Managing the rise of **third-party risk**: strategies for better oversight

Cybersecurity Awareness Month 2025

Janvi Mewada
BDO Canada

In today's interconnected business landscape, organisations rely on more third parties than ever—cloud vendors, SaaS providers, supply chain partners, and contractors.

In today's interconnected business landscape, organisations rely on more third parties than ever—cloud vendors, SaaS providers, supply chain partners, and contractors. While this ecosystem accelerates innovation and efficiency, it also increases risk exposure. As the saying goes,

"Your organisation is only as secure as its weakest third party."

Nearly one third of organisations surveyed by International Data Corporation (IDC) identify third-party risk management as a major weakness, making it one of the most frequently cited gaps across industries. Alongside vulnerability management, this lack of oversight continues to fuel preventable, externally driven threats. The message is clear: organisations need to rethink their approach to managing third-party risks.

Why third-party risk is rising

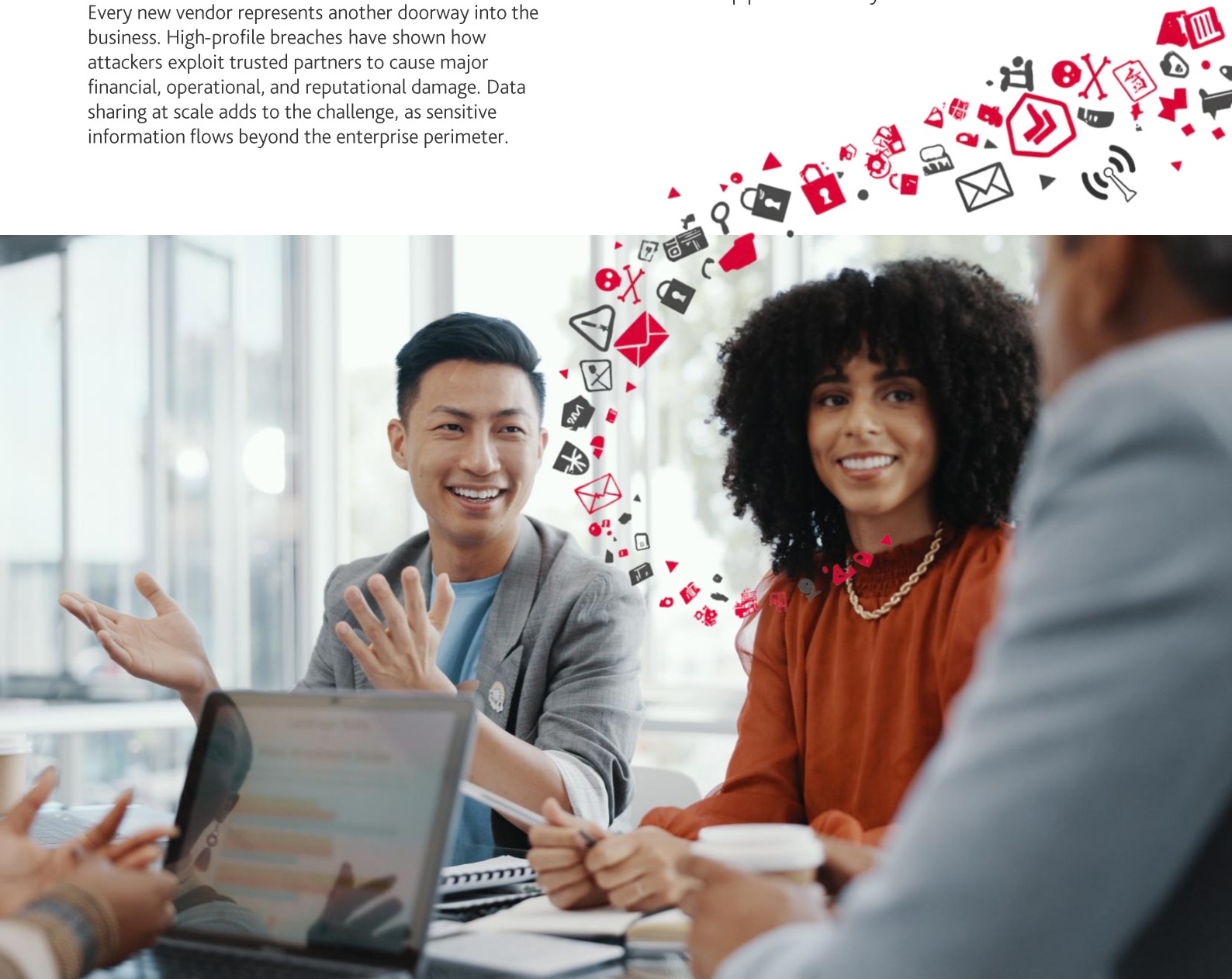
Third-party risk is growing rapidly, driven by global and digital pressures. Geopolitical tensions, fragmented supply chains, and the lingering effects of COVID-19 have disrupted what was once predictable.

Trade restrictions, regulatory changes, and regional instability now make vendor relationships less stable, especially for mid-market organisations with international exposure.

At the same time, the attack surface has expanded. Every new vendor represents another doorway into the business. High-profile breaches have shown how attackers exploit trusted partners to cause major financial, operational, and reputational damage. Data sharing at scale adds to the challenge, as sensitive information flows beyond the enterprise perimeter.

Many leaders admit they are not prepared. The same survey from IDC showed supply chain risk ranking second among the risks business leaders felt least prepared for. IDC shows that while supply chain attacks are among the top three cyber threats, they often rank much lower on executives' stated priorities. The issue is not awareness, but execution.

Oversight practices often remain outdated. Responsibility for third-party risk is frequently fragmented across procurement, IT, and security, with no clear accountability. Vendor assessments are still largely treated as one-off events at onboarding, and too often, companies rely on static questionnaires and annual audits rather than the real-time monitoring needed to keep pace with today's threat environment.



Building a resilient third-party risk programme

Recognising the challenges is only the first step. The real opportunity lies in building a third-party risk management (TPRM) programme that is resilient, collaborative, and intelligence-led. Rather than treating vendor oversight as a checklist, resilience comes from embedding risk management throughout the entire vendor lifecycle—from selection to active collaboration, to secure exit.

Before onboarding: Setting the foundation

- Conduct thorough due diligence and apply risk tiering to identify high-criticality vendors.
- Include clear requirements in contracts and SLAs, and align with procurement and legal to set accountability from day one.
- Educate third parties on your security policies and standards, and set clear expectations.
- Diversify through flexisourcing (nearshoring and friendshoring) to reduce reliance on high-risk regions and strengthen supply chain continuity.

During the relationship: Active monitoring and collaboration

- Move from annual reviews to continuous monitoring using analytics, automation, and AI for real-time insights.
- Work with vendors to adopt shared standards (ISO, NIST, GDPR, HIPAA) to build trust and consistency.
- Use regular audits, joint exercises, and outcome-focused metrics (such as fewer incidents, faster detection, quicker remediation) to measure success.

After the relationship: Secure exit

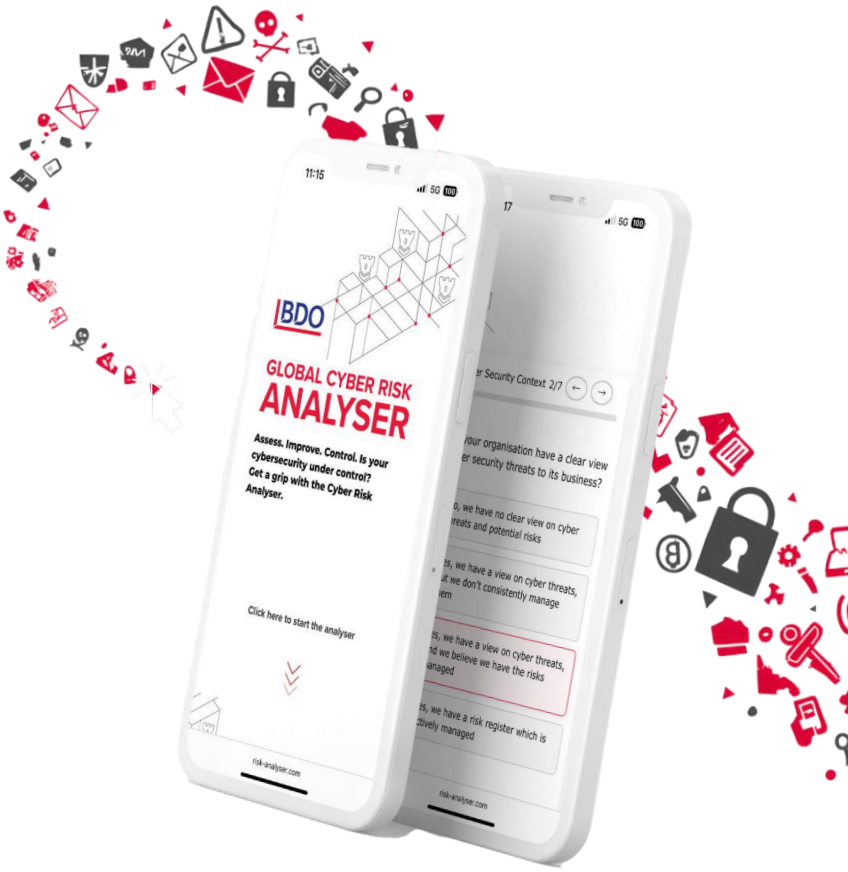
- Revoke access, return or delete sensitive data, and confirm obligations are met.
- Conduct post-engagement reviews and feed lessons learned back into governance and procurement processes.

Final takeaway

Third-party risk will continue to grow as business networks become more interconnected, but this does not have to hinder innovation.

With the right governance, continuous oversight, and resilient vendor relationships, organisations can flip the narrative. By adopting proactive oversight strategies, leveraging technology, and embedding cybersecurity into vendor relationships, organisations can build resilience and foster trust.

In a world of interconnected risks, the ability to manage third-party relationships effectively is key to scaling securely, innovating confidently, and staying ready for what's next.



DOWNLOAD THE REPORT

REGISTER FOR OUR WEBINAR

EXPLORE THE CYBER RISK ANALYZER