurance companies are unable to accurately assess risk, prioritise mitigation efforts, or respond effectively to emerging threats. The sector's complexity — characterised by multiple layers of

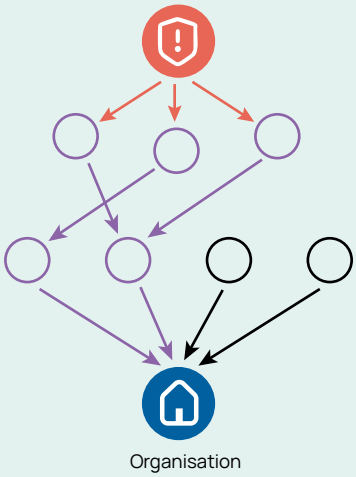
64%

of survey respondents lack full visibility into their extended supply chains beyond direct third parties

Individual Concentration Risks

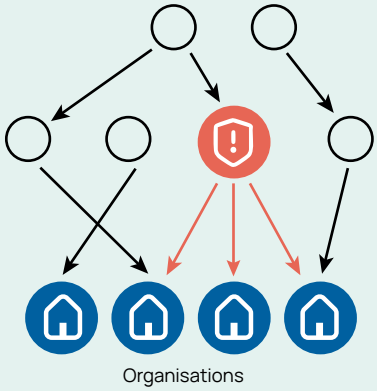


4th-party concentration risk

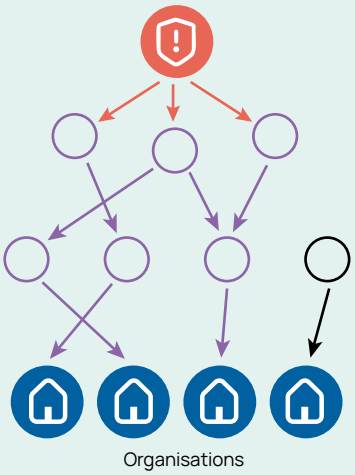


5th-party concentration risk

Systemic Concentration Risks



3rd-party systemic risk



5th-party systemic risk

carriers, reinsurers, brokers, and technology vendors — compounds the challenge, making it difficult to map relationships and identify systemic points of failure.

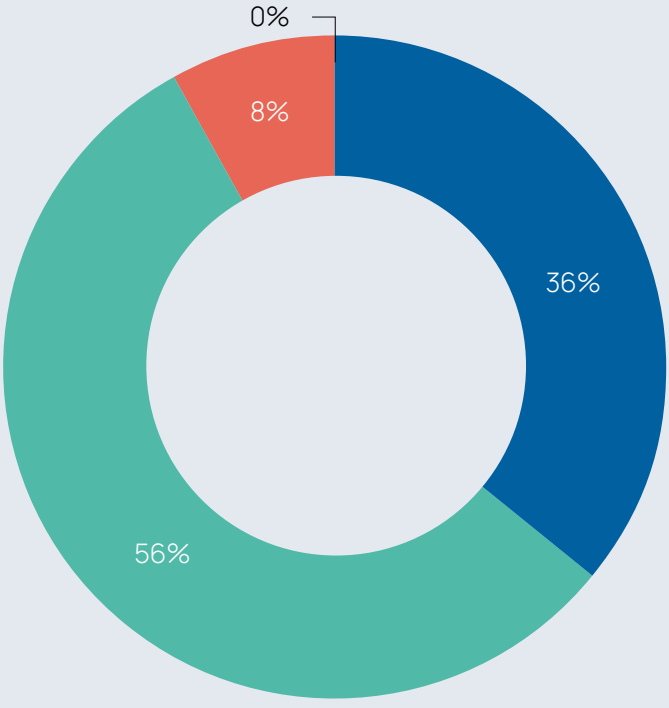
3.4. Key Takeaways

Concentration risks are widely recognised but not always well managed. Most insurance companies lack the comprehensive visibility needed to identify and mitigate concentration and systemic risks, limiting their ability to respond proactively when supply chain attacks occur.

Traditional TPRM, focused on direct suppliers and periodic reviews, cannot uncover the complex dependencies of modern supply chains. Major incidents like MOVEit and Log4j have shown how unseen vulnerabilities in deeper tiers can trigger widespread disruption. Regulators' calls for deeper supply chain mapping reflect the urgent need for collective visibility. Without it, both organisations and entire sectors remain at risk from cascading failures. Enhanced supply chain visibility is now essential for true operational resilience.

Survey Results

Q7. 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

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

This section explores the perspectives of industry experts on the vital role that enhanced collaboration plays in improving supply chain security within the UK insurance sector. By sharing insights, threat intelligence, and best practices, organisations can gain greater visibility into potential vulnerabilities, identify concentration risks, and build collective resilience against evolving cyber threats. We will examine how fostering stronger partnerships and open communication across the industry can help transform supply chain security from a fragmented challenge into a unified defence strategy.

4.2. The Current State of Collaboration

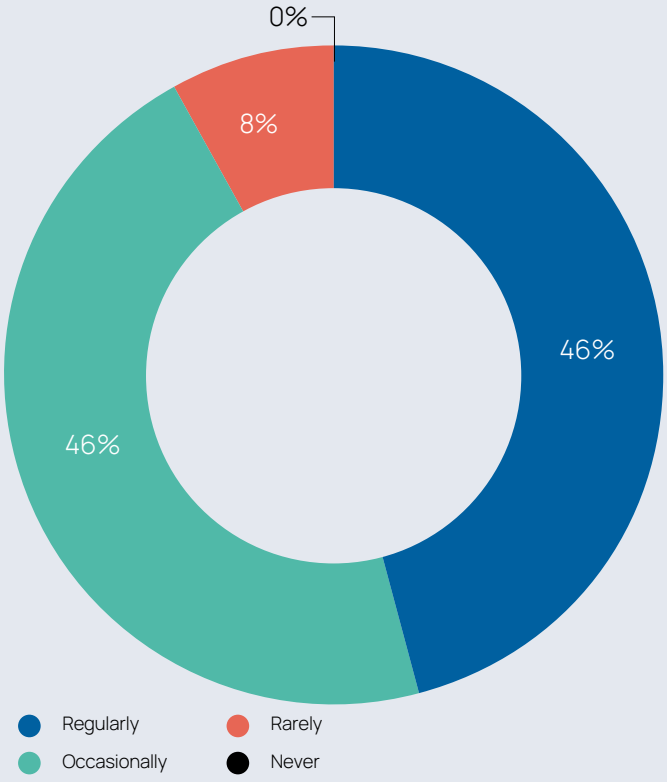
While collaboration is improving, significant barriers remain. Nearly half (46%) of TPRM functions regularly collaborate with industry peers, and another 46% do so occasionally. However, 8% rarely participate in information-sharing initiatives, and a lack of collaboration is nonetheless cited as a key shortcoming by 36% of respondents. Cultural, operational, and competitive dynamics continue to inhibit the free flow of information, limiting the sector's ability to identify and respond to systemic threats.

Regulators are also expected to encourage or mandate cross-industry collaboration and information sharing, recognising that collective action is essential to addressing the scale and complexity of modern supply chain threats. The insurance sector, with its unique position at the intersection of risk transfer and risk management, has a critical role to play in shaping and implementing these regulatory reforms.

Overall, these are positive signs. Insurers and brokers are also increasingly offering risk management services to clients and partners, including threat analysis, tabletop exercises, and incident response planning. These initiatives are fostering a more collaborative approach to cyber resilience, but their reach and impact remain uneven across the sector.

Survey Results

Q8. How often does your Third-Party Risk Management function collaborate with industry peers and participate in information-sharing initiatives to identify systemic risks



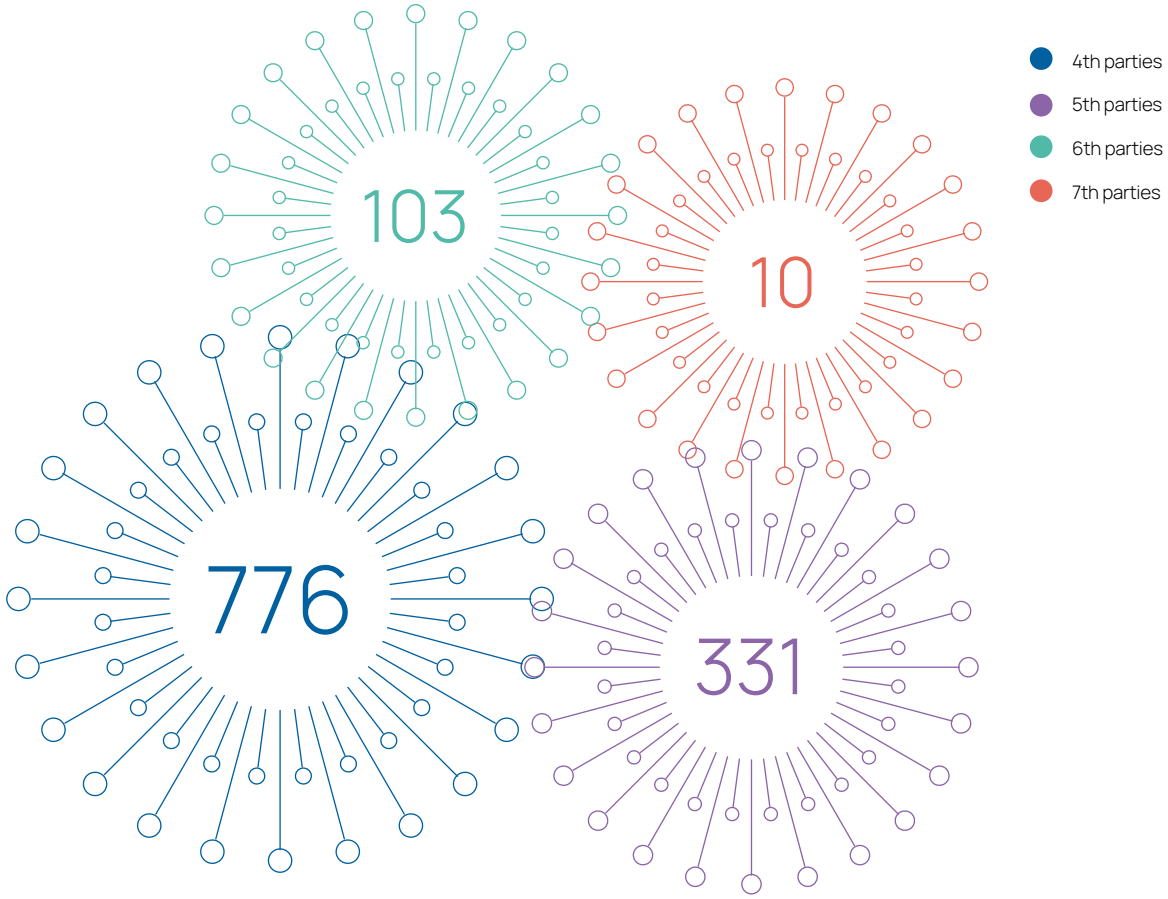
4.3. Sharing Supply Chain Data Can Uncover Systemic Risks

Across the UK's most critical sectors, organisations are already embracing a new model of collective defence — working together to identify supply chain risks, which no single entity could do 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. Given their often significantly overlapping supply chains, doing so enables them to map complex supplier relationships, far beyond immediate third-parties, and coordinate risk mitigation efforts while reducing the burden on both these organisations and their suppliers. This new ethos to Defend-as-One yields tangible results, as the following data from the Risk Ledger platform demonstrates.

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

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, 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.

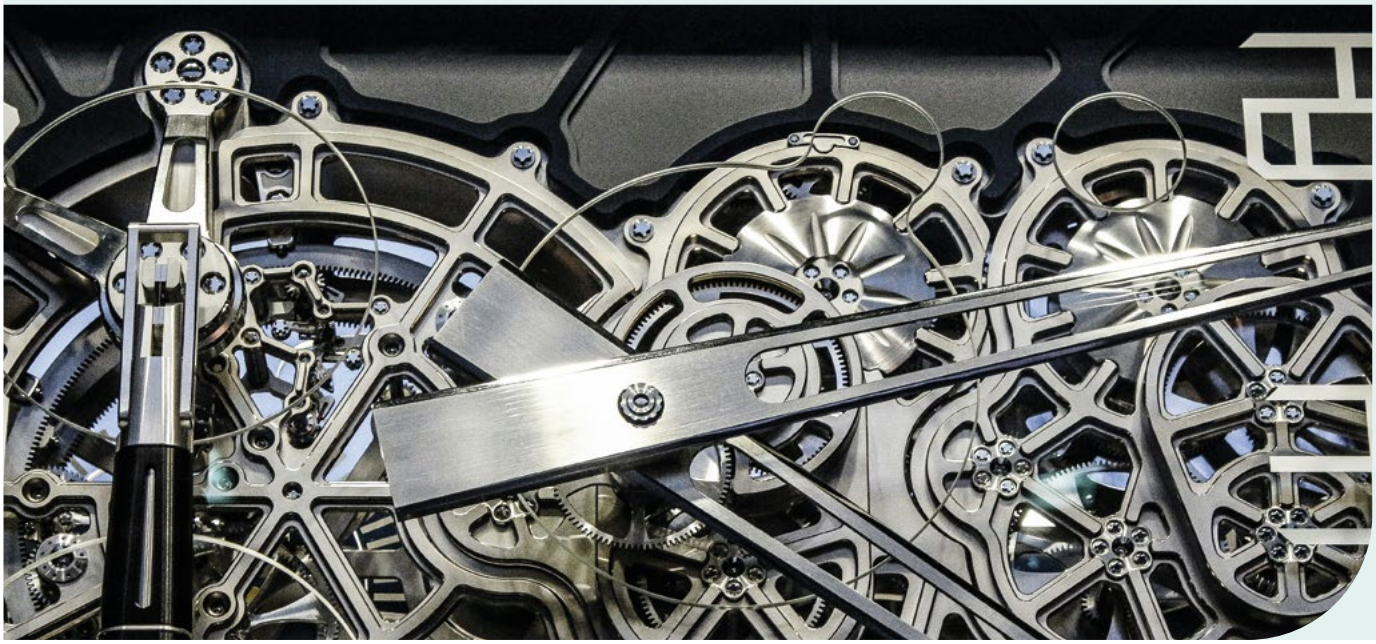
14 of these were direct 3rd parties connected to at least 50% of all community members.

4.5. 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 insurance 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 within the same industries.

Greater collaboration with industry peers that often share substantially overlapping supply chains can overcome many of the current shortcomings with Third-Party Risk Management. 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 fifth-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.
- Collaboratively triage, prioritise, and mitigate risks, offering stronger, sector-wide resilience through real-time information sharing and coordinated responses.

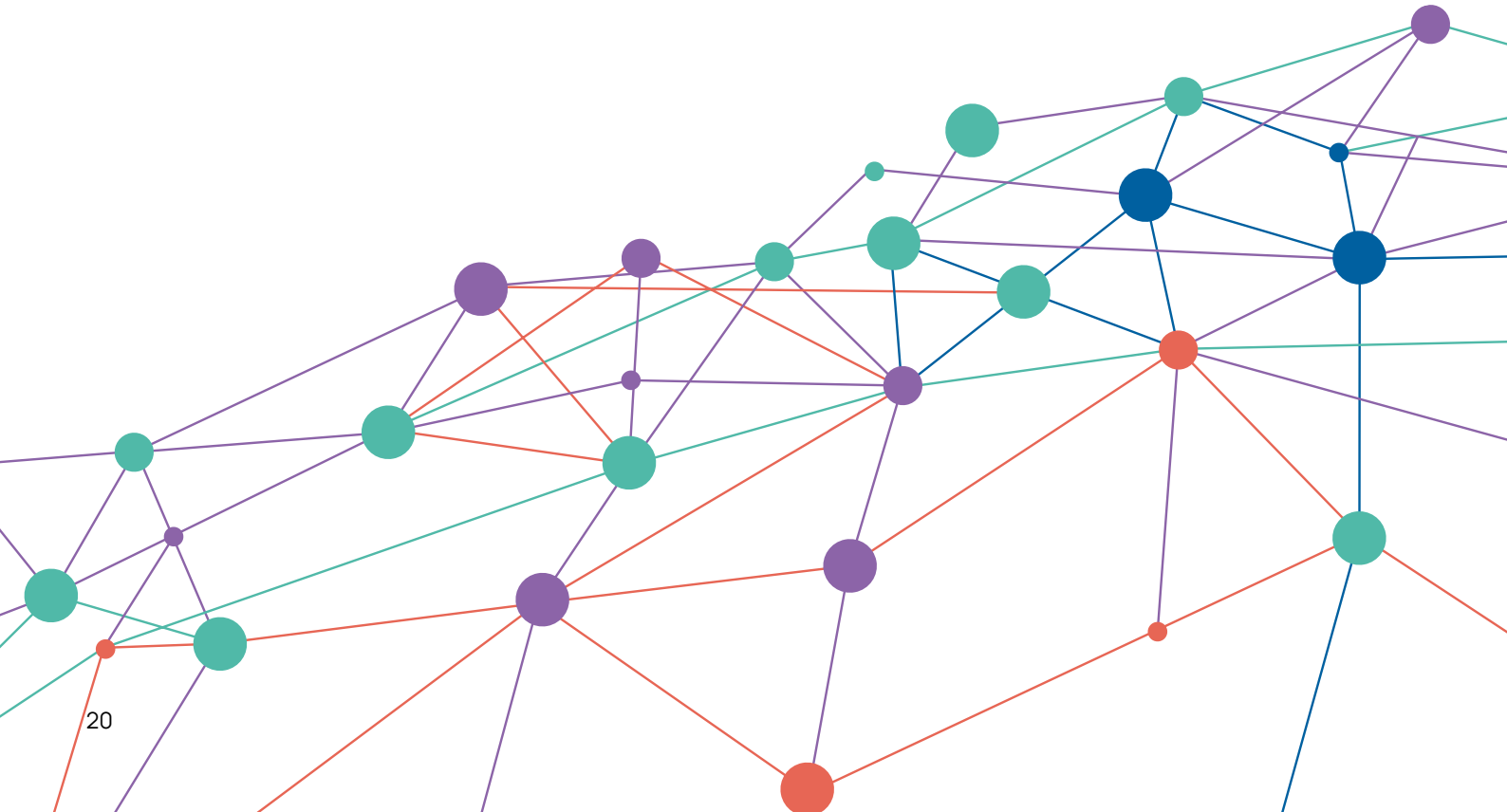


Conclusions

The UK insurance sector stands at a pivotal moment in its approach to supply chain cyber security. The rise of supply chain attacks — driven by digital transformation, complex interdependencies, and sophisticated adversaries — has elevated third-party risk to a board-level concern. Traditional TPRM frameworks, while foundational, are no longer sufficient to address the scale and complexity of modern threats. Gaps in continuous monitoring, limited supply chain visibility, and insufficient collaboration are exposing insurers to systemic risks that threaten not only individual organisations but the stability of the sector as a whole.

To meet these challenges, the sector must embrace a new paradigm of risk management — one that prioritises continuous, real-time assessment, deepens visibility into extended supply chains, and fosters a culture of collaboration and information sharing. Regulatory reforms are creating the conditions for change, but lasting progress will depend on the sector's willingness to invest in advanced technologies, build trusted partnerships, and lead by example.

The path forward is clear: only through collective action and a shared commitment to resilience can the UK insurance industry protect its operations, customers, and reputation in an increasingly hostile and complex cyber environment.



Appendix: Survey Methodology

This report draws on a robust, mixed-methods approach combining authoritative open-source data, a targeted survey of UK cyber security professionals, and empirical insights from Risk Ledger's platform data.

Data sources

Open-source data

We analysed publicly available open-source sources where necessary to contextualise supply chain cyber security trends and regulatory developments.

Survey of UK cyber security professionals

Conducted by Censuswide, the survey gathered responses from professionals actively involved in cyber security and Third-Party Risk Management across the UK insurance sector. The survey targeted individuals with varying levels of involvement in their organisation's cyber security and third-party risk management strategies, including senior decision-makers (CISOs, Heads of TPRM, Security Directors) and critical operational staff. Key demographic and role-based screening questions ensured relevance and quality of responses.

The questionnaire covered four main areas:

- **Supply Chain Threat Landscape:** Incidence and perceived vulnerability of cyber attacks within supply chains.
- **Effectiveness of Third-Party Risk Management:** Frequency of supplier assessments, perceived efficacy, and key shortcomings.
- **Systemic Concentration Risks:** Visibility into extended supply chains beyond direct third parties and collaboration practices.
- **Regulatory Outlook:** Priorities for government action in strengthening supply chain security. Platform data analysis Complementing the survey, Risk Ledger's proprietary platform data was analysed to identify supply chain dependencies up to the 7th tier within communities of peer organisations. This enabled detection of systemic concentration risks and mapping of complex interdependencies that are often invisible to individual organisations.

Platform data analysis

Complementing the survey, Risk Ledger's proprietary platform data was analysed to identify supply chain dependencies up to the 7th tier within communities of peer organisations. This enabled detection of systemic concentration risks and mapping of complex interdependencies that are often invisible to individual organisations.

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