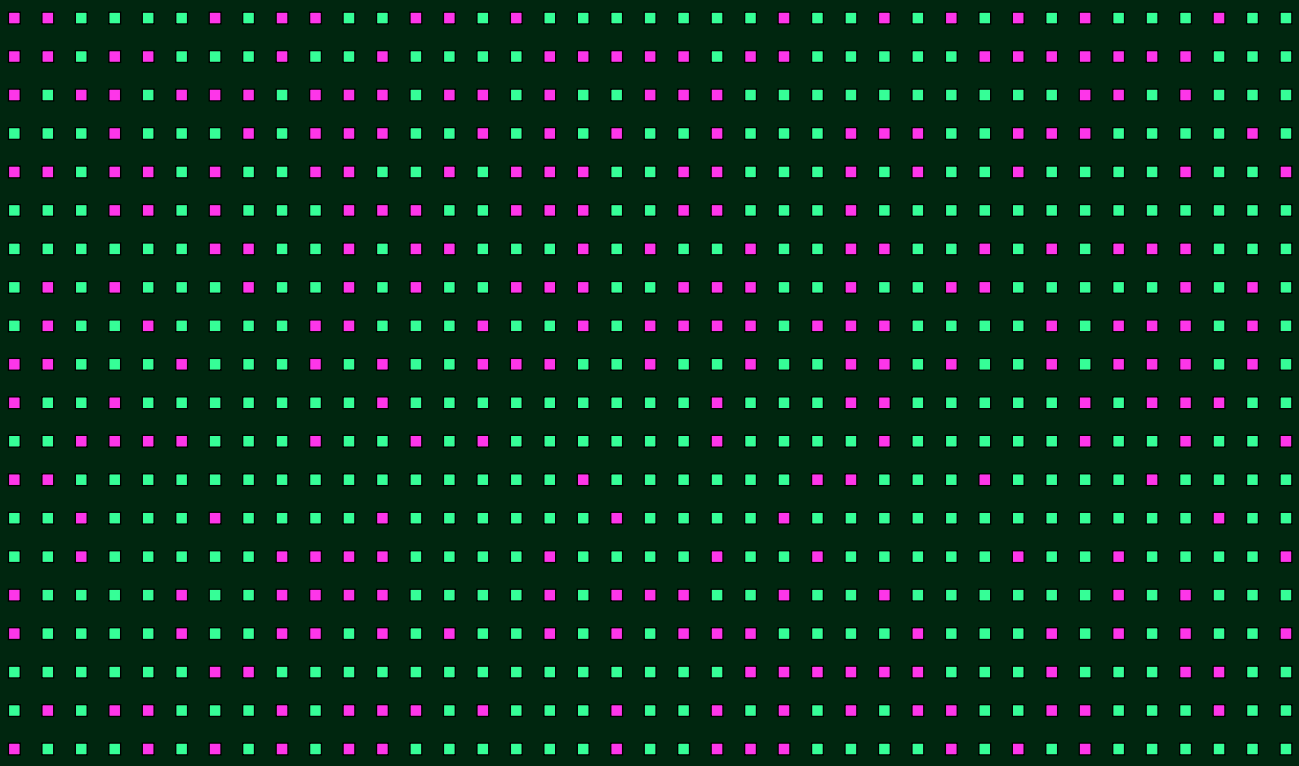
Public V1.0

# Securing the Supply Chain

## Insights from the IO State of Information Security Report on how supplier ecosystems are reshaping risk, governance, and resilience



## The state of information security report 2025

# Foreword

**Chris Newton-Smith**
CEO

## One of the strongest signals in the 2025 State of Information Security report data is the acceleration of supply chain risk.

Once considered a relative background issue, it has become a defining security and governance challenge. Organisations now operate within complex, interdependent ecosystems which include cloud platforms, MSPs, SaaS providers, open-source software, logistics partners, and data processors all of which collectively shape their resilience.

This interconnectedness has clear benefits, but it also amplifies exposure. Attackers exploit shared dependencies, concentration risk, and uneven assurance between suppliers to turn a single compromise into a multi-organisation event.

The data shows the pressure is mounting. 41% of organisations identify managing third-party risk as a top challenge. 61% experienced a third party-related incident in the past year, and 23% say supply chain compromise is their biggest concern for the year ahead. A majority (60%) describe third-party risks as "innumerable and unmanageable."

Despite the strain, there are signs of progress. 80% strengthened third-party and vendor risk management during the past year, and 64% plan to increase spend further. The majority (96%) have re-evaluated suppliers in light of geopolitical risk. At the same time, assurance expectations have risen sharply, with suppliers increasingly asked to demonstrate compliance with frameworks including ISO 27001, ISO 27701, SOC 2, NIST CSF, and GDPR.

The message from the data is clear: the modern enterprise is only as secure as its supply chain and that chain now reaches further than ever before.

***The message from the data is clear: the modern enterprise is only as secure as its supply chain and that chain now reaches further than ever before.***

# The expanding supply chain attack surface

## Digital transformation continues to multiply integration points across every organisation.

Cloud APIs, data pipelines, identity federations, and open-source components have created a lattice of dependencies that evolve daily. Each one represents a potential entry point for attackers or a weak link in governance.

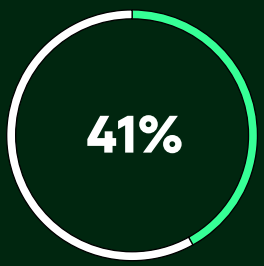
The result is an environment that is:

- **Transitive**
  Risks cascade across fourth and fifth parties beyond direct visibility.
- **Concentrated**
  Reliance on a small number of core providers creates systemic exposure.
- **Dynamic**
  Continuous software delivery means new risks emerge with every update.
- **Geopolitically sensitive**
  Changes in regulation or trade conditions can shift a supplier's risk profile overnight.

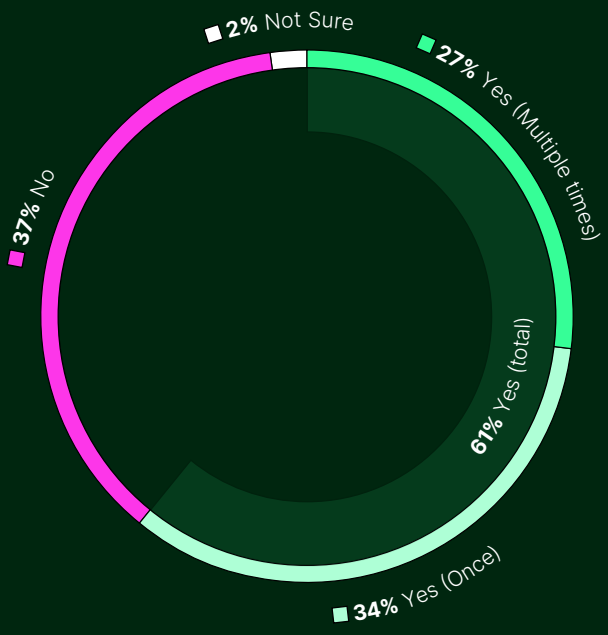
In this landscape, supply chain risk is no longer a by-product of global business, it is an operational constant.

***"One vendor's patch cadence is every customer's incident tempo."***


feel third-party risks are *"innumerable and unmanageable."*




list third-party risk as a top challenge




**In the last 12 months, has your business been impacted because of a cybersecurity/ information security incident caused by a third-party vendor or supply chain partner?**

## What the data says:

# Scale, impact, and momentum

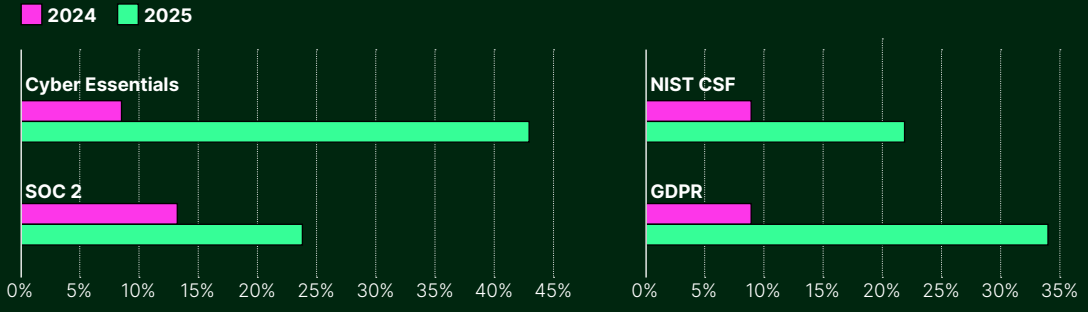
**The numbers underline the urgency. 41% of respondents cite third-party risk and compliance as a leading challenge, reflecting the sheer scale of supplier ecosystems. Most organisations manage dozens, if not hundreds, of vendors with direct access to sensitive systems or data.**

61% report that a third-party incident affected their business in the past year. The knock-on effects are significant:


Despite the impact, investment is increasing. 80% have already strengthened their vendor risk management programmes, and 64% plan further increases next year. Supplier requirements are expanding too. Cyber Essentials adoption has climbed from 8% to 43%, SOC 2 from 13% to 24%, NIST CSF from 9% to 22%, and GDPR alignment from 9% to 34%.

ISO standards remain the foundation for supplier assurance, providing globally recognised frameworks for security and privacy management. These trends together suggest that organisations are moving from informal due diligence to structured, evidence-based oversight.

However, not all sectors are keeping pace. Smaller organisations are less likely to have strengthened third-party risk management (71% versus 82% among large enterprises) and more likely to keep spending flat. This imbalance introduces fragility into wider ecosystems, where attackers often exploit the weakest node to reach the strongest target.




**Which information security standards or regulations, if any, do you require of your suppliers?**

# Where supply chain risk lives now

## The data reveals that supply chain vulnerabilities are emerging across several dimensions of business operations.

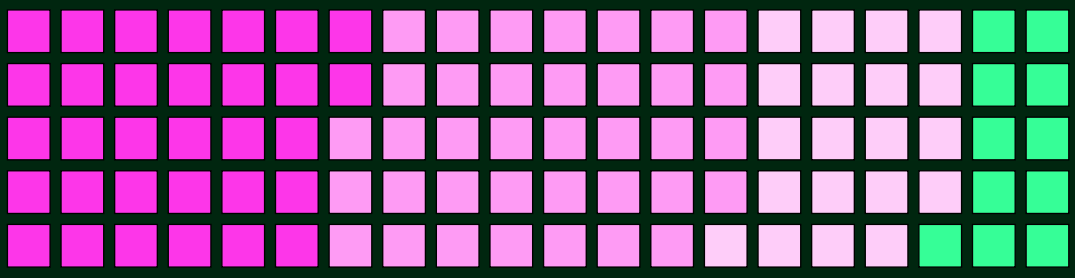
Software dependencies and updates remain a consistent threat. The growing reliance on open-source and third-party components means that a single vulnerability can ripple across thousands of organisations. The rise in supply chain incidents, from 7% in 2024 to 15% in 2025, underscores how attackers are weaponising these shared dependencies.

Identity and access integrations are another flashpoint. Over-privileged service accounts, weak API authentication, and misconfigured SSO connections provide lateral pathways between systems. Authentication breaches increased to 20%, suggesting attackers are exploiting trust between partners as much as between people and systems.

Data sharing and processing further widens the risk perimeter. When information flows through complex networks of processors and sub-processors, organisations inherit their vendors' data-handling weaknesses. 20% of respondents reported that a partner data breach led to reputational damage or customer loss.

Operational reliance on service providers continues to grow. MSPs and technology partners offer efficiency and expertise, but their interconnected tooling and shared credentials can magnify the impact of compromise.

Finally, geopolitical factors are reshaping how organisations think about supplier risk. 88% of respondents are concerned about state-sponsored threats, and almost all (96%) have reassessed suppliers based on geographic and political stability.



**How concerned, if at all, are you about state-sponsored cyberattacks targeting your organisation?**

Extremely concerned  Somewhat concerned  Slightly concerned  Not at all concerned

**The overall pattern is clear: supply chain exposure is no longer a discrete technical problem, it is systemic, intertwined with governance, resilience, and global operations.**

# Consequences and compliance pressure

**Supply chain failures are not only operational events; they increasingly trigger legal, financial, and regulatory repercussions. 71% of organisations received a data-protection fine in the past 12 months, and nearly a third of those exceeded £250,000.**

Even when a breach originates with a third party, regulators expect clear evidence of due diligence and proportional oversight. Customers and partners expect the same, demanding transparency, accountability, and faster response times.

As boards take greater ownership of cyber risk, supplier assurance has become a visible measure of governance maturity. Whether the obligation arises from NIS 2, DORA, GDPR, or sector-specific mandates, the expectation is consistent: resilience must extend beyond organisational boundaries.


**What is the total amount your business has received in fines for a data breach or violation of data protection rules in the last 12 months?**

**Whether the obligation arises from NIS 2, DORA, GDPR, or sector-specific mandates, the expectation is consistent: resilience must extend beyond organisational boundaries.**

## Why governance matters:

# Building trust through structure

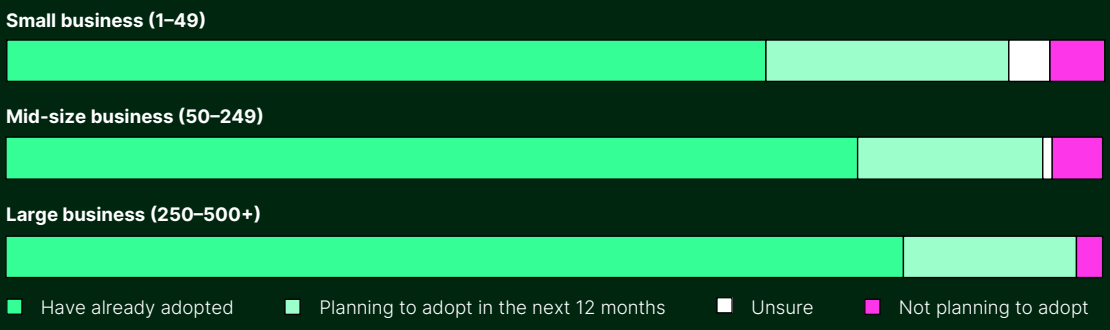
**The organisations that have begun to regain control over third-party risk share one defining trait: they've moved from reactive oversight to structured governance. Instead of treating supplier assurance as a procurement checkbox, they've built it into their core management systems.**

A well-defined Information Security Management System (ISMS), or an integrated approach through an IMS, provides the framework to manage supplier risk with consistency, accountability, and evidence. Among the standards referenced in this year's research, ISO 27001 stands out as the unifying foundation, covering the controls most other frameworks and regulations depend on. It formalises how supplier relationships are risk-assessed, how data and access are governed, and how performance and compliance are reviewed over time.

Crucially, ISO 27001 allows organisations to connect supplier oversight with broader business resilience. As regulations such as NIS 2 and DORA extend accountability across digital supply chains, ISO 27001's risk-based structure offers a proven way to demonstrate readiness; ensuring supplier security, privacy, and operational resilience are not managed in isolation but as part of one auditable system.

When aligned with complementary frameworks such as ISO 27701 for privacy and SOC 2 for service assurance, the ISMS evolves into the governance backbone of supplier security, uniting oversight, evidence, and accountability across every partner relationship.

In effect, ISO 27001 turns what many describe as "innumerable and unmanageable" supplier risks into a governed ecosystem, one where obligations are mapped, controls are clear, and accountability is continuous.




**Have you, or are you planning to adopt initiatives to strengthen third-party and vendor risk management?**

## Turning risk into resilience:

# The role of governance platforms

**The findings from the 2025 State of Information Security study confirm that third-party risk is now inseparable from core business risk. The pace and scale of supply chain interdependence demand governance that is structured, continuous, and transparent.**

An effective ISMS or IMS does more than satisfy auditors, it establishes the rhythm of oversight. It turns ad-hoc supplier assessments into ongoing risk evaluation and transforms compliance from a static task into a living practice.

As organisations extend their digital ecosystems, resilience will increasingly depend on how well they govern what lies beyond their immediate control. Those who treat supplier assurance as a central pillar of security, rather than an administrative function, will not only reduce exposure but build the trust and agility needed to operate confidently in a connected world.

**Governance isn't bureaucracy; it's resilience by design across every partner you depend on.**

# Get the full story in

## The state of information security report 2025

Read the full report →


Explore more at **isms.online**