Third-Party Cyber Vulnerabilities and How to Stop Them: One-Page Summary

NORTH RISK PARTNERS® | WEBINARS

Why Third-Party Cyber Risk Matters

Cyber incidents don't always start inside your organization—they often start with a trusted third party. A single vendor with weak controls, broad system access, or exposure to sensitive data can cause operational disruption, financial loss, and reputational damage. That's why third-party cyber risk is no longer just an IT issue—it's a core business risk leaders need to manage actively.

Top Five Takeaways

1. **Visibility comes first:** Maintain a centralized inventory of vendors, including SaaS tools and contractors. You can't respond quickly to risk if you don't know who has access.
2. **Follow the data:** Understand where sensitive data flows and which vendors access it—especially customer, employee, and proprietary information.
3. **Risk isn't tied to spend:** Smaller vendors can pose a significant risk if they support critical processes or handle sensitive data.
4. **Limit the impact of a breach:** Don't let one vendor problem become an enterprise-wide problem—limit access, separate systems, and contain issues before they spread.
5. **Plan for vendor incidents:** Incident response plans should include vendor breaches and outages, and be tested with leadership through tabletop exercises.

> "Managing third-party cyber risk isn't about eliminating risk—it's about understanding it and being prepared when it matters most."

Emerging Cyber Risks to Watch

- Employees can quickly adopt **unvetted AI tools** that may expose proprietary or regulated data
- **AI-driven phishing and deepfake impersonation** are raising the stakes for social engineering attacks
- **Multiple vendors may rely on the same platforms**, creating unseen single points of failure

What Insurance Carriers are Looking For

- **Standalone cyber coverage** to address real incident costs
- **Strong first-party controls,** as response and recovery costs often drive claims
- **Evidence—not attestations—** of security practices like multi-factor authentication (MFA), managed detection and response (MDR), and vendor risk management
- **SOC 2 reports** that support—but do not replace—ongoing risk evaluation

Create a 12-Month Action Plan

MONTHS 1-3: Build a vendor inventory and identify critical and high-risk vendors

→

MONTHS 4-6: Audit high-risk contracts and validate access controls

→

MONTHS 7-9: Perform deeper reviews or monitoring for your top-risk vendors

→

BY YEAR END: Run a vendor-breach or outage tabletop exercise with executives

Have Questions?

A thoughtful approach to vendor cyber risk can uncover blind spots, strengthen decision-making, and support more informed conversations about protection and preparedness.

If you have questions, please **contact your North Risk Partners Risk Advisor**.