techUK
FOR WHAT COMES NEXT

Supply Chain Security in Practice

Real-world strategies from techUK members

May 2026

Table of Contents

Introduction

It's an inescapable fact - the integrity of our supply chains has become synonymous with the UK's national and economic resilience. No longer can supply chain security be relegated to a niche procurement checkbox; it is a fundamental pillar of modern operational security. This playbook explores the multifaceted nature of these risks and provides a strategic roadmap for navigating the complexities of the digital and physical supply networks that underpin the UK's critical infrastructure and essential service.

The strategic imperative

The shift in the threat landscape has moved from localised disruptions to sophisticated, cross-border systemic vulnerabilities. Organisations today face a diversion of risk where sanctioned entities, cyber threats, and material shortages are often hidden behind layers of corporate obfuscation or fragmented data silos. To address these challenges, our priority areas focus on three core pillars: Visibility, Accountability, and Proactive Intelligence.

- **Visibility:** Moving beyond "Tier-1" oversight. Tier 1 is the traditional security and procurement practice of only monitoring and assessing an organisation's direct, immediate suppliers. We need to illuminate deep-tier dependencies, including raw material provenance and hidden beneficial ownership.
- **Accountability:** Shifting from passive contractual compliance to active, evidence-based governance where security is embedded into the entire lifecycle of a supplier relationship.
- **Proactive Intelligence:** Transitioning from reactive incident response to continuous monitoring, utilising data fusion, graph analytics, and automated vulnerability management/mitigation to identify risks before they materialise.

Lessons from the frontline

The case studies presented in this playbook illustrate how these principles are applied across diverse sectors, including defence, retail, and Critical National Infrastructure (CNI). You will find examples of:

- Technological Orchestration: How "zero-access" data handling and overlay architectures allow sensitive information to flow securely across the supply chain without any intermediary accessing the underlying data.
- Operational Resilience: The implementation of "Secure-by-Design" collaborative environments that allow multiple partners to work on sensitive projects within a unified, UK sovereign cloud boundary.

- Evidence-Based Governance: Strategies for using passive scanning and automated Software Bills of Materials (SBOMs) to verify the security posture of suppliers, ensuring that "compliance is the floor, not the ceiling".
- Consolidation and Standardisation: How simplifying fragmented supplier ecosystems into accountable frameworks reduces risk and strengthens resilience in critical national security supply chains

Supply chain security is not a standalone technical function but a shared responsibility that requires the alignment of procurement, engineering, operations, and security teams. As you explore these pages, the recurring theme is clear: transparency and collaboration are our strongest defences. By moving away from "point-in-time" assessments and audits and toward a model of continuous, data-driven assurance, we can build automated supply chains that are not only efficient but fundamentally resilient against the threats of tomorrow.

Chris Jenkins, Senior Principal Chief Architect in Red Hat's Field CTO Office

Compliance is the floor not the ceiling: An approach to closing the OT supply chain governance gap in UK critical national infrastructure

Amentum is a global mission-critical services and solutions company operating across defence, intelligence, and critical national infrastructure sectors, providing cybersecurity advisory and assurance services across complex supply chains.

Context and challenge

Across UK critical national infrastructure particularly in energy, water, and transport organisations have invested heavily in compliance frameworks. Many hold ISO 27001 certification and have assessed well under CAF v3.2. Yet as these organisations expand their use of remote monitoring, IIoT, and third-party managed services, a common pattern emerges: IT-centric governance fails to keep pace with the operational technology environments it is meant to protect.

Legacy protocols and firmware dependencies embedded in Tier-2 and Tier-3 telemetry supply chains frequently sit outside the scope of existing information security management systems. Third-party suppliers are assessed through contractual compliance clauses rather than active security evaluation. The release of CAF v4.0 with its emphasis on evidencing the effectiveness of controls rather than simply their presence is exposing this gap at scale across the sector.

Response

When Amentum UK engages with CNI operators facing this challenge, our approach is structured around three interconnected workstreams governance, assessment, and accountability designed to move organisations from a compliance posture to a resilience posture.

Governance first: bringing the right people into the room. The most common structural failure we encounter is fragmented ownership. Engineering teams understand the OT environment but don't think in threat models. IT security teams understand the threat landscape but lack visibility into operational constraints. Procurement manages supplier relationships but without security context. Our starting point is always to establish a cross-functional view of the OT supply chain mapping the full chain of components, firmware dependencies, remote access arrangements, and integration points between IT and OT networks. For many organisations, this is the first time that picture has existed in one place. The governance intervention often precedes any technical assessment, because without shared ownership, findings rarely translate into action.

Assessment aligned to CAF v4.0 contributing outcomes. Rather than mapping existing controls to the new Indicators of Good Practice on paper, we conduct active, evidence-based assessment. This means evaluating firmware provenance and update mechanisms, examining how third-party component vulnerabilities are tracked and acted upon, reviewing remote maintenance access controls, and testing logging and anomaly detection capabilities across OT-facing supplier interfaces. The work is explicitly aligned to CAF v4.0's "Understanding Threat" contributing outcome the question we are always asking is not "does this control exist?" but "does this control work, against the threats that are actually present?"

Building accountability into the supply chain. Findings from the assessment phase inform a redesign of how organisations manage ongoing supplier risk. This typically involves rewriting supplier assurance criteria to reflect CAF v4.0 requirements, incorporating the incoming obligations of the EU Cyber Resilience Act including secure by design requirements, software bills of materials, and vulnerability disclosure obligations applying from September 2026 and updating procurement frameworks to require evidence of active security practice rather than compliance attestation. Critically, we help organisations move from flowing requirements down through contracts to treating key suppliers as security partners, with shared visibility into threat intelligence and collaborative vulnerability management processes.

Throughout this work, our focus is on embedding accountability structurally rather than documenting it procedurally. The organisations that navigate the CAF v4.0 transition well are those that use it as a genuine diagnostic not a box-ticking exercise reframed for a new framework.

Outcomes and lessons learned

Across CNI sectors, the organisations that approach CAF v4.0 as an opportunity for honest reassessment rather than a compliance migration consistently surface risks that previous frameworks had not captured. The most common findings involve legacy firmware running outside active vulnerability management programmes, remote maintenance access that meets contractual requirements but would not withstand active scrutiny, and OT-facing supplier interfaces with insufficient logging to support meaningful anomaly detection.

The core lesson Amentum UK draws from this work is straightforward: compliance frameworks measure the presence of controls; they do not measure whether those controls work. Organisations managing OT supply chains should treat CAF v4.0 as a diagnostic opportunity, map EU Cyber Resilience Act obligations across their supply chain now rather than at enforcement, and bring engineering, security, and procurement into a shared governance structure before a regulator or an attacker forces the conversation.

Benjamin Byrne, Engineering Manager

When Procurement Signs the Contract and Security Disappears: Rebuilding Supply Chain Accountability Across a Critical Services Portfolio

Axiologik is a B-Corp certified digital, technology, and engineering consultancy operating across government, financial services, and critical infrastructure sectors, helping organisations assess and strengthen their cyber resilience and supply chain security posture.

Context and challenge

Across a series of cyber risk reviews we conducted with mid-market UK organisations in regulated sectors including financial services, pensions, and critical infrastructure services, we encountered a consistent and acute supply chain security challenge. Our clients had invested in security at the point of procurement: due diligence questionnaires, onboarding checks, initial contract negotiation. But none had a structured mechanism to sustain that assurance through the active supplier relationship.

In every engagement, critical third-party suppliers were providing platform services, managed technology, and operational systems without enforceable security obligations, audit rights, or ongoing monitoring. When we performed passive attack surface scanning across our clients' key suppliers (without requiring supplier cooperation) we found critical-severity vulnerabilities, including subdomain takeover risks and confirmed credential exposure in threat actor forums, of which our clients were entirely unaware. In one case, a major offshore technology supplier had credentials circulating in breach repositories and was actively susceptible to impersonation attacks. The client had no visibility of this. The root cause was structural. Procurement did not own cyber risk. Security assessments, where they existed, were conducted after contracts were signed. No client had secured a contractual right to audit their suppliers.

Response

Our response operated across three parallel workstreams, designed to address both the immediate evidence gap and the structural accountability failures we had identified.

Establishing a supplier risk baseline through passive assessment: The first and most urgent step was giving our clients actual evidence of their suppliers' security posture. Using Precursor Security's Edge Protect platform, we performed non-intrusive passive attack surface and vulnerability scanning across each client's critical supplier base. This required no supplier cooperation and produced severity-rated findings across each supplier's externally visible digital estate. Findings included critical-rated cloud subdomain takeover vulnerabilities, exposed SSH interfaces with weak encryption, unsupported and unpatched software versions listed in active exploit catalogues, susceptibility to email spoofing enabling threat actors to impersonate supplier personnel, and confirmed credential exposure across public breach repositories. In several cases, vulnerabilities were already being actively exploited in the wild against organisations in the same sector.

This established a supplier risk baseline grounded in external evidence rather than self-reported questionnaire responses. Our clients could now enter supplier conversations from a position of knowledge rather than assumption.

Rebuilding governance and contractual accountability: The second workstream addressed the structural gap directly. Working with each client, we developed a supplier risk framework that embedded security obligations into the procurement lifecycle rather than treating them as a post-signature concern. We introduced tiered supplier risk scoring based on criticality of access and data exposure, with the depth of assurance activity proportionate to each tier. We drafted minimum security obligations for inclusion in contract terms covering incident notification timelines, penetration testing cadence, audit rights, right to access security documentation, and termination rights for material security non-compliance. For existing suppliers where contracts lacked these provisions, we supported clients in identifying which relationships warranted renegotiation as a priority based on the risk evidence we had gathered. We also worked directly with procurement functions (not just security teams) to embed a cyber risk assessment gate into the supplier selection process. Identified risks above a defined threshold now require a formal risk acceptance decision at an appropriate governance level before contracts can be signed. This shifted ownership of supply chain cyber risk from the security function to the organisation as a whole.

Integrating supply chain security into the operating model: The third workstream ensured that supply chain security did not remain a parallel activity disconnected from how the organisation managed risk day to day. We integrated supplier security incidents into central security incident management processes, developed specific business continuity and disaster recovery scenarios for partial or full loss of critical supplier platforms, and extended monitoring scope to include the integration points: APIs, data feeds, and access pathways, connecting supplier systems to client infrastructure. These had previously been entirely outside the scope of security event detection. Throughout, we emphasised proportionality: minimum viable assurance for all suppliers, with deeper and more frequent assurance concentrated on those with privileged access or critical operational dependencies.

Outcomes and lessons learned

The most significant immediate outcome was visibility. Our clients had no prior view of their suppliers' external security posture. Through passive scanning, they gained actionable, evidenced findings they could act on directly and use to anchor supplier conversations in fact rather than assumption. Contract renegotiation discussions were materially strengthened as a result. Structurally, embedding cyber risk into procurement created accountability that had been entirely absent. Security was no longer something that happened at onboarding and then stopped.

The central lesson we take from these engagements is that supply chain security accountability cannot be created at the point of incident, it must be built into the commercial relationship from the outset. The highest-risk moment with a supplier is not during onboarding; it is six to twelve months into delivery, when nobody is looking. Ongoing monitoring, contractual audit rights, and defined incident integration are not enhancements. They are the minimum conditions for managing supply chain risk responsibly, and without them no organisation can genuinely claim to understand the risk its supply chain represents.

Terry Hancock, Head of Service Operations & Cyber Resilience

Creating a resilient and accountable defence training supply chain through Project Selborne

Capita is a UK-based, AI-enabled business process and services partner, operating across the public and private sectors to design, run and improve the delivery of essential services at scale on behalf of government, regulated organisations and businesses.

Context and challenge

The Royal Navy operates one of the most complex and safety-critical defence training systems in the UK, preparing sailors and Royal Marines across maritime, engineering, warfare and leadership roles. Prior to Project Selborne, this system relied on a fragmented supplier landscape, comprising 27 separate contracts delivered across multiple sites and disciplines. This created challenges around accountability, consistency, resilience and risk management, at a time of increasing operational complexity.

The legacy model limited the Navy's ability to adapt quickly to evolving threats, technologies and workforce requirements. Assuring quality and security across the full training pipeline—from initial entry to advanced specialisation—was difficult. In supply chain terms, responsibility for outcomes was dispersed, governance was complex, and the ability to respond coherently to disruption—whether geopolitical, technological or operational—was constrained.

These challenges were compounded by wider pressures affecting global defence supply chains:

- Growing reliance on digital systems, introducing new cyber and data risks.
- Increasing demand for globally deployable skills.
- The need to ensure workforce resilience and skills continuity over decades.

The Ministry of Defence and Royal Navy recognised that modernising training delivery was both a capability and supply chain security challenge, requiring a new model of accountability and partnership.

Response

Project Selborne was established as a 12-year strategic partnership, awarded in 2021 to Team Fisher, a consortium led by Capita alongside Raytheon UK, Fujitsu UK, Elbit Systems UK and the University of Lincoln. It was designed to transform around 80% of the Royal Navy's shore-based individual training, replacing fragmentation with a single, accountable delivery framework.

Selborne represents a shift from transactional outsourcing to a consolidated, outcome-focused supply chain, where responsibility for integration, performance and resilience is clearly owned. Key features include:

- Unified accountability: Replacing 27 contracts with one framework has simplified governance and created clear ownership for delivery, quality and risk, enabling faster and more coherent decision-making.

- Integrated, multi-partner delivery: Consortium partners operate within a shared delivery model, combining technology, training systems and digital infrastructure with academic accreditation from the University of Lincoln, embedding recognised qualifications into naval careers.
- Technology-enabled resilience: Modern learning platforms, digital content, virtual libraries and advanced simulators increase capacity and flexibility, reducing reliance on single points of failure.
- Global perspective, local delivery: Training is delivered across 14 UK sites, including HMS Raleigh and Britannia Royal Naval College, supporting tens of thousands of learners annually while allowing adaptation to operational contexts.
- Long-term skills assurance: Apprenticeships and accredited education—covering over 90% of recruits in some areas—support the sustainability and transferability of critical skills.

Outcomes and lessons learned

Since April 2021, Project Selborne has delivered measurable improvements:

- Streamlined supply chain management through a single accountable partnership.
- Ofsted 'good' ratings across all establishments within scope.
- Delivery of hundreds of training pathways across engineering, warfare and leadership disciplines.
- Consistent training provision to tens of thousands of learners each year.
- Demonstrated adaptability, including the 2025 expansion to marine engineering training (c.£97m).

Public reporting values the programme at approximately £1.2bn–£1.3bn over its lifetime, reflecting its strategic importance to defence capability and resilience.
Beyond delivery, Selborne has strengthened supply chain security and national resilience:

- Reduced systemic risk through consolidation and clearer accountability.
- Improved adaptability, enabling faster updates in response to emerging threats and technologies.
- Strengthened public-private collaboration, integrating industry, academia and defence into a single delivery ecosystem.
- Enhanced workforce resilience, with professionalised training roles underpinned by recognised qualifications supporting retention and long-term capability development.

These impacts demonstrate how supply chain design directly influences operational readiness and security.

Why this matters for UK supply chain security:

Project Selborne shows how consolidating fragmented supplier ecosystems into accountable, partnership-based frameworks can reduce risk and strengthen resilience in critical national supply chains.
For the UK, where defence, digital and skills systems face increasing disruption, Selborne highlights three key lessons:

- Accountability matters more than scale alone.
- Long-term partnerships enable sustained investment in resilience and skills.
- Integrated governance is a foundation for security, not an administrative overhead.

Steve Andrews, Head of Service Portfolio

Strengthening multi-tier supply chain resilience in UK public sector procurement - Rare earth exposure in supply chains

Dun & Bradstreet supports UK public sector procurement teams in improving supply chain security and resilience through data-led supplier intelligence, multi-tier supply chain mapping, risk analytics and compliance screening.

Context and challenge

In this case study, Dun & Bradstreet Limited carried our detailed analysis around rare earth elements as the public and private sector alike are dependent on these for consumer electronics, wind turbines, aerospace and defence, to name a few.

Response

UK public sector organisations rely on complex, multi-tier supply chains to deliver critical infrastructure and essential services. However, procurement visibility typically stops at tier 1 or 2, limiting the ability to spot upstream concentration risks and security or resilience issues embedded in components and materials.

The challenge was to identify where likely rare earth dependency existed across a sample set of organisations so that Department's category leads could understand risk, which looked at suppliers beyond tier 1 and prioritise practical actions where disruption could affect service continuity and delivery commitments.

The process was to apply a structured, data-led workflow to move from a "tier 1-only" view to a multi-tier, contract-linked understanding of risk and resilience, and to turn that insight into accountable actions for the Departments.

Build a single, supplier view aligned to actual spend

The proxy supplier data, including the identifiers, addresses, and categories, was matched to the D&B Data Cloud to apply a business identifier the D U N S® Number for entity resolution purposes, so standardising names and addresses, resolving duplicates and connecting subsidiaries to global parents. This created a consistent baseline for analysis and reduced the risk of missing exposure due to fragmented supplier records.

Identify suppliers likely to embed rare earths

Taking example rare earth elements, suppliers were segmented to isolate those most likely to rely on these across the Departments' relevant supplier portfolios– typically, specialist component and original equipment manufacturers (OEMs), for example, those building mobile phone and electric vehicles. Outputs included a ranked list of suppliers with likely exposure, the types of products driving that exposure, and early concentration indicators (e.g., single-source reliance, limited geographic diversity and corporate linkage concentration).

Illuminate upstream dependencies beyond tier 1

The approach expanded the supplier view using additional data sources such as trade payment, shipping logistics data to identify global suppliers and their upstream trading links (tier 2/3 and, where supported, tier 4/5). We scoped the exercise around critical contracts and components, resolved entities to the same identity standard, and normalised key attributes (industry, location, corporate group). Then relationships were validated using checks, for example sector fit, geography and linkage logic and produced network views to highlight shared dependencies and potential choke points (high-dependency nodes and geographic clustering).

Apply consistent risk and resilience analytics across tiers

The suppliers were then screened across the network using a common set of indicators: global corporate ownership clarity and linkage, Dun & Bradstreet proprietary financial health scores and ratings signals, geographic and concentration risk, compliance screening (e.g., sanctions/watchlist exposure where applicable), ownership/control red flags (including complex ownership chains and government-linked entities where relevant), ESG-related indicators, as well as Cyber Risk ratings.

These also aligned to public sector procurement obligations, and operational resilience factors such as site dependence and criticality to multiple tier 1 suppliers. This approach allows Departments to overlay multi-tier risk back onto the Tier 1 contracted suppliers to prioritise mitigations where disruption would have the greatest service impact or longest recovery time.

Outcomes and lessons learned

The analysis helped define how Departments can monitor, escalate, and manage identified risks through defined governance.

Supporting targeted supplier engagement, such as transparency requests, resilience planning and automated questionnaires, as well as data driven identification of comparable alternative suppliers to inform dual sourcing strategies, framework expansion and broader contingency planning.

The process highlighted areas where risk visibility was limited and where potential upstream raw-material exposure pathways, inferred from supplier site location and a broader assessment of country risk, using the Dun & Bradstreet Country Risk multi-dimensional analysis (MDA scores).

This informed on good practice - to resolve entities to a common identifier, to allow for supply chain mapping for critical suppliers beyond tier 1, apply risk indicators, validate upstream sites, and link findings to contracts with clear mitigations such as dual sourcing, supplier engagement and ongoing monitoring.

Patrice Bendon, Client Success Director - Public Sector

From reactive response to shared accountability in supply chain cyber security

Littlefish Group is a UK-based provider of managed IT, digital transformation, and advanced cyber security services, operating across the public and private sectors and acting as an operational security partner that delivers monitoring, response, and assurance across customers and their supplier ecosystems.

Context and Challenge

Long Clawson Dairy operates within a complex supply chain that includes third party technology providers, suppliers, and partners supporting core business and operational systems. As cyber threats continued to increase in sophistication and the organisation's attack surface expanded, it became clear that cyber risk could not be effectively managed through internally resourced teams alone.

The organisation required a security operating model that provided continuous monitoring, specialist response capability, and independent assurance, while also demonstrating to customers, partners, and regulators that cyber risks were being managed proactively and could be evidenced. Key challenges included limited visibility across systems and suppliers, the risk of delayed or inconsistent incident response, and the need to reduce exposure to common causes of compromise such as phishing and known technical vulnerabilities. Without a coordinated approach, supplier or user originated incidents had the potential to disrupt core operations and undermine confidence in the wider supply chain.

Response

To address these challenges, Littlefish Group worked with Long Clawson Dairy to design and deliver a fully managed MDR SOC service that strengthened visibility, accountability, and assurance across the organisation and its supporting supply chain.

The service was built around Microsoft Sentinel as the central SIEM and XDR platform, providing a consolidated view of security events and enabling consistent detection, investigation, and response. This was supported by threat intelligence feeds to improve contextual awareness, alongside phishing simulation, user education, and vulnerability management to reduce risk at source. These capabilities were integrated with the Littlefish ITSM platform, ensuring incidents were handled through clear workflows with defined ownership, escalation, and communication processes. From the outset, Littlefish focused on governance as well as technology. Clear roles and responsibilities were agreed across internal teams and relevant third-party providers, with documented escalation paths to remove ambiguity during security events. Structured reporting and regular service reviews were established to provide ongoing oversight, accountability, and assurance to stakeholders.

An initial engagement phase was used to confirm priorities, define service scope, and identify the systems and suppliers presenting the greatest potential risk. This allowed delivery to be phased and focused where it would deliver the most operational value, rather than applying controls uniformly. Success criteria were aligned to operational risk reduction and business impact, rather than compliance alone.

Throughout the engagement, Littlefish Group maintained close collaboration with the customer and third-party providers to validate assumptions, refine detection and response requirements, and ensure the service evolved in line with operational and supply chain needs. User Education and Awareness initiatives were also introduced to reduce the likelihood of phishing and social engineering incidents, while Vulnerability Management enabled the identification, prioritisation, and remediation of technical weaknesses before they could be exploited.

Together, these actions established a coordinated operating model that combined continuous monitoring, preventative controls, and structured governance, embedding cyber security into day-to-day operations rather than treating it as a standalone compliance activity.

Outcomes and lessons learned

The engagement resulted in improved visibility, control, and assurance across the customer's environment and its wider supply chain. Centralised monitoring and response enabled earlier detection and more consistent handling of security events, reducing the likelihood that incidents originating from users or suppliers could impact core operations. Clear governance and escalation improved response effectiveness and accountability, while regular reporting provided ongoing insight into security posture and trends.

Key lessons included the importance of early stakeholder engagement, clearly defined ownership, and proportionate application of controls based on business impact. The case study demonstrates that supply chain cyber risk is most effectively managed when detection and response are combined with preventative measures such as user education and vulnerability management, and when security responsibilities are embedded into operational processes and maintained through ongoing collaboration.

Mike Buckley, Technical Cyber Security Consultant

Credential Orchestration for Defence Supply Chain Visibility

Origin Secured is a UK-based credential orchestration platform operating in the defence and national security sector, enabling supply chain data to flow securely from industry to government without any intermediary accessing the underlying information.

Context and challenge

The UK Ministry of Defence requires supply chain data from thousands of suppliers across hundreds of Defence Conditions (DEFCONs). Suppliers submit the same information repeatedly, in different formats, for different contracts, teams, and DEFCONs, consuming significant resource capacity across industry. MOD built an internal tool to aggregate this data, but had no automated, secure mechanism to collect it from industry at scale. Primes and sub-tier suppliers were managing submissions manually through spreadsheets, tools, documents, and email, with no standard format and no standard method. Data was often out of date on the day it was submitted. The core challenge was not a lack of data, but the absence of a trusted, automated mechanism to move it from industry to MOD without creating additional bureaucracy, data exposure, or duplication of effort. Key stakeholders included the MOD programme team, four prime contractors, and Origin Secured as the technology provider.

Response

Origin Secured partnered with a MOD programme team to design and deliver a credential orchestration capability that automates the flow of supply chain data from industry into MOD's internal systems. The programme began with DEFCON 565 supply chain data and is being rolled out across prime contractors, with the ambition to extend to the wider supply chain by 2027.
The programme is built on three technical principles that directly address the security and trust barriers that had prevented previous attempts at automation.

First, overlay architecture. Origin Secured's platform sits on top of suppliers' existing systems, whether ERP, CRM, SharePoint, or any other tool already holding the relevant data. There is no requirement to replace existing technology, adopt new systems, or change internal processes. Data is captured in the format suppliers already use and transformed for MOD consumption automatically. This removes the most common adoption barrier: the expectation that suppliers must invest in new infrastructure to participate.

Second, zero-access data handling. Origin Secured's technology moves supply chain information from industry to MOD without the platform operator ever seeing, storing, or processing the underlying data. The architecture uses hardware-attested trusted execution environments and end-to-end encryption so that data is inaccessible in transit and at rest within the platform. There is no third-party data store and no intermediary holding supplier information.

This addresses the primary security concern raised by primes: the sensitivity of sharing supply chain data through any external system.

Third, direct automated delivery. Data flows from the supplier directly to MOD's internal systems on a daily, automated basis. Origin Secured handles the orchestration, transformation, and delivery without retaining a copy of the data. Each interaction is recorded on an append-only cryptographic audit trail (the Event Chain), providing full provenance, attribution, and tamper evidence for every data point. Independent verifiers can endorse data within the same framework, adding a layer of trust that is absent from manual submission processes.

The programme has demonstrated the full end-to-end workflow with prime contractors: data ingestion in the same format used for operational DEFFORM 565 submissions, Digital Licence creation for participating entities, credential verification, Event Chain audit recording, and export in the format required by MOD's internal systems. The programme achieved 100% of its technical and operational success criteria across all six measured areas.

The MOD programme lead co-presented the programme at DPRTE 2026, publicly endorsing the ambition to onboard all prime contractors by end of 2026 and extend to the wider supply chain by 2027. The programme has also identified four areas where MOD action will accelerate adoption: clarification of data classification for supply chain information flowing through the platform, hosting within MOD's cloud environment, the overlay integration approach as the default, and a clear roadmap to ensure stakeholder buy-in across both MOD and industry.

Outcomes and lessons learned

Following DPRTE 2026, Origin Secured was approached by a number of MOD Suppliers requesting inclusion in the programme. Four systems integrators and resellers expressed interest in channel partnerships to accelerate deployment. The programme is now moving into prime onboarding, with several large MOD prime partners among the next introductions.

The primary lesson is that the technology barrier to automating defence supply chain data is already solved. The real barriers are administrative: data classification governance, stakeholder buy-in, and internal change management within both MOD and industry. Organisations managing similar supply chain security challenges should prioritise overlay approaches that work with existing systems rather than requiring suppliers to adopt new ones, ensure data handling architectures eliminate the need for trust in the platform operator, and invest in stakeholder engagement as early as the technology development itself.

Stuart Kenny, CEO and Co-Founder

UK Sovereign Supply Chain Security & Application Hosting

Prolinx deliver trusted, UK sovereign secure multi domain, managed cloud services that assures the UK's Protectively Marked and IP data, enabling edge to enterprise interoperability and collaboration. We work across Industry, Government, CNI and Academia.

Context and challenge

A global engineering and advisory firm was scaling its UK public sector portfolio, with rapid growth in Defence and Security programmes delivered with multiple delivery partners and specialist subcontractors. Project teams needed to collaborate across organisational boundaries while protecting intellectual property and meeting UK government handling requirements for OFFICIAL SENSITIVE information. The key challenge was that prime contractors existing IT environments were not assured to handle this classification of data, nor were they able to provide a secure access method for their supply chain (including SMEs with immature infrastructure) to collaborate. Their existing infrastructure created a risk of sensitive data exposure through external public-cloud and un-assured on premises hosting. This included unmanaged contractor devices and inconsistent security controls with potential impact including loss of IPR, non compliance and programme delays.

Response

Prolinx were selected to implement and operate a secure collaborative working environment ("Citadel Secure") hosted in a UK sovereign cloud assured at OFFICIAL SENSITIVE. This solution is a productised, secure-by-design service (SBD) that has been developed to provide supply-chain resilience across industry partners working on sensitive programmes for the UK MOD.

First, the solution gave teams reliable access to the applications and data they needed wherever they were working without fragmenting work across multiple non-secure networks or uncontrolled endpoints. This was achieved by deploying a combination of enhanced GPU Virtual Desktops for each partner, accessed via their corporate device, or a dedicated Prolinx-managed secure laptop. The environment delivered a familiar end-user experience, including Microsoft 365 software and a secure deployment of up to 80+ specialist applications, including high end graphics software and PLM tools. This ensured sensitive datasets and processing was inside the UK sovereign cloud, reducing exposure from local installs and unmanaged endpoints.

This gave project teams a reusable OFFICIAL SENSITIVE workspace that removed day to day friction while improving control of sensitive data and intellectual property. This provided the customer with the following outcomes:

- Teams could keep using the specialist tools they already relied on (Bring Your Own Applications), while the platform hosted them centrally at OFFICIAL SENSITIVE.
- New projects could be mobilised faster because VMs and workloads could be deployed rapidly and capacity could be scaled as demand grew.

- Users accessed the required specialist applications in one assured workspace, with a consistent experience and less switching between networks or environments.
- Teams could work securely from anywhere and onboarding to projects was faster through standard role profiles and repeatable provisioning for internal staff and delivery partners.

Second, the service provided strict governance and access management to reflect third party participation. Role based access and least privilege were enforced for all users of the service. Controls were embedded across all architecture and infrastructure. Data protection focused on preventing unauthorised data import and export with clear handling rules aligned to secure-by-design for OFFICIAL SENSITIVE material.
Third, the assurance could scale with project demand. Prolinx delivered the platform as a fully managed service, covering service desk, provisioning, application publishing and ITIL aligned processes / practices. This reduced supply chain risk by removing reliance on ad hoc partner IT practices and ensuring consistent controls across programmes. Innovation was enabled through controlled sandboxing so teams could safely experiment, validate and launch new tools within the OFFICIAL SENSITIVE boundary.

Finally, resilience and growth were baked in from the outset. The platform was engineered for high availability with the ability to scale on demand for new projects, new partners and peaks in CAD / engineering workloads without redesigning the control set. This delivered operational agility, faster deployment, scaling and adaptation as programme needs changed. Capacity, licensing and application onboarding were managed through agreed service processes and Prolinx provided transparent supplier management and cost control as usage expanded.

Outcomes and lessons learned

The organisation onboarded up to 500 users with minimal disruption and enabled secure collaboration across multiple Defence and Security programmes while keeping data and IPR inside a UK sovereign environment. Centralised controls reduced dependence on individual partner tooling and lowered the risk from unmanaged contractor endpoints, misconfiguration and inconsistent handling practices.

Key lessons were:

• Treat identity and onboarding / offboarding as a supply chain control.
• Use secure-by-design assured VDI and UK sovereign hosting to keep sensitive processing and data within a controlled boundary and minimise data at-rest on unsecured and unmanaged devices.
• Invest in user adoption to prevent workarounds.

Building on this foundation, the customer is now reviewing a move to Fortress Red at SECRET to support higher classification programme needs.

Steve Andrews, Head of Service Portfolio

How Local Authorities are defending-as-one Against Supply Chain Cyber Risk

Risk Ledger is a network-first platform delivering Active Supply Chain Security.

Context and challenge

UK local authorities are providers of essential public services that require the processing of sensitive citizen data, including social care, financial, and voting records. As these councils are undergoing a digital transformation, they have become increasingly dependent on a complex web of thousands of external suppliers and service providers, including third-party home care providers, waste collection contractors, or ICT vendors. This entire ecosystem is supported by governing bodies like NCSC, the Ministry for Housing, Communities and Local Government (MHCLG), and regional Warning, Advice and Reporting Points (WARPs). Risk Ledger provides the collaborative Third-Party Risk Management (TPRM) platform on which a group of 31 councils have come together to collaborate to improve their supply chain security postures.

Today, local authorities face a plethora of rising supply chain threats and systemic fragility. Industry research found that 86% of UK councils experienced a supply chain cyber incident in the past year alone. A prominent example occurred in June 2025, when a vulnerability in a third-party contractor for Glasgow City Council's ICT provider disrupted essential services, including online planning, pension portals, and election-related forms. Contributing factors to supply chain incidents likes these include fragmented, outdated IT infrastructures, limited financial resources, and a shortage of skilled cyber security personnel. Crucially, traditional TPRM processes that rely on manual spreadsheets are inefficient and not scalable, are not providing visibility into extended supply chain dependencies and shared systemic risks, or allowing for a more effective incident response in times of emerging threats.

Response

Recognising that no council can secure its supply chain in isolation, a group of 31 UK councils, supported by regional WARPs across Scotland, England and Wales, came together and partnered with Risk Ledger to transition from manual, siloed processes to a collaborative "Defend-as-One" model. This transformation centered on the adoption of the Risk Ledger platform, which uses a unique "social network" approach to TPRM. Instead of every council sending separate questionnaires to each of their individual suppliers, suppliers using Risk Ledger maintain a standardised security profile, mapped against international standards like ISO27001 and the NCSC CAF, on their products, services, and internal security controls. This profile is shared instantly with all connected clients on the platform, significantly reducing "audit fatigue" and improving supplier engagement.

This shift towards a new and more collaborative model of TPRM involved significant changes across technology, governance, and supply chain collaboration for UK councils, but brought immediate benefits.

Technological and Process Transformation: The participating councils joined Risk Ledger's cloud-based platform to automate and standardise their TPRM activities. This allowed councils to instantly connect with a majority of their third-party suppliers. They found on average that at least 75% of these suppliers were already on the platform, which meant they could instantly connect with them and review their already completed and peer-vetted security assessments, significantly reducing the administrative burden and common onboarding frictions.

Governance and Collaboration: The initiative was led by regional WARPs, such as ISfL and SEGWARP, which established a dedicated "community" for the participating councils on the Risk Ledger platform. Through this community, participating councils agreed to securely share supplier risk intelligence and overlay their respective supply chain network maps. This collective governance allowed for:

- **Systemic Risk Identification:** Councils gained visibility beyond immediate third parties into 4th and nth-party dependencies, uncovering hidden concentration risks that could trigger sector-wide failures.
- **Continuous Monitoring:** The platform provides real-time alerts when a supplier's security controls change, enabling a proactive defence rather than a reactive posture.
- **Coordinated Remediation:** Security teams now collaborate directly with suppliers on the platform to mitigate risks. Peers can collaboratively lobby unresponsive suppliers, using their combined commercial strength to incentivise better security practices.

Alignment with National Strategy: The initiative aligns with the UK Government Cyber Security Strategy by improving the understanding of supplier dependencies. It also helps councils meet the specific requirements of the Local Government CAF (LG CAF) regarding supply chain governance. By centralising visibility, the sector has moved from a fragmented approach to a unified network capable of rapid, coordinated incident response

Outcomes and lessons learned

The collaborative community of 31 councils (& growing) connected and is monitoring a total of 995 direct third party suppliers on the platform, which has revealed another 2017 additional supplier dependencies across these councils n-th parties, from the 4th all the way down to the 8th party tier. Most importantly, the platform was able to identify 84 potential concentration risks that were previously invisible to these councils, including 8 direct third parties, connected to at least 50% of the participating councils.

Security improved materially:

- Councils identified 17% of their suppliers did not have Cyber Essentials certification.
- Councils also found 33% of suppliers have yet to sign up to the Early Warning system, which the NCSC has encouraged material suppliers to do.
- Since joining the platform, Risk Ledger has published 6 emerging threats (Like Axios NPM Package), notifying councils on whether their suppliers are affected, investigating or remediating, significantly speeding up their ability to identify whether and how their supply chains might be impacted.
- ctionable insight like these allowed for targeted remediation and improved resilience across the sector.

Lessons and Recommendations:

- Collaboration is Force Multiplication: No single organisation can secure its chain in isolation; pooling intelligence is the only way to uncover nth-party systemic risks.
- Standardisation Benefits Everyone: Using a standardised assessment framework reduces the burden on suppliers, making them more responsive.
- Visualisation is Essential: Organisations should map entire ecosystems to identify single points of failure where a disruption could cascade across the sector.

Patrick James, Local Authorities Lead

Strengthening Supply Chain Visibility and Risk Management in Retail through Continuous Monitoring

SCC is a UK-based IT solutions provider supporting organisations across public and private sectors with cyber security, infrastructure, and digital transformation services.

Context and challenge

An established UK fashion and clothing retailer with a growing e-commerce presence was increasingly reliant on a diverse network of third-party suppliers, including logistics providers, payment platforms, and overseas manufacturers. This created a broad and largely unmanaged digital supply chain footprint.

The retailer had limited visibility of cyber risk across its suppliers and no consistent way to assess or monitor third-party exposure. Concerns were raised following a series of high-profile retail breaches linked to compromised suppliers, as well as internal audit findings highlighting gaps in supplier assurance processes. In particular, the business lacked the ability to identify vulnerabilities, detect compromised credentials, or understand how supplier risk could impact core operations such as online sales and distribution.

From a governance perspective, the organisation was also under pressure to demonstrate stronger alignment to recognised frameworks such as ISO 27001 and NIS-style controls, particularly around supplier risk management and continuous assurance. Existing processes relied heavily on periodic questionnaires, which were proving insufficient in evidencing ongoing control effectiveness.

The challenge was to introduce a scalable and continuous approach to supply chain security without creating additional operational overhead or slowing down supplier onboarding.

Response

SCC worked with the retailer to design and implement a more proactive and intelligence-led approach to supply chain security, centred around CrowdStrike's supply chain monitoring capabilities within the Falcon platform.

The first step was to establish a clear inventory of critical suppliers. SCC facilitated workshops with IT, security, and procurement stakeholders to identify and prioritise suppliers based on their access to systems, data sensitivity, and operational impact. This created a defined scope aligned to both business risk and governance requirements. CrowdStrike was then deployed to provide continuous monitoring of the retailer's supply chain. This enabled visibility into supplier risk indicators such as exposed credentials, vulnerabilities, misconfigurations, and signs of compromise. Moving away from static, point-in-time assessments, the retailer gained real-time intelligence that could be acted on quickly and consistently.

Alongside the technology, SCC supported the introduction of a more structured governance model. This included defining clear ownership of supplier risk across teams, setting risk thresholds, and establishing escalation paths for identified issues.

The approach aligned closely with control requirements under ISO 27001 Annex A supplier relationships and NIS principles around supply chain risk management, allowing the retailer to demonstrate stronger control maturity and audit readiness.

Crucially, the solution was embedded into existing business processes. Insights from CrowdStrike were integrated into supplier onboarding, and likely in the future, procurement decision-making. This will ensure that security considerations become part of standard supplier governance rather than an isolated technical function.

SCC also are planning to provide ongoing advisory support, helping the retailer interpret findings, engage constructively with suppliers where risks were identified, and refine internal processes. This should include supporting internal reporting, enabling the business to evidence continuous monitoring and control effectiveness to both internal stakeholders and external auditors.

Outcomes and lessons learned

The retailer achieved a step change in visibility and control across its supply chain, moving from reactive, questionnaire-led assurance to continuous monitoring supported by real-time intelligence. This reduced the risk of supplier-related incidents impacting critical operations such as online sales and fulfilment.

From a governance perspective, the organisation was able to demonstrate improved alignment to recognised frameworks, with clearer ownership, better evidence of control effectiveness, and stronger audit positioning.

A key lesson was that effective supply chain security requires more than periodic assessments. Continuous monitoring, combined with clear governance and cross-functional ownership, provides a far more robust and scalable approach. Organisations facing similar challenges should focus on integrating security into supplier management processes rather than treating it as a standalone activity.

Richard Hodgson, Security Sales Manager

Finding the needle in the haystack - Prioritising vulnerabilities that really matter

Stackable builds the Stackable Data Platform (SDP), an open source distribution of 15 data applications and 16 Kubernetes operators, serving as an upstream technology provider in the data platform supply chain.

Context and challenge

The Stackable Data Platform (SDP) is a Kubernetes-native distribution that bundles 15 open source data applications, including Apache Kafka, Apache Airflow, and other projects, together with 16 Stackable-developed Kubernetes operators. A significant share of our customers are public sector and financial institutions, operating under regulatory regimes such as the EU's Digital Operational Resilience Act (DORA), which makes supply chain security a first-class concern for them and, by extension, for us.

The core challenge is scale. SDP is a very large code base with a deep dependency tree, most of which sits outside our direct control. Vulnerability scanners surface a large number of known CVEs across these dependencies. Layered on top of this, the EU Cyber Resilience Act (CRA) will require reporting of actively exploited vulnerabilities from 11 September 2026. Without a structured approach, our security team risks drowning in scanner output and losing sight of the vulnerabilities that genuinely matter to our customers.

Response

We built a risk-based vulnerability management pipeline around open source tooling, designed to move from raw scanner noise to a prioritised, actionable set of findings, and to communicate that status transparently to downstream consumers.

Generating comprehensive Software Bills of Materials (SBOM)s: The foundation is an accurate, complete Software Bills of Materials for every component we ship. We generate SBOMs as part of our build pipeline so that every released artefact has a corresponding machine-readable inventory of its dependencies, including transitive ones. Without trustworthy SBOMs, everything downstream, scanning, prioritisation, analysis and reporting, rests on shaky ground.

Scanning and managing vulnerabilities with open source tools: We feed these SBOMs into the open source vulnerability scanners Trivy and Grype and import the scan results into the vulnerability management system SecObserve, that aggregates findings across components, tracks their state over time, and prevents the same CVE from being re-triaged several times. Using open source tooling keeps our stack aligned with the ethos of the product itself and avoids lock-in.

Enriching vulnerabilities with exploit information: Raw CVE data is not enough to judge real-world risk. We enrich findings with information about whether a vulnerability has known exploits from sources such as CISA KEV, Metasploit and others, or is likely to be exploited by using the Exploit Prediction Scoring System (EPSS) score.

This enrichment is what ultimately lets us satisfy CRA-style reporting expectations, which centre on actively exploited vulnerabilities rather than the full universe of theoretical ones.

Risk-based prioritisation rules: On top of enriched data we apply explicit, documented prioritisation rules. These combine factors such as severity and exploitability. The goal is to separate the small number of findings that require urgent action from the long tail that can be analysed with a lower priority at a later time.

Analysis and treatment: Prioritised vulnerabilities then flow into an analysis and treatment workflow: Supported by a custom AI skill we check all relevant information including the description of the vulnerability, the hierarchy of how the dependency is imported and the source code of the vulnerable library and its callers to assess if the product is affected by the vulnerability and its real severity in our setup. Depending on this assessment we decide how to treat the vulnerability, e.g. update the affected library to a newer version, document a workaround or document why our product is not affected.

Communicating status with VEX: Finally, we publish our assessments as Vulnerability Exploitability eXchange (VEX) documents alongside our SBOMs. This gives customers a machine-readable statement of which CVEs genuinely affect which SDP components, instead of forcing them to re-derive that analysis themselves.

Outcomes and lessons learned

The result of our approach is a shift from reactive scanner-chasing to a sustainable, risk-based process. Engineers spend their time on the vulnerabilities that actually matter, while customers in regulated sectors receive SBOMs and VEX documents that plug directly into their own supply chain security and regulatory workflows. This makes SDP materially easier to operate under frameworks such as DORA and the upcoming CRA reporting obligations.

Key lessons for organisations facing similar challenges: invest early in high-quality SBOMs, because every downstream control depends on them; treat prioritisation rules as a first-class, written artefact rather than tribal knowledge; enrich CVE data with exploit context before triaging, let AI do some of the heavy analysis lifting; and use VEX to communicate results - silent fixes or unstructured advisories do not scale across a complex supply chain.

Stefan Fleckenstein, Chief Information Security Officer

Navigating global complexity: Leveraging global data fusion to uncover hidden supply chain risks

YC World is an international data analytics platform that enables due diligence, compliance, supply chain security, AML/CFT procedures, and sanctions compliance for both companies and individuals. It uncovers hidden connections and consolidates official company data, UBO networks, politically exposed persons, sanctions lists, and high-risk indicators across 82+ jurisdictions, providing a single workspace for comprehensive risk assessment and operational security.

Context and challenge

The primary challenge is the extreme fragmentation of global supply chain data. Traditional KYC/KYB/KYCC tools often operate within national silos, failing to detect sophisticated "transshipment" schemes where high-priority dual-use goods (e.g., CNC machines) are diverted to sanctioned entities via third-country intermediaries (e.g.,Turkey or the UAE).

Our analysis based on open data enables interested parties to identify and take into account a significant security gap: high-precision equipment from European manufacturers reaching the Russian defense complex despite active sanctions. The key contributing factor is the use of "shell" companies—entities with no prior history in industrial tech (e.g., former tobacco traders) suddenly importing military-grade hardware.

This lack of transparency undermines UK and international sanctions, creates immense reputational and legal risks for manufacturers, and directly contributes to the proliferation of weapon systems. Without cross-border data correlation and historical UBO (Ultimate Beneficial Owner) tracking, organisations remain blind to these hidden networks.

Response

To address these systemic vulnerabilities, YC World implemented a multi-layered technological approach that shifts supply chain security from reactive compliance to proactive intelligence. The core of our response is to uncover hidden insights and show sanctioned entities that are kept behind complex corporate structures.

Data Fusion and Global Integration - The primary action was the aggregation of over 350 data sources, including national business registries, real-time customs databases, and international sanctions lists from 82+ jurisdictions. By centralising this data, we eliminated the "national focus" blind spot. For the tech sector, this means a UK company can instantly verify if a new distributor in a third-party country has sudden, unexplained links to high-risk regions or prohibited end-users. Advanced Graph Intelligence for Hidden Connections - We deployed Graph Visualization technology to map corporate ecosystems. Instead of reviewing entities in isolation, our platform automatically builds relationship webs.

This allows compliance officers to identify "hidden connections"—for instance, where a seemingly independent Turkish trading hub shares a historical UBO (Ultimate Beneficial Owner) or a physical address with a sanctioned Russian defense contractor. This visual audit trail is essential for identifying "shell" companies that have been rapidly repurposed to bypass export controls.

Deep Compliance: UBO, PEP, and Sanction Linkage - Our technology automates the identification of Politically Exposed Persons (PEPs) and their close associates within the supply chain. By cross-referencing historical ownership data with real-time sanctions updates, YC World detects attempts to obfuscate control through "proxy" owners or family members. We provide not just a risk score, but a direct link to the original source documents, ensuring that every red flag is verifiable.

Continuous Monitoring and Historical Analysis - We moved beyond "point-in-time" checks. The platform tracks historical changes in corporate structures, enabling organisations to see if a partner changed its ownership or business focus (e.g., from consumer goods to industrial components) just as new sanctions were implemented. This "time-series" analysis is a critical enabler for detecting pre-emptive sanctions evasion.

Process Transformation - These technological measures allow for a standardised, repeatable process applicable to every link in the supply chain. Whether it is a routine onboarding of an SME supplier or a deep-dive investigation into a global distributor, the same rigorous data-driven scrutiny is applied. This collaboration-ready format allows stakeholders across the supply chain to share intelligence and maintain a unified security posture against sophisticated trans-border threats.

Outcomes and lessons learned

Implementing a deep data analysis approach allows for the transformation of compliance processes into a system of proactive risk detection. Leveraging Open Data analytics enables the identification of complex cross-border networks and hidden beneficial ownership links that are difficult to detect during standard reviews. This approach creates the conditions for pre-emptively avoiding reputational threats and secondary sanctions by providing a detailed analysis of affiliated structures across various jurisdictions during the counterparty assessment or supply chain audit phase. Working with obscured supply networks demonstrates the importance of a comprehensive approach that extends beyond local registries.

Recommendations:

- Global Visualisation: Use graph analysis to uncover connections between beneficiaries and sanctioned entities across multi-layered intermediary structures.
- Historical Data Analysis: Review changes in ownership structure retrospectively to identify newly established intermediary firms.
- Unified Data Sourcing: Base decisions on verified primary sources from multiple jurisdictions (80+) simultaneously to eliminate information gaps within supply chains.
- Automated real-time monitoring is vital as yesterday’s data may already be outdated; the ability to instantly refresh graphs ensures a dynamic and accurate visualisation of current supply chain connections.

Nataliia Chornohub, CEO YC World & Open Data Director

Securing and streamlining supply chain engagement

Zscaler is a cloud cybersecurity provider, operating in the technology/SaaS sector, and plays the role of a security and access-control platform vendor that helps organisations and their suppliers securely connect to applications, data, and third-party services across the digital supply chain.

Context and challenge

In this case study, we supported a UK-headquartered organisation operating across multiple regions with a complex digital supply chain spanning SaaS providers, cloud infrastructure, managed service partners, and key third parties requiring access to internal applications and data. The operating environment was hybrid (on-prem and multi-cloud) with a largely remote workforce, and stakeholders included IT security, procurement/vendor management, business owners, and external suppliers.

The organisation encountered heightened supply chain risk driven by inconsistent third-party access controls and limited visibility of supplier activity across applications. Contributing factors included rapid onboarding of new vendors, reliance on legacy network access methods (ea.g., VPNs), fragmented identity and device posture signals, and differing security standards across geographies. The impact was increased exposure to credential compromise and lateral movement, slower incident response, and delays to business-critical supplier workflows due to manual verification and approvals.

Response

To address the identified supply chain access and visibility risks, the organisation implemented a programme focused on tightening third-party connectivity, improving assurance, and standardising controls across business units and regions.

Process and governance changes. A cross-functional working group was established spanning security, IT operations, procurement/vendor management, and key business owners. Together they defined a consistent third-party access policy and minimum security requirements for suppliers. Procurement processes were updated so that security requirements (identity standards, MFA, logging expectations, data handling, and access review cadence) were embedded into onboarding and contract renewals. A risk-based tiering model was introduced to differentiate controls for strategic suppliers, high-privilege managed service partners, and lower-risk vendors. The organisation also formalised access review and recertification, with clear ownership for approving, monitoring, and removing supplier access.

Technology and control improvements. The legacy approach of broad network access via VPN was reduced in favour of a Zero Trust, application-centric model. Access to internal and partner-facing applications was moved behind policy enforcement based on user identity, device posture, and contextual risk (e.g., location, anomalous behaviour).

This enabled suppliers to reach only the specific applications they were authorised for, rather than gaining implicit network-level reach. Where relevant, privileged access paths were tightened with stronger authentication, conditional access policies, and segmentation of administrative workflows.

Visibility, monitoring, and incident readiness. Centralised logging was enhanced to provide clearer visibility of third-party access, including who accessed what, from where, and under what conditions. Alerts and playbooks were tuned to identify suspicious supplier behaviour such as unusual access times, impossible travel, excessive download activity, or repeated authentication failures. Incident response procedures were updated so that supplier accounts and access paths could be quickly isolated without disrupting broader internal connectivity. The organisation also ensured that access decisions and audit trails were available for compliance and post-incident investigation.

Collaboration across the supply chain. Key suppliers were engaged early to align on controls and rollout timelines, supported by clear guidance and communications. For managed service partners, joint workshops were run to map critical access journeys, reduce standing privileges, and agree escalation paths for urgent access. Regular governance checkpoints were introduced to track adoption, handle exceptions, and share lessons learned across regions, helping the organisation move from ad-hoc supplier access decisions to a consistent, measurable approach to supply chain security.

Outcomes and lessons learned

The programme reduced supply chain exposure by replacing broad network access with application-level, policy-based access for third parties, improving control over “who can access what” and under which conditions. Centralised visibility and alerting increased confidence in detecting anomalous supplier activity and enabled faster isolation of risky sessions without disrupting core operations. Standardised onboarding, tiering, and periodic recertification reduced access sprawl and improved audit readiness, while clearer supplier engagement streamlined approvals and reduced delays for business-critical workflows.

Key lessons were to treat third-party access as a governed lifecycle (onboard, monitor, review, remove), align procurement and security requirements early, and apply risk-based controls rather than one-size-fits-all policies. Recommended good practices include minimising standing privileges, enforcing strong identity and device checks, maintaining high-quality logs, and running regular joint reviews with critical suppliers to validate controls and response procedures.

Andy Mills, Solutions Consultant

Conclusion

Securing supply chains is a complex and evolving challenge for businesses, and through this playbook techUK members have demonstrated how they are supporting the resilience of the UK's most critical sectors. From multinational organisations to small to medium-sized enterprises (SMEs), our members play a crucial role in ensuring supply chain security is recognised as a core component of operational resilience topic.

The case studies throughout this playbook have highlighted importance of combining continuous monitoring with structured response capabilities, adopting risk-based tiered models and establishing clear governance and accountability frameworks. They also demonstrate the breadth of expertise across the techUK membership in helping organisations strengthen visibility across their supply chains, enforce security obligations and better understand and manage third-party risk.

Beyond delivering practical solutions, techUK members also act as trusted advisors, helping organisations address wider challenges relating to accountability, consistency and risk management, while supporting them in understanding the potential impact of these issues on business operations.

techUK would like to thank all of the members who contributed their expertise and insights to this playbook. This work is stronger for the breadth of experience represented across it, and we are grateful to everyone who took the time to share their knowledge. techUK remains committed to creating ongoing opportunities for collaboration and knowledge sharing across industry connecting members, sharing best practice and supporting the development of strong and resilient supply chains across the UK's economy, public services and critical national infrastructure.

Jill Broom, Head of Cyber Resilience, techUK

Annie Collings, Senior Programme Manager, Cyber Resilience, techUK

Olivia Staples, Junior Programme Manager, Cyber Resilience, techUK

techUK
FOR WHAT COMES NEXT

About techUK

techUK is a membership organisation that brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. We collaborate across business, Government and stakeholders to fulfil the potential of technology to deliver a stronger society and more sustainable future. By providing expertise and insight, we support our members, partners and stakeholders as they prepare the UK for what comes next in a constantly changing world.

linkedin.com/company/techuk

youtube.com/user/techUKViews

@techuk.bsky.social

info@techuk.org