ETHIXBASE360

2026

APRIL 2026

A PRACTICAL GUIDE TO THIRD-PARTY CYBER RISK MANAGEMENT

ETHIXBASE360

EXECUTIVE SUMMARY

Third-party cyber risk has become one of the most significant and least understood threats facing modern organizations. As businesses increasingly rely on cloud platforms, managed service providers, and outsourced technology, attackers are shifting their focus away from direct targets and toward suppliers that offer the most efficient path into multiple organizations at once.

This guide provides a practical, business focused view of Third-party Cyber Risk Management as a critical evolution of traditional Third-party Risk Management (TPRM). It explains why third-party cyber incidents are accelerating, how attackers exploit supplier ecosystems, and why many organizations remain exposed despite existing vendor risk processes.

Ultimately, this guide is designed to help organizations move from fragmented, reactive approaches toward a resilient, enterprise level model for managing third-party cyber risk, one that reflects how modern attacks occur and how modern businesses operate.

TABLE OF CONTENTS

WHAT IS THIRD-PARTY RISK MANAGEMENT

Third-party risk management (TPRM) is the discipline of identifying, assessing, and reducing the risks created by external organizations that support your business, suppliers, service providers, outsourcers, and partners.

These risks typically span multiple domains, including:

- operational disruption
- data protection and privacy
- regulatory and compliance exposure
- financial stability
- reputational damage

In practice, TPRM ensures that organizations understand who they rely on, how critical those relationships are, and what level of risk those relationships introduce across the business lifecycle from onboarding through to off-boarding.

ETHIXBASE360

A NEW VENDOR RISK DOMAIN: WHAT IS THIRD-PARTY CYBER RISK MANAGEMENT?

Third-party cyber risk management is an emerging vendor risk domain within TPRM that focuses on the cybersecurity and information security exposure of your third parties. Third-party cyber breaches occur when a company is compromised through one of its external vendors, partners, contractors, or service providers, rather than through a direct attack on its own systems.

These third parties often include:

- Cloud and SaaS platform providers
- IT service providers and managed service providers (MSPs)
- Payroll, HR, and other operational vendors
- Customer service, marketing, and analytics platforms

A breach through a third party is particularly attractive for bad actors because it can be just as damaging for organizations, or even worse because:

- Vendors often hold privileged system access
- Organizations typically have limited visibility into vendor security environments
- Breaches may go undetected for extended periods
- A single compromised vendor can impact hundreds or even thousands of downstream customers

In practice, third-party cyber risk management exists to answer one critical question:

How confident are you that the organizations you rely on will not become the easiest way into your business?

HOW THE RISK LANDSCAPE HAS CHANGED

Why third-party cyber risk management matters

As digital ecosystems expand and organizations rely on increasingly complex networks of external providers, third-party cyber incidents are fast becoming the norm rather than the exception. In 2025, nearly 30% of reported global data breaches were linked to third-party vendors, double the proportion seen the year before.

The growth in third-party incidents is not coincidental. It reflects how modern organizations operate today. Third-party breaches happen because of several factors.

1. **Organizations are More Dependent on Vendors than Ever**

Every business function now relies on external platforms, from finance and HR to customer service, sales, and supply chain operations. While SaaS adoption has delivered enormous efficiency gains, it has also significantly expanded the attack surface beyond internal IT environments.

2. **Vendors often have Excessive or Persistent Access**

To operate effectively, vendors frequently require access to internal systems, data, or credentials. Once attackers compromise a vendor, they can often move laterally into client environments with little resistance, sometimes without triggering immediate alerts. Several high-profile breaches in 2025 followed this exact pattern.

70% of organizations say they are highly concerned about supply chain cyber risk (Supply Chain and Demand Executive)

3. Vendors are Prime Targets for Social Engineering

Attackers increasingly recognize that breaching a vendor employee is often easier than penetrating the defenses of a large enterprise. A single successful compromise can provide access to multiple organizations, offering a high return on investment for threat actors.

4. Internal Teams aren't Sharing Risk-Critical Information

Third-party cyber risk is often treated as an IT issue, yet many of the most important controls sit with Compliance, Legal, Procurement, and Risk teams. These groups manage contracts, due diligence, SLAs, data-handling obligations, and monitoring requirements.

When this information is fragmented across teams, no one has a complete view of vendor risk. During an incident, this lack of shared visibility can delay detection and response, allowing breaches to escalate unnoticed.

5. Lack of Continuous Monitoring

Many organizations conduct vendor risk assessments only during onboarding. But vendors don't remain static over time. They may:

- Change systems or infrastructure
- Introduce new subcontractors
- Update software or security controls

Without continuous monitoring, early warning signs are easily missed.

79% of companies have less than half of their supply chain covered by cybersecurity programs, meaning most risk is still invisible *(SocRadar)*

82% of organisations give third parties access to all cloud data *(Wiz Research 2025)*

ETHIXBASE360

WHY THIRD-PARTY CYBER-ATTACKS ARE ATTRACTIVE TO ATTACKERS

One breach, many victims

When attackers compromise a single supplier, they don't just gain access to one organization, they potentially gain access to hundreds or even thousands of downstream customers at once. Modern organizations rely heavily on vendors, creating a force multiplier effect for attackers. One successful breach can cascade across an entire ecosystem, turning a single vulnerability into a systemic event with widespread operational, regulatory, and reputational consequences.

High return on effort

Third-party attacks offer attackers a far better return on investment than traditional, organization by organization attacks. This efficiency is especially attractive in ransomware and data extortion campaigns, where attackers aim to maximize impact while minimizing time, cost, and exposure. Once a supplier is compromised, the attacker can move laterally, reuse tooling, and repeat tactics across multiple victims with very little additional effort.

Attacks have more leverage

Third-party cyber incidents create outsized leverage compared to direct attacks. When a critical vendor is breached, the impact is rarely confined to data loss alone. Organizations can face operational outages, service disruption, regulatory scrutiny, and immediate reputational damage — all at once.

Attackers understand and exploit this dynamic, putting pressure on organizations to negotiate, respond and pay quickly.

REAL-WORLD INCIDENTS: CAUTIONARY THIRD-PARTY CYBER RISK TALES

Third-party breaches are not confined to smaller business without mature process, they impact:

Marks & Spencer

Overview

Marks & Spencer, a major British retailer known for its food, clothing, and home goods was breached via a third-party cyber-attack. Marks & Spencer stressed that the breach was via a third party, rather than a direct failure of its own systems. The cybercriminals used phishing and social engineering methods to breach Marks & Spencer's customer data.

Impact

The disruption caused shelving and stock availability issues, with some stores even experiencing empty shelves. The retail giant estimated the incident could cost around £300 million in lost profits for the year. Since the incident, the retailer has been working closely with experts to mitigate incidents and working diligently in the media to limit reputational damage.

Co-op

Overview

The Co-operative Group, a UK-based consumer cooperative operating groceries, insurance, and funeral services, suffered a breach via a third-party IT vendor. Attackers leveraged a misconfigured contractor system to access customer data.

Impact

Customer names, addresses, emails, and loyalty program data were exposed. The breach led to estimated disruption costs of £206 million in revenue, operational reviews and increased scrutiny of third-party contractors to prevent future incidents.

Qantas Airways

Overview

Quantas, Australia's largest airline and flag carrier, operating domestic and international passenger and cargo services was breached earlier in 2025 via a third party. A third-party customer service platform integrated with their systems was breached.

Impact

Cybercriminals used the exploited vendor environment to extract over 6 million customer records, including personal data.

While no sensitive financial data was stolen, the financial toll still spirals due to regulatory and reputation fallout. Under Australia's Privacy Act, Qantas could face fines of up to A$50 million or 30% of a company's adjusted turnover during the period of the breach – whichever is greater.

WHO'S RESPONSIBLE FOR THIRD-PARTY CYBER RISK

As a relatively new vendor risk domain, ownership of third-party cyber risk is largely unknown and undefined. On one hand, there are assumptions that InfoSec and IT teams would largely shoulder responsibility. However, due to the ongoing changes within an organization's value chain, it can also be argued that the responsibility should also be on Compliance, Risk, and Procurement teams.

This leaves the glaring question for all organizations to really think about:

Who actually owns third-party cyber risk?

The uncomfortable truth: there is no single owner

There is no perfect, universal answer and while this can sound like a cop-out, the reality is that ownership depends on how the organization defines and governs risk.
What does consistently fail is treating third-party cyber risk as:

- purely a technical problem
- a onetime onboarding check
- or something that can be delegated to a single function without shared accountability

Modern third-party cyber incidents demonstrate that this approach leaves dangerous oversight.

What effective ownership really looks like

Leading organizations are moving away from the question “Which team owns third-party cyber risk?” and toward a more pragmatic model:

- Shared accountability, with clear executive sponsorship
- Defined roles across IT, Risk, Compliance, Procurement, and the business
- Central visibility and governance, rather than fragmented ownership
- Cyber risk embedded into third-party risk management, not bolted on

In other words, while cyber expertise may sit with security teams, ownership of third-party cyber risk sits at the enterprise level.

INTEGRATING CYBERSECURITY INTO YOUR TPRM PROGRAM

Third-party cyber risk must be embedded into the full TPRM lifecycle with shared ownership across business units to empower organizations with the visibility they need.

Vendor onboarding

At onboarding, organizations should clearly establish baseline cyber expectations aligned to the vendor's role, access level, and criticality. This includes security standards, evidence requirements, and minimum control thresholds.

Risk segmentation

Not all vendors introduce the same level of cyber risk, and controls should reflect that reality.

Cyber requirements should be **scaled based on**:

- Vendor's overall risk profile
- Level of system and network access
- Business criticality and operational dependency

This risk-based segmentation prevents teams from over-assessing low-risk suppliers while missing material exposure in critical ones.

Due diligence and assessment

Effective cyber due diligence goes beyond policy checks.

Security questionnaires, independent attestations, evidence-based reviews, and external, deep permission-based scans should be utilized alongside policy checks.

Contractual enforcement

Security obligations, breach notification timelines, audit rights, and remediation responsibilities must be explicitly defined and enforceable within vendor contracts. Without this, organizations lack leverage when issues arise and face delays precisely when speed matters most.

Continuous monitoring

Point-in-time assessments are no longer sufficient.

Vendor cyber risk changes continuously as:

- New vulnerabilities emerge
- Systems and access change
- Threat actors shift tactics
- Suppliers onboard subcontractors

Organizations must be able to detect changes in exposure, vulnerabilities, and threat signals between formal reviews, not months after the fact.

Incident response integration

Similar to all risk, visibility of cyber risk from vendors doesn't always equate to prevention of breaches. That's why incorporating incident response process and resources is crucial to minimizing impact of third-party breaches.

CONCLUSION

Third-party cyber breaches are not rising by accident. They are the predictable outcome of expanding digital ecosystems, accelerated SaaS adoption, and attackers who increasingly view suppliers as the most efficient route into enterprise environments.

Organizations that continue to treat third-party cyber risk as a narrow IT problem will struggle to keep pace with modern threat dynamics, regulatory scrutiny, and the real-world impact of supplier failures. By contrast, those that integrate cyber risk into their broader TPRM operating model are far better positioned to detect issues early, respond effectively when incidents occur, and limit operational, financial, and reputational damage.

AUTHORS

NATASHA MARTIN

Director of Product,
Ethixbase360

JONNY SHENXANE

Product Marketing Manager,
Ethixbase360

ABOUT ETHIXBASE360

Ethixbase360 empowers confident third-party risk management through smart automation, expert-led due diligence, and responsive support. Our platform provides a single, connected view of global third-party risk, with insight and audit readiness built in. Designed to flex with risk and change, it adapts to shifting regulations and priorities, giving organizations control and the ability to respond at pace. Its proven configurability is backed by expert teams who bring human intelligence to every decision. Covering Anti-Bribery and Corruption, Modern Slavery, Human Rights, and Cyber, Ethixbase360 helps organizations stay resilient and agile, enabling faster decisions, greater value chain transparency, and clarity in an increasingly complex risk landscape. Learn more at www.ethixbase360.com.

 Website  LinkedIn  Mail