RISK LEDGER

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

A Risk Ledger Data Insights Report

About this report

This report, "Every Link Matters: The State of Supply Chain Security in Energy 2025 — UK Edition" provides a comprehensive analysis of supply chain security risks in the UK energy 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

Contents

Introduction

The UK energy sector is currently navigating one of the most profound transformations in its history. Driven by the urgent imperative of Net Zero targets, the industry is undergoing a "Great Transition"—a rapid shift from centralised, analogue infrastructure to a decentralised, highly digitalised smart grid. This evolution promises greater efficiency and sustainability, but it has also fundamentally altered the sector's risk profile. By connecting historically siloed Operational Technology (OT) systems to corporate IT networks and the cloud, and by integrating a vast array of Distributed Energy Resources (DERs) and smart meters, the energy sector has exponentially expanded its digital attack surface.

This new ecosystem relies heavily on a complex web of external partners—from software vendors managing grid control systems to cloud providers hosting critical telemetry data. As a designated Operator of Essential Services (OES) under UK Critical National Infrastructure (CNI), the energy sector's resilience is no longer just a commercial concern but a matter of national security. Any serious disruption here could threaten public safety, economic stability, and the ability of the nation to function.

The stakes have never been higher. The National Cyber Security Centre (NCSC) has issued repeated warnings regarding the "playbook" of hostile state actors, who are increasingly pre-positioning themselves within CNI networks to cause disruption during times of geopolitical tension. Recognising this shifting threat landscape, the regulatory environment is tightening. Building on the foundation of the NIS (Network and Information Systems) Regulations 2018, the forthcoming Cyber Security and Resilience Bill signals a decisive shift in focus. By bringing Managed Service Providers (MSPs) and Critical Suppliers directly into regulatory scope, the UK government is acknowledging a hard truth: in a hyper-connected grid, you cannot secure the energy supply without securing the supply chain.

Section 1: The Rise of Supply Chain Attacks

1.1. Section Overview

In the energy sector, a supply chain attack represents an indirect but highly effective pathway to compromising critical infrastructure. Rather than attacking a well-defended energy operator directly, threat actors increasingly opt to compromise a third-party provider—such as a software supplier, an industrial hardware manufacturer, or an engineering consultancy—to gain privileged access to the target's network.

While ransomware gangs motivated by financial gain remain a persistent nuisance, the primary concern for the UK energy sector is increasingly the rise of sophisticated, state-sponsored adversaries. For these actors, the motive shifts from extortion to sabotage, disruption, and strategic pre-positioning. In this context, the supply chain is not just a vector for data theft; it has become the backdoor to the industrial control systems that keep the lights on and the economy moving.

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

The UK energy sector stands at the intersection of technological vulnerability and geopolitical conflict. As nations such as Russia, China, and Iran continue to develop offensive cyber capabilities, UK CNI has become a primary target. The NCSC has warned that these actors actively target the engineering and manufacturing supply chains to pivot into critical operational networks. The threat is not theoretical; it is escalating rapidly. In 2023 alone, the sector witnessed 48 successful attacks on UK utilities, representing a staggering 586% rise from 2022.

This surge is being driven by the exploitation of interconnected systems, with approximately 45% of breaches now originating from third-party vendors, particularly software providers. The impact is widespread, with supply chain compromises affecting the data of over 140,000 individuals in the UK, often as collateral damage in broader campaigns by state-backed actors.

45%

of breaches now originating from third-party vendors

The threat is amplified by the rapid convergence of IT and OT. Historically, OT systems were air-gapped and secure by isolation. Today, they are increasingly connected to the internet via IT service providers to enable remote monitoring and efficiency. Attackers have learned to exploit vulnerabilities in these bridging vendors to access the legacy ICS and SCADA systems that physically manage power generation and distribution—systems that were often not designed to withstand modern cyber threats.

Key Trends and Incidents (2023–2025):

- **Utility Vendor Breaches (2023):** A significant spike in attacks targeted the third-party IT and software suppliers that underpin utility operations. In fact, 67% of energy breaches in this period were traced back to these third-party vectors, highlighting how the "soft underbelly" of the supply chain is being systematically targeted to bypass the stronger defences of major energy operators.
- **NCSC-Reported Exploits (2024):** The UK's National Cyber Security Centre (NCSC) identified a disturbing trend of threat actors establishing persistent access within energy supply chains using "living off the land" techniques—utilising native system tools to evade detection. This pre-positioning poses a direct risk to critical infrastructure, including power distribution networks, following specific warnings of destructive intent against UK assets.
- **AI-Driven Third-Party Attacks (2025):** The threat landscape has evolved further with the integration of Artificial Intelligence. A recent Bridewell report detailed how AI-enhanced phishing campaigns against vendors are accelerating the speed of compromise. 62% of energy organisations faced such incidents in the past year—exceeding the UK average. These attacks are particularly dangerous for legacy OT systems in sectors like offshore wind, where mitigation can take an average of 5.8 hours—a lifetime in a critical operational environment.

94%

of survey respondents rank supply chain incidents among their top three cyber security concerns for 2025

Industry Sentiment vs. Reality:

The scale of this challenge is reflected starkly in the industry's own data. According to our survey of cyber security and risk professionals across the UK energy sector, 94% of respondents now rank supply chain cyber incidents among their top three concerns in 2025. This anxiety is well-founded: 78% of firms reported experiencing at least one supply chain cyber incident in the past 12 months. More alarmingly, this is rarely a one-off event, with 46% of organisations suffering two incidents and 12% experiencing three or more within the past year alone.

When asked to identify the perceived weakest links within their supply chains, the industry pointed directly to "digital bridge" vendors. 38% of respondents cited IT service providers (such as MSPs and software suppliers) as the most vulnerable part of their supply chain, followed by Operational Technology (OT) suppliers (22%) and Cloud/SaaS providers (20%).

Global events support these findings. The 2021 ransomware attack on the Colonial Pipeline in the US demonstrated how a compromise in a billing system could force the precautionary shutdown of physical fuel supplies, causing nationwide chaos. Similarly, attacks on Ukraine's power grid have shown how supply chain compromises can be weaponised to trigger physical blackouts.

78%

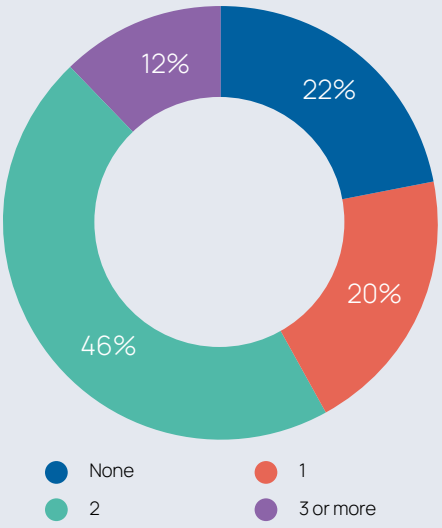
of respondents reported experiencing at least one supply chain cyber incident in the past 12 months

1.3. Key Takeaways

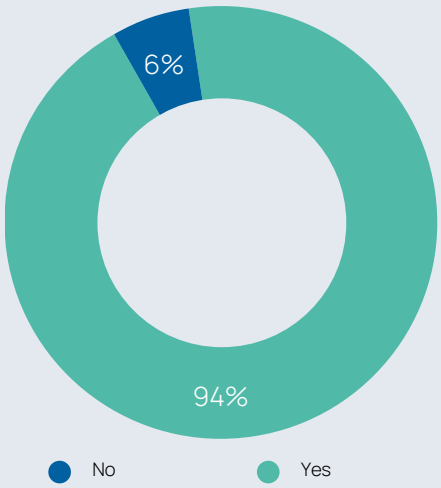
- **The Battlefield has Shifted:** Cyber defence in the energy sector is no longer just about guarding the perimeter; it is about managing the security of a vast, interconnected digital ecosystem.
- **The IT/OT Risk Nexus:** The industry itself identifies IT service providers and OT suppliers as its most vulnerable links, confirming that the convergence of these two worlds creates the sector's most critical exposure point.
- **Safety Over Secrecy:** Unlike other sectors where data loss is the primary fear, resilience in energy must prioritise operational continuity and physical safety. A supply chain attack here threatens the machinery of the nation itself.

Survey Results

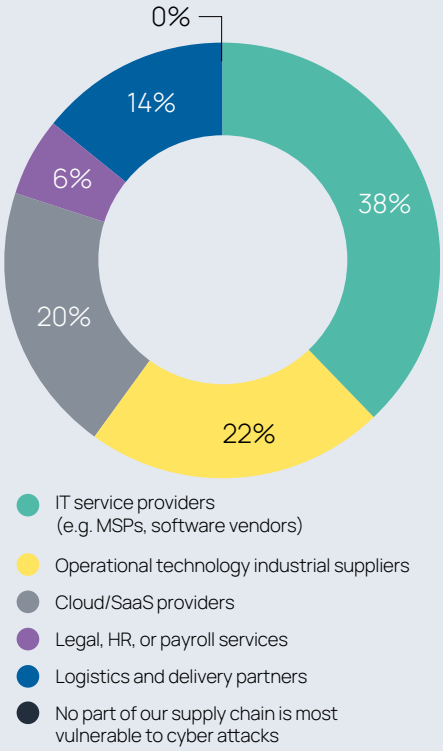
Q1. In the past 12 months, how many cyber security incidents have you experienced in your supply chain?



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 attacks, if any?



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

Top Three Shortcomings with Traditional Third-Party Risk Management

50%

of UK cyber security professionals identified the inability to continously monitor suppliers' internal security controls as a key shortcoming

36%

of UK cyber security professionals identified the lack of visibility into supply chain dependencies as a key shortcoming

34%

of UK cyber security professionals regard the lack of collaboration and information sharing with industry peers as a key shortcoming

2.1. Section Overview

In the face of these mounting supply chain threats and aggressive nation-state actors, the effectiveness of traditional Third-Party Risk Management (TPRM) is coming under intense scrutiny. Historically, TPRM in the energy sector has been driven by procurement cycles and regulatory compliance frameworks like the European and UK NIS Regulations. In practice, this translated into a reliance on periodic assessments, static security questionnaires, and point-in-time audits.

While these methods provide a snapshot of risk and might have been sufficient to demonstrate compliance, the question remains: are they sufficient to detect dynamic, real-time threats in an increasingly hyper-connected grid? As the sector prepares for the rigorous demands of the upcoming Cyber Security and Resilience Bill, the gap between "being compliant" and "being resilient" is becoming increasingly apparent.

2.2. Third-Party Risk Management Under Scrutiny

Our survey reveals a sector that is grappling with the limitations of its current supply chain risk management toolkit, which is currently limited to the methods and processes of third-party risk management, focussing as it does primarily on direct vendor relationships and exposure. When asked about the effectiveness of traditional TPRM in reducing supply chain cyber risks, confidence is lukewarm at best. While 26% of respondents rated their current methods as "Very effective," the majority (64%) view them as only "Somewhat effective." Perhaps most telling is that 10% of industry professionals—the people on the front lines of defending CNI—already consider traditional TPRM to be "Not very effective."

This skepticism is largely driven by the "frequency gap." New cyber risks can emerge in minutes, yet risk assessments often occur on timelines measured in months or years. Our data shows that only 40% of energy organisations currently conduct continuous monitoring of their critical suppliers, and this relatively high number has to be taken with more than just a grain of salt, and has more to do with prevailing definitions of what constitutes "continuous monitoring" in the context of supply chain cyber risk management than reflecting the genuine ability of organisations to stay on top of emerging cyber risks in their supply chains in real-time. The remaining 60% rely on periodic checks, with 28% assessing once a quarter, 18% twice a year, and 14% checking annually or even less frequently. This sporadic approach creates massive blind spots, leaving organisations unaware of vulnerabilities—such as a zero-day exploit in a cloud platform, a lapsed patch in an OT component or the introduction of potentially highly vulnerable shadow IT—that can emerge at any time between assessment cycles.

However, the problem runs deeper than just frequency. When asked to identify the single biggest shortcoming of their current TPRM programme, 50% of respondents cited the "Inability to continuously monitor suppliers' internal security controls." This is a critical distinction in the energy sector. While external scanning tools can assess a vendor's internet-facing perimeter, they cannot see inside the network or the organisation to verify the internal controls that matter most for CNI safety—such as network segmentation, privileged access management, employee IT hygiene and security training, or the patching status of air-gapped industrial controllers.

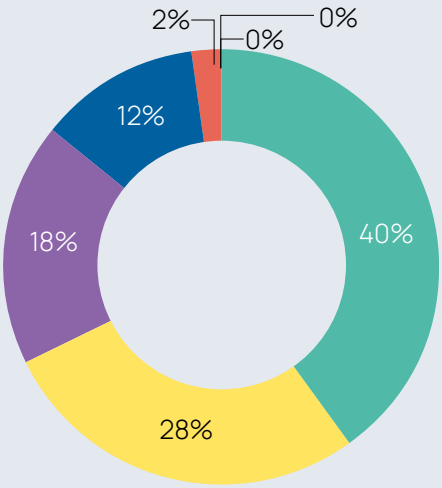
Other significant barriers include a "Lack of visibility into supply chain dependencies" (36%) and a "Lack of collaboration and information sharing between TPRM teams and their industry peers" (34%). These findings paint a picture of a sector that knows it needs to look deeper and work more closely together, but is currently held back by the limitations of legacy tools, processes and a culture of siloed defence.

2.3. Key Takeaways

- The Compliance Trap: While the sector is diligent about compliance, the current "tick-box" approach to TPRM is struggling to keep pace with the speed and sophistication of modern threats.
- The Monitoring Gap: With 60% of the sector lacking continuous monitoring capabilities, there are significant windows of exposure where critical supplier risks can go undetected.
- The Need for Internal Insight: The industry's primary frustration is the inability to see inside supplier networks. To secure the grid, energy operators need more than just perimeter scans; they need assurance that the internal controls protecting critical OT systems are robust and effective.

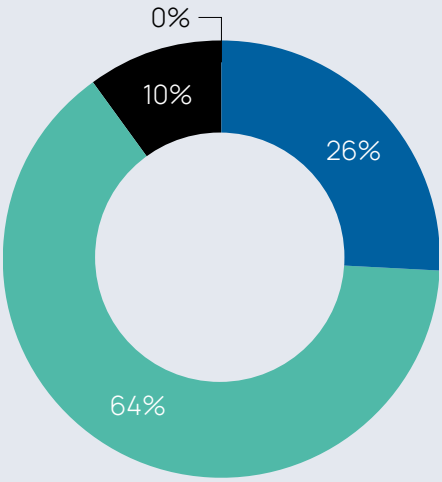
Survey Results

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



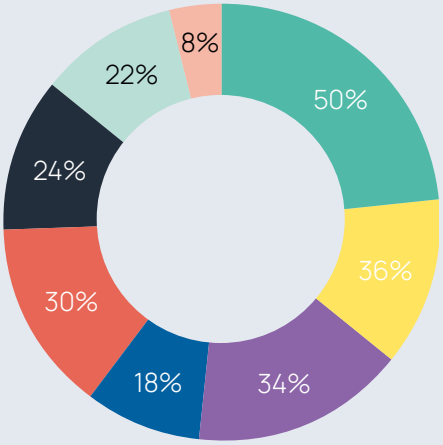
- We continuously monitor the security postures of our critical suppliers
- Once a quarter
- Twice a year
- Annually
- Every two years or less frequently
- Only during onboarding or contract renewal
- We do not assess the security of our critical suppliers

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

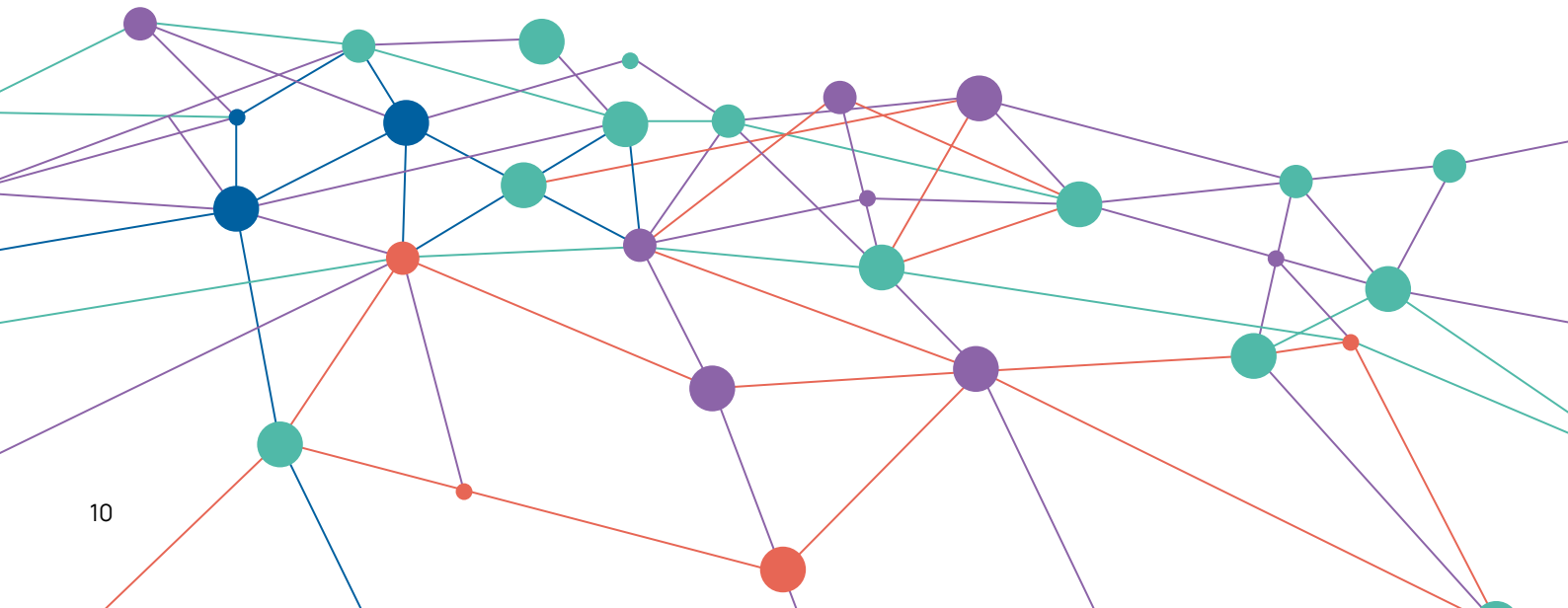


- Very effective
- Somewhat effective
- Not effective

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



- Inability to continuously monitor suppliers' internal security controls
- Lack of visibility into supply chain dependencies
- Lack of collaboration and information sharing with industry peers
- Lack of regulatory oversight of suppliers
- Lack of human and financial resources committed to TPRM
- Inability to conduct supplier assessments at scale
- Lack of supplier engagement
- No shortcomings



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

3.1. Section Overview

Under the UK's operational resilience framework, regulatory bodies like Ofgem, the HSE, and the NCSC are increasingly focused on the concept of Important Business Services (IBS)—the critical functions that, if disrupted, would cause intolerable harm to consumers or market stability. For an energy company, an IBS might be the balancing of the grid, the management of gas storage pressure, or the operation of a 24/7 control room.

However, delivering these services is rarely a solo endeavour. It relies on a sprawling ecosystem of interconnected third parties, from gas traders and specialist engineering firms to software vendors and cloud platforms. This section examines a critical vulnerability in this model: if you cannot see the full chain of dependencies supporting your IBS, you cannot identify the single points of failure that threaten them.

3.2. What are Concentration Risks

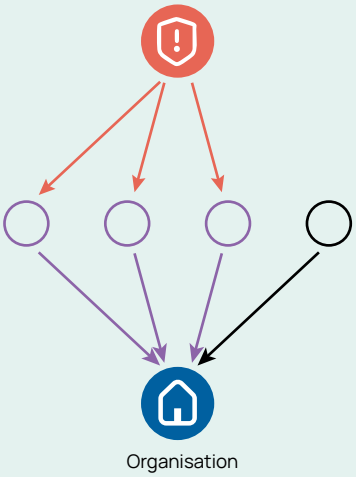
Concentration risks occur when an organisation relies too heavily on a single supplier for multiple critical functions, or—more dangerously—when multiple critical suppliers all rely on the same fourth-party vendor. In the energy sector, these risks are systemic. A single software vulnerability in a widely used SCADA system or a cloud outage at a major hyperscaler could simultaneously impact dozens of energy operators, bypassing individual redundancies and threatening the stability of the entire national grid.

Our survey indicates a high level of maturity and awareness regarding this issue. When asked if they can currently identify concentration risks in their supply chain, 62% of respondents confidently answered "Yes." This suggests that energy risk professionals understand the danger of "all eggs in one basket." However, acknowledging a risk and having the data to map it are two very different things.

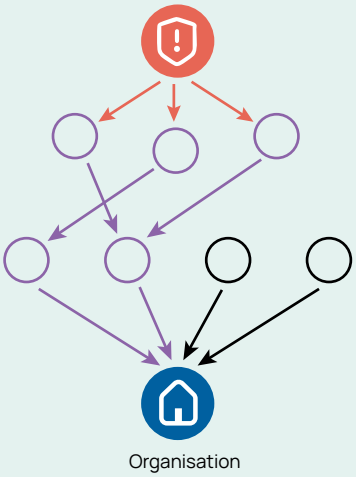
Specific to the UK energy transition, two forms of concentration risk are becoming acute:

- **Critical Cloud/SaaS Dependencies:** As OT moves to the cloud, the sector is aggregating risk around a small number of major cloud providers and specialised SaaS platforms for functions like smart metering and energy trading.
- **Specialist OT Monocultures:** The operational technology market is dominated by a select group of global manufacturers. A vulnerability deep within the firmware of a common PLC or widely used industrial protocol represents a "silent" concentration risk that exists across the entire industry, often invisible to the OES until it is exploited.

Individual Concentration Risks

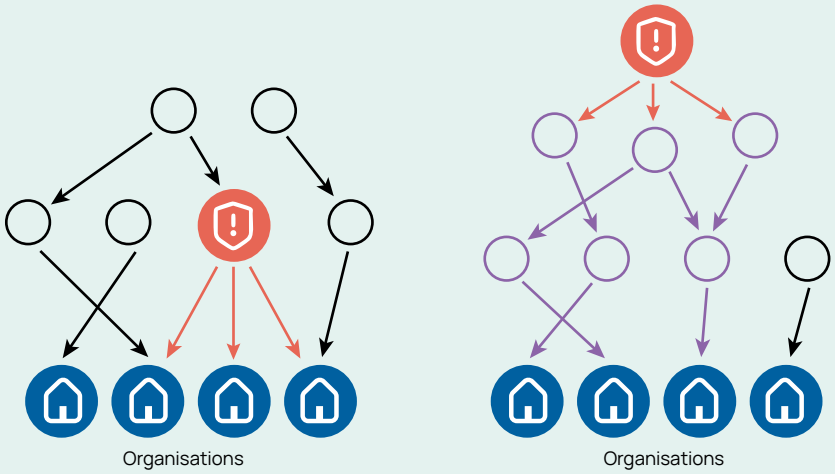


4th-party concentration risk



5th-party concentration risk

Systemic Concentration Risks



3rd-party systemic risk

5th-party systemic risk

3.3. The Importance of Supply Chain Visibility

While awareness of concentration risk is high, our data reveals a stark "Reality Gap" in the industry's ability to see it. True resilience requires mapping dependencies not just to immediate third parties, but deeper into the 4th, 5th, and Nth tiers where critical software and hardware components originate or single points of failure could hide.

When asked about their level of visibility:

- Only 26% of respondents claimed to have "Excellent" visibility into all tiers of their extended supply chain.
- The majority (52%) reported "Good" visibility, but admitted it is limited beyond the most obvious and critical 4th parties.
- 22% have "Limited" visibility, effectively flying blind beyond their direct contracts.

This in effect means that 74% of the UK energy sector has a "visibility ceiling." They can see who they pay, but they cannot sufficiently see who their suppliers rely on. This is a critical vulnerability in an era where attacks like SolarWinds and Log4j exploit deep-tier components to compromise high-value targets.

This visibility challenge is being compounded by decarbonisation. The integration of Distributed Energy Resources (DERs)—such as EV charging networks, battery storage facilities, and solar aggregators—is bringing a wave of new, smaller, and often less mature technology vendors into the critical grid ecosystem. These new entrants introduce complex, unmapped dependencies that traditional visibility tools are struggling to track, creating new pockets of hidden concentration risk.

52%

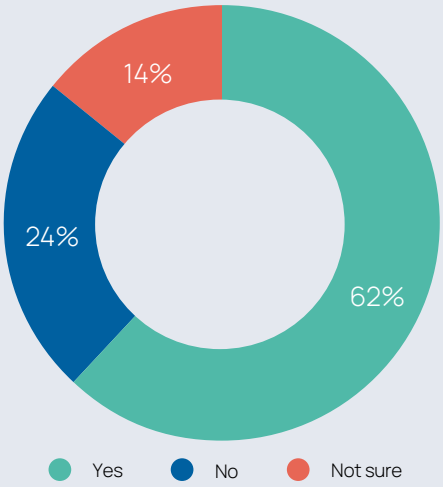
of UK cyber security professionals say they have good visibility into most critical 4th parties, but limited visibility beyond

3.4. Key Takeaways

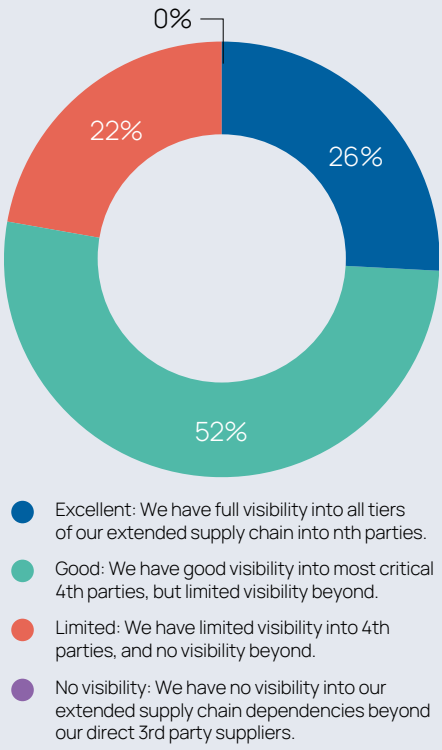
- **The Paradox of Awareness:** While 62% of the sector believes they can identify concentration risks, 74% lack the deep-tier visibility required to actually map them fully. This gap between confidence and capability is a major blind spot.
- **IBS as the North Star:** To build true resilience, the sector must pivot from managing "vendors" to managing the "digital supply chain of Important Business Services," regardless of how many tiers deep that chain goes.

Survey Results

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

In an ecosystem where every major energy provider relies on the same core infrastructure and technology stack, isolation in itself represents a vulnerability. No single energy operator can effectively map and defend its entire, complex international supply chain in isolation. Collaboration between industry peers is increasingly recognised as the only viable mechanism to manage systemic cyber risk.

This section explores the state of collaboration between TPRM and cyber security teams within the UK energy sector. It examines whether current practices are sufficient to combat nation-state threats and illustrates how a "Defend-as-One" approach—sharing supply chain risk intelligence rather than guarding it—can uncover hidden vulnerabilities that no single organisation could find on its own.

60%

of survey respondents say their TPRM functions only occasionally collaborate with industry peers and participate in information-sharing initiatives to identity shared systemic risks

4.2. The Current State of Collaboration

While the desire for collaboration is evident, the reality on the ground is inconsistent. Our survey indicates that "collaboration" for many energy companies remains an ad-hoc activity rather than an operational discipline. Only 24% of respondents reported that their TPRM function collaborates with industry peers "Regularly." The vast majority (60%) do so only "Occasionally," while 16% rarely or never participate in information-sharing initiatives.

This sporadic approach—often limited to post-incident deliberations or industry conferences—is insufficient for identifying real-time systemic threats. However, the appetite for change is undeniable. When asked what the UK Government should focus on in the upcoming Cyber Security and Resilience Bill, 50% of respondents called for "Providing incentives or mandates for cross-industry collaboration and information sharing."

This was a top-tier priority, ranking alongside "Greater emphasis on identifying systemic risks" (52%) and "Enhancing powers for regulators" (48%). The industry is effectively asking the regulator to help break down the barriers to cooperation, recognising that legal and competitive silos are hindering more effective national defence.

4.3. Sharing Supply Chain Data Can Uncover Systemic Risks

The traditional "siloed" model of TPRM is also grossly inefficient. Today, a critical vendor serving the UK energy market—such as a major cloud provider or a specialist engineering firm—might receive hundreds of identical security questionnaires from different energy operators. This duplication wastes resources for both the operators and the vendors.

By moving to a collaborative platform model, the sector can transition to a "secure once, share with many" approach. When one energy company assesses a supplier and shares that data securely with the community, every other peer benefits instantly. More importantly, this data aggregation and the sharing of supply chain dependencies and risk intelligence can generate a collective supply chain map. By overlaying the supply chain networks of multiple CNI operators, the industry can instantly visualise shared dependencies, identifying the "super-nodes" in the network that, if compromised, would cause systemic failure.

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

To understand the potential impact of this collaborative approach, we can look to a parallel exercise conducted within the highly regulated financial services sector—another pillar of UK CNI with similar complexity and regulatory pressures.

In this case study, a community of just 8 financial services organisations utilised the Risk Ledger platform to map their shared ecosystem.

- Collectively, they inputted only 98 direct third-party supplier connections.
- However, by leveraging the network effect of the platform, this small input automatically revealed 1220 further dependencies in their overlapping extended supply chains (4th, 5th, and 6th parties).

The results were stark. By overlaying their maps, the community identified 92 potential concentration risks—single points of failure shared by multiple institutions. Crucially, 62 of these risks were located at the 4th party level and beyond, meaning they would likely have remained invisible to any single bank operating in isolation. Furthermore, 14 direct suppliers were found to be connected to at least 50% of the community, highlighting immediate systemic chokepoints.

The Lesson for the UK Energy Sector

The UK energy sector is arguably even more concentrated than finance, relying on a narrow set of specialised OT vendors and legacy engineering firms. If a small group

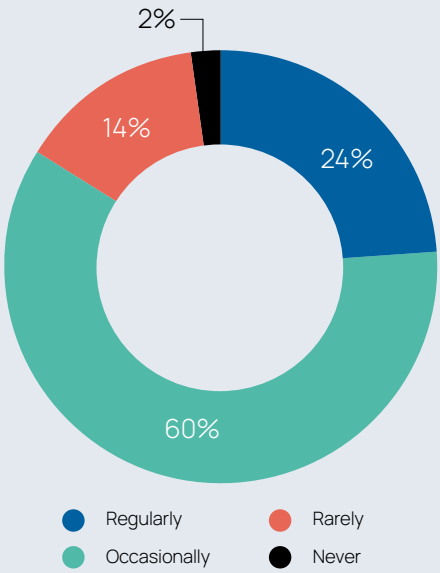
of financial firms could uncover nearly 100 systemic risks simply by sharing data, the potential for the energy sector to uncover critical vulnerabilities in the national grid through similar collaboration is immense.

4.5. Key Takeaways

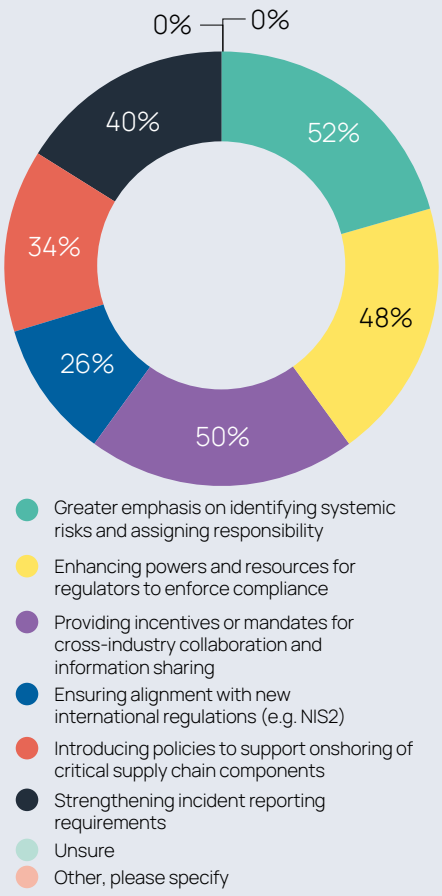
- **Collaboration is a Force Multiplier:** Individual risk assessments protect one company; shared risk intelligence protects the grid. The industry explicitly desires a regulatory push to make this standard practice.
- **The Network Effect:** As demonstrated by the financial sector case study, sharing supply chain data allows organisations to see deeper into the Nth tier than they ever could alone, revealing hidden concentration risks.
- **Defend-as-One:** To counter state-sponsored threats, the energy sector must move from a competitive mindset to a collective defence strategy, where a vulnerability found by one is a vulnerability fixed for all.

Survey Results

Q9. How often does your TPRM function collaborate with industry peers and participate in information-sharing initiatives to identify systemic risks.



Q10. What, if anything, should the UK Government focus on in the upcoming Cyber Security and Resilience Bill with regard to strengthening your sector's supply chain security? (Select up to 3)



Conclusions

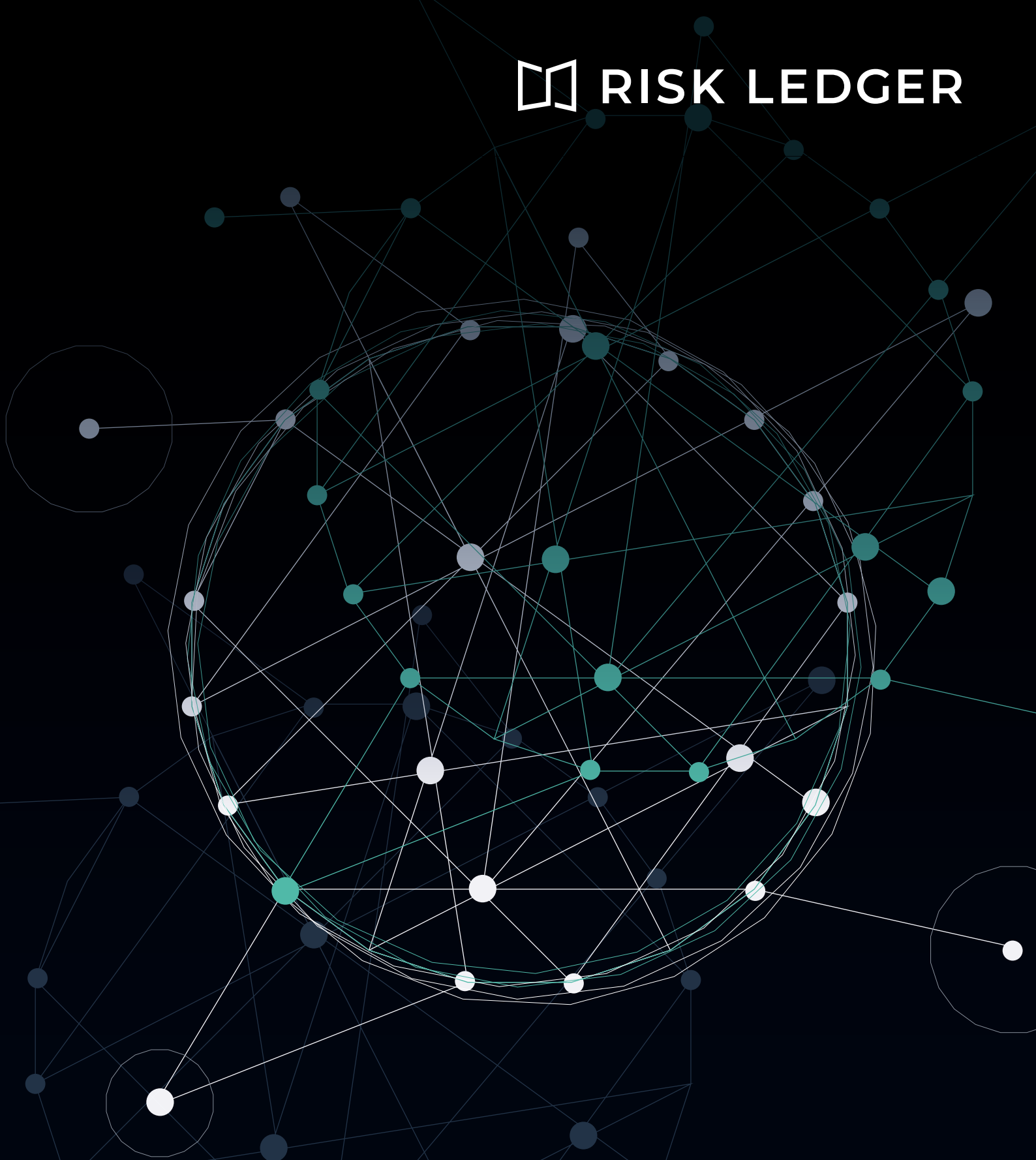
The UK energy sector stands at a pivotal moment. The convergence of IT and OT, coupled with the geopolitical prioritisation of CNI disruption by hostile state actors, has created a threat landscape of unparalleled complexity. As our report demonstrates, the industry is acutely aware of this danger—94% of professionals rank supply chain incidents as a top concern—but the tools they are using to fight it are falling short.

Traditional TPRM, with its reliance on periodic assessments and siloed data, has created a "visibility ceiling" that leaves 74% of the sector blind to deep-tier dependencies. In an era where a single vulnerability in a 4th-party software component can cascade through the national grid, this gap is not just a compliance failure; it is a resilience failure. The sector's own data confirms the need for change: 50% of organisations lack continuous monitoring of supplier controls, and there is a clear industry-wide demand for government-led mandates on collaboration and systemic risk identification.

The forthcoming Cyber Security and Resilience Bill represents a critical opportunity to close these gaps. By formalising the responsibility to manage Critical Suppliers and encouraging cross-industry intelligence sharing, the Bill aligns perfectly with the sector's own priorities. However, regulation alone is not the answer. True resilience will require a cultural shift towards a "Defend-as-One" strategy—leveraging shared platforms to map the ecosystem, monitor risks in real-time, and collectively fortify the digital supply chain.

In the UK energy sector, there is no such thing as an isolated incident. Every vendor, every component, and every connection is part of the same critical national machine. Securing it requires us to accept a fundamental truth: Every link matters.

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