If Your Vendor is Vulnerable, So Are You
Why Third-Party Cyber Risk Needs a Connected Approach

In today's business environment, no organization operates in isolation. Every company depends on a network of third parties including suppliers, contractors, technology partners, and service providers to run its operations. This reliance enables efficiency and scale, but it also introduces a critical vulnerability: if your vendor is vulnerable, so are you.

Cyberattacks are escalating in frequency and sophistication and third-party ecosystems have become one of the most exploited weak links. While many organizations are investing heavily in their own defences, they often overlook the cyber resilience of the businesses they depend on. This oversight can have devastating financial consequences as well as operational disruption and reputational damage that takes years to repair.

The rising tide of third-party attacks

Recent high-profile cyber breaches have highlighted how vulnerable organizations are to weaknesses in their supply chains. Despite significant investments in internal cybersecurity, several major retailers, including Marks & Spencer, the Co-op and Harrods, have suffered serious disruption following third-party attacks. The financial and reputational impact can be staggering. Marks & Spencer, for example, is estimated to have suffered a £300 million loss in profits following a supply chain breach. And these are not isolated incidents.

[1] 93% of boards see cyber-risk as a threat to stakeholder value.

-2024 Gartner Board of Directors Survey

From risk to resilience – with Ethixbase360

The challenge of limited visibility in third-party cyber risk

One of the biggest barriers to effectively managing third-party cyber risk is visibility. Too often, responsibility for cyber due diligence sits solely within IT and Security teams. While these teams play a critical role, managing risk in isolation or silos can create blind spots. Reviews may be performed on a narrow subset of vendors, usually those perceived as "high IT risk." Meanwhile, others who may still hold sensitive data or provide critical services, go unassessed. Without a holistic, cross-functional process that includes procurement, legal, compliance, and risk management, organizations leave themselves exposed to unmanaged vulnerabilities.

Why Third-Party Risk Can't Be Ignored

It may be tempting to assume that because your organization has strong cybersecurity controls, you're well protected. Unfortunately, that assumption ignores the importance of supply chain interdependence. If a supplier experiences a breach, attackers could exploit that to target you directly. Even if they don't gain entry to your systems, disruption to your vendor's operations can impact yours. Consider the implications of losing access to a critical cloud provider or having an API integration suddenly compromised. The fallout could include delayed operations, contractual breaches, regulatory fines, and very likely, lost revenue.

The contagion effect of reputation damage

The reputational stakes are even higher. Customers expect their data to be safeguarded across the entire value chain. A breach linked to a third party can erode trust instantly, undermining brand value and trust. And it is the end company, not the supplier or partner, that shoulders the ultimate reputational damage in the eyes of its customers and the market.

Maintaining visibility with robust assessments

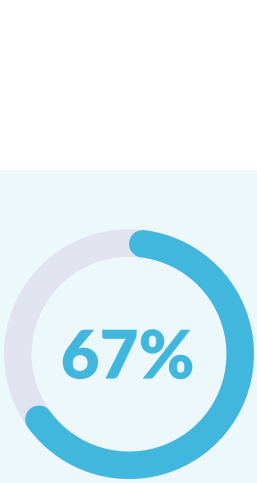
Addressing third-party cyber risk requires more than contracts or one-off checks. Companies must treat third-party resilience as an extension of their own security strategy. First, they must map the ecosystem, i.e. identify all suppliers, partners, and service providers with access to data, systems,or business processes. Crucially, this should not be restricted to IT vendors. Then they should assess risk proportionately by segmenting third parties into risk tiers based on the criticality of services provided, the sensitivity of data accessed, and the potential business impact of disruption. Questionnaires should be supplemented with independent validation, such as vulnerability scans, certifications, or audit results, for a more accurate picture of their risk.

Oversight must be continuous

Monitoring is an ongoing exercise. A third party considered low risk today may face new vulnerabilities tomorrow. Active and passive testing can be deployed depending on the third-party status and inherent risk they present to your business. It is also vital to integrate the management of cyber risk into the business. Risk insights should be embedded into procurement, compliance, legal, and operational processes to ensure comprehensive coverage and avoid duplication.

Ensuring rapid, defensible response

Organizations should establish clear pathways including defined escalation channels, remediation and mitigation plans, and accountability frameworks for when issues are detected. To achieve resilience, companies must go beyond compliance box ticking. Protecting customer trust and safeguarding brand reputation must remain at the core of third-party cyber risk management.



[2] 67% medium businesses and 74% of large businesses in the UK reported a cyber security breach or attack in the last 12 months.

-The Cyber Security Breaches Survey 2025, UK Department for Science, Innovation and Technology (DSIT) and Home Office

From risk to resilience – with Ethixbase360

From Risk to Resilience

What separates resilient organizations from vulnerable ones is their ability to act decisively, not simply react. By gaining visibility across their value chain, prioritizing based on inherent risk, and embedding cyber risk into broader governance, companies can transform a weak link into a source of strength. This requires investment in processes, collaboration across functions, and a shift in mindset. The organizations that succeed will be those that treat their third-party ecosystem with the same rigor and scrutiny as their own internal systems.

Author

Tristan Atkins
Chief Product and Technology Officer, Ethixbase360

Tristan joined Ethixbase360 in April 2022, bringing deep experience in regulatory compliance, SaaS, product management, and engineering from both enterprise and high-growth scale-up environments. Prior to Ethixbase360, Tristan served as Chief Technology Officer at a financial/regulatory compliance software company, guiding its evolution from a niche on-premises solution to a diversified SaaS portfolio.

In his current role, he leads the strategy and execution of product and technology initiatives that help organizations manage third-party risk. Known for driving innovation, building high-performing teams, and bridging technical and business goals, Tristan is passionate about designing scalable platforms that deliver impact.

About Ethixbase 360

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**.

1. https://www.gartner.com/en/documents/5533395
2. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025