McKinsey & Company

Risk & Resilience Practice

Taking a business-critical approach to supplier nth-party IT risk management

Supply chain cybersecurity vulnerabilities frequently make headlines, so being prepared must be a priority. Here's a new approach to protecting business-critical processes from nth-party risks.

This article is a collaborative effort by Charlie Lewis, Justin Greis, and Lamont Atkins, with Emily Schenck and Jacob Faria, representing views from McKinsey's Risk & Resilience Practice.

July 2025

In the modern economy, almost every business is a tech business, with digitization, automation, and data solutions embedded into multiple operations. But with these advancements come risks. One of the most critical risks is that responsibility for technology often does not sit with companies themselves but instead with an array of third-party suppliers, service providers, and subcontractors. By outsourcing IT services, companies can unlock efficiencies and innovation. The downside is that they can also struggle to ensure that their businesses remain secure and resilient.

Modern technology supply chains are not much like chains at all. In fact, they are more like three-dimensional spiderwebs, each strand of which is connected to and dependent on others, and some of which are far removed from the company itself. As such, technology risk management is increasingly concerned not only with immediate supplier relationships but also with distant and sometimes ambiguous third parties, or nth parties, which often sit several layers away from the company's direct line of sight.

Third- and nth-party supplier cyberincidents are a significant source of risk, in some cases leading to the loss of data for hundreds of millions of people.[1] Indeed, over the past two years, nearly one-third of cyber breaches has been associated with technology supply chains, and multiple incidents have highlighted the cascading effects that a single compromised supplier can have on organizations and sectors.[2] Moreover, despite companies sometimes spending millions on controls, supply chain oversight is often surprisingly basic—comprising unvalidated responses in risk questionnaires or simple clauses contained in contracts. Alternatively, companies spend so much time focusing on supplier cyber risks that they drag their feet and fail to implement a useful, high ROI solution in a timely fashion.

As the number of ransomware incidents, data breaches, and supply chain attacks continues to rise (up 83 percent, 135 percent, and 236 percent, respectively, over the past two years), companies urgently need to ramp up their capabilities.[3] To some extent, this is already mandated by regulation. The European Union's Digital Operational Resilience Act (DORA), the United Kingdom's Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) operational resilience rules, and Australia's APRA CPS 230 are among initiatives that lay out strict standards for IT risk management. These vary somewhat in their detail, but one underlying principle holds true: Companies have a duty to ensure that their approaches to supplier risk management reflect both their unique risk profiles and the criticality of the business processes in question.

Traditional third-party risk management (TPRM) frameworks often emphasize the confidentiality and integrity aspects of the CIA (confidentially, integrity, and availability) triad. But the availability—and, more specifically, the resilience of *business-critical* systems (the ability to withstand an adverse event without interruption)—is equally as important. Indeed, focusing on business-critical nth-party relationships, rather than getting bogged down in hypercomplexity, is an excellent way to get a grip on supply chain risks. At a time of rising cyberthreats, companies that can put this distinction into practice achieve the double win of protecting their vital operations and building competitive advantage.

1 "Looking back at third-party breaches and vendor cybersecurity incidents in 2024," Tenchi Security, December 10, 2024.
2 Verizon Data Breach Investigations Reports, Verizon, 2023–25.
3 Verizon Data Breach Investigations Reports, Verizon, 2023–25.

Beyond traditional supplier risk management

Nth-party risk management programs often fall short in mitigating emerging risks, with companies missing vulnerabilities as simple as phishing emails and seeing impacts reverberate through their operations. Moreover, as supplier inventories grow, ownership shifts and overlapping relationships often obscure dependencies. As a result, risk management programs can quickly become overwhelmed (exhibit). Here are a few of the most widespread challenges:

— *High numbers of suppliers.* Organizations engage with a vast number of suppliers and service providers. As a result, they struggle to comprehensively evaluate and monitor every supplier in the ecosystem, leaving significant gaps in oversight.

— *Lack of in-depth inspection.* Traditional programs often rely on periodic assessments and static checklists, characterized by questionnaire-based compliance and security certifications. They do not delve into the operating effectiveness or coverage of the controls in the service providers' environment. This can give a false sense of security if not validated.

— *Cost and resource constraints.* Comprehensive risk assessments and continuous monitoring of third-party relationships require financial and human resources. Many organizations face budgetary and staffing limitations, which can hinder their ability to thoroughly vet each supplier.

— *Interconnected risks.* A breach or disruption at one supplier can have a ripple effect throughout the network. Often, programs may not adequately account for these interconnected risks.

— *Blind spots beyond tier one.* Most firms map tier-one suppliers but lack visibility into fourth- and fifth-party dependencies, where critical services often reside.

— *A dynamic and evolving threat landscape.* Traditional frameworks may not be designed to adapt quickly, leaving organizations exposed to new threats.

— *Pace of change.* Current processes are designed to assess suppliers at specific points in time, such as during a service contract. However, with technologies often seeing continuous updates without formal contracting cycles, oversight processes fail to keep up.

— *A lack of automation and real-time alerting.* Companies often lack automated solutions and dashboards to monitor complex risks such as the integration of new data into existing work streams. Real-time alerts are also often absent.

— *Too many audits.* Often, individual business units are auditing separately, despite being served by the same supplier, creating unnecessarily heavy cost and operational burdens.

— *No minimum standards.* Companies fail to put in place contracted minimum supplier standards to support supplier resilience.

— *Concentration risk.* There are a relatively small number of suppliers that operate the underlying infrastructure and networks that run most large organizations' enterprise systems. An outage or attack on one of these could lead to catastrophic consequences for a business without a contingency plan or alternative provider.

Exhibit

A traditional nth-party risk management program consists of nine key elements. Organizations can go above and beyond these capabilities to truly evaluate and mitigate nth-party risk.

Traditional nth-party risk management program and enhancement opportunities

● Scope and segmentation ● Control element ● Governance framework

	Element	Definition	Enhancements
●	Scope	Methodology for prioritizing 3rd parties engaged in software development	
●	Segmentation	3rd-party segmentation based on criticality	Standard segmentation defines nth-party risk tiers. An enhanced program identifies the top-tier nth parties that are critical to the business (ie, business could come to a standstill without them)
●	Due diligence	Best practice–driven 3rd-party assessments; tiered based on risk	
●	Control system	Controls to monitor and enforce compliance with policies and standards; driven by 3rd-party type	
●	Scorecard and risk assessments	Risk assessments tied to an objective standard	Questionnaires and external monitoring scorecards are the baseline. Top-tier nth parties require additional scrutiny in the form of a holistic business impact assessment of the supplier
●	Governance	Appropriate escalation criteria for risk acceptance and reporting requirements for risk owners (business leadership): cross-functional/geography committees	Governance for top-tier suppliers means that the business has identified alternative strategies (eg, manual work-arounds, alternate suppliers) in case a critical supplier goes down
●	Organization	Cross-functional collaboration between procurement, cybersecurity, the business, and multiple geographies	True business resilience requires ongoing, mutual collaboration between your organization and its critical nth parties to address and mitigate risks effectively
●	Policy framework	Policies and standards that extend to 3rd parties	
●	Tools and data	Integration of 3rd-party risk data to enterprise risk register for assessment components; automation of vendor scorecards	

To address shortfalls in oversight of IT supply chains, leading companies are taking an alternative approach. Rather than try to keep tabs on every party in their supply chains, they prioritize their most strategically important relationships. Thus, instead of the traditional focus on “cyber critical” suppliers, they focus on “business critical” relationships that enable their most critical processes. The summation of these form what is known as the “minimum viable company”: the smallest set of people, processes, technologies, and suppliers required to run the core functions of the company even when upstream nth-party links fail.

A strategic approach to nth-party risk management

By being selective, a modern approach to fostering resilient IT supply chains gives companies scope to go beyond the checklist-based paradigms of the past. Leading companies are showing that three guiding principles can create a solid foundation on which to move forward (see sidebar, "Building nth-party resiliency with the Blue Cross Blue Shield Association").

Principle 1: Focus on business criticality

When it comes to risk, not all suppliers are equal. The most significant danger lies in third parties whose failure could derail essential business processes, cause revenue shocks, or tarnish a brand's reputation. Thus, a good place for companies to start is to establish a system of risk tiers based on variables such as the level of the third party's access to data, the nature of that data, and their criticality to business operations.

— *Action:* Document the organization's critical business processes to identify single points of failure and then map and rank suppliers based on their potential operational impact to the most important processes. Ensure finite resources are channeled to deeper, more frequent assessments of the riskiest partners, leaving lighter evaluations for those in lower tiers.

— *To get started:* Assemble a cross-functional team that includes people from procurement, IT, and operations. Identify any overlap or concentration risk (for example, multiple processes reliant on a single supplier or subcontractor) around the critical business processes.

Principle 2: Elevate availability and resilience through rigorous business impact assessments

Formulate a clear view of the operational, financial, and reputational consequences of a supplier being compromised or going offline.

— *Action:* Go beyond routine questionnaires to support prioritization of high-impact scenarios and set a baseline for supplier accountability:

- Pinpoint the operational, financial, regulatory, and brand damage (for example, hourly revenue at risk, customer trust) if a critical supplier cannot deliver.
- Consider risk exposure based on business preparedness (that is, the ability to maintain operations through a third-party outage and third-party preparedness, meaning the ability to recover and communicate updates while safeguarding data).
- Define the metrics and thresholds that would trigger escalation (for example, maximum allowed downtime).
- Elevate expectations for the most critical suppliers. Embed conditions into contracts, making sure security controls, service-level agreements, and incident-reporting expectations are explicit and enforceable.

— *To get started:* Select one high-impact supplier and perform a tabletop exercise simulating a major cyber breach or operational failure. Document who must be involved, escalation thresholds, and the supplier's communication and recovery timeline. Use these insights to refine contract terms and internal response protocols.

Building nth-party resiliency with the Blue Cross Blue Shield Association

The Blue Cross Blue Shield Association (BCBSA), also known as "The Blues," is a US-based federation with 33 independent and locally operated BCBSA companies that provide health insurance to more than 115 million people in the United States. McKinsey Partner Charlie Lewis and alumnus Justin Greis, sat down with BCBSA's managing director of Systemwide and FEP Cybersecurity, Andrew MacKenzie, to discuss the federation's business-focused approach to supplier risk management.

McKinsey: Were you surprised by the number of suppliers that mapped to critical business processes?

Andrew MacKenzie: I was not. However, I was surprised by some of the companies providing the services, many of which are relatively unknown but are critical to healthcare infrastructure. By mapping suppliers to critical business processes, we accelerated our ability to manage an incident and understand who is affected. We were also able to highlight concentration risk and the associated planning needed to build resiliency and collaborate with key suppliers.

McKinsey: Did you find there was a complete, accurate, and common understanding of how the suppliers mapped to critical business processes? Prior to the effort, was there an understanding of what business processes mattered most to the business?

Andrew MacKenzie: Prior to this effort, we did not have a unified understanding of critical business functions and processes. A few of our plans championed the concept of a minimal viable company [MVC], but for the most part, we did not have an agreed systemwide view. Now the MVC idea is gaining traction, especially as the plans are looking for efficient and reliable ways to recover critical business functions in the case of an adverse event where traditional recovery doesn't work.

McKinsey: Upstream and downstream process dependencies can be difficult to map and understand. How is BCBS [Blue Cross Blue Shield] as a system thinking about this?

Andrew MacKenzie: We are well coordinated and understand the responsibilities our plans have to their members, while also taking into account the fact that we are a federation of companies that work together seamlessly to provide our members with critical services. As a system, we focus on the fabric that binds our Blue Plans together and we use the concept of minimal viable system [MVS] to build resiliency. Executive-level buy-in and sponsorship are key, as is educating folks on the concept of MVS.

I've found that once folks "get" the concept, they are open to supporting and providing input. Then the process of service mapping begins, with a focus on the people, processes, and technology that support key services. Next steps include creating continuity and recovery strategies such as immutable backups of critical data and building an infrastructure that can connect data to applications so the business can get back up and running in case of a cyber event. This is easily stated but can be costly and complicated to implement.

McKinsey: There are a lot of ways to risk rank suppliers. What are some of the factors that BCBS uses, and what do you think matters most?

Andrew MacKenzie: Risk ranking suppliers is an important part of our annual supplier risk refresh. To create a meaningful ranking, we use a scoring rubric that takes into account the inherent risk of our member plans and key criterion such as data classification and level of impact if the supplier went offline. The rubric allows us to rank our suppliers in a meaningful way that supports resiliency planning.

McKinsey: Over and above a simple questionnaire, what are some of the ways BCBS is enhancing its supplier risk program? What advice would you give organizations on this journey?

Andrew MacKenzie: Supplier risk management is a huge topic that has many tentacles. Making sure that fundamentals—standards, assessments, a sound TPRM [third-party risk management] program—are in place is table stakes. I think some of the "softer" aspects of a supplier risk management program should be to focus on understanding who your suppliers are by risk and then building relationships with their key security team members. Those relationships will pay dividends in case of an incident.

It is key to understand that security is often not a core competency in the supplier community, so by all means, share practices and knowledge to help the supplier come up to speed where needed. Building resiliency is vital, just as putting all one's eggs in one basket is never a good idea. You can start the process with BIAs [business impact assessments] in key business areas, analyzing the results for concentration risk or other indicators of risk.

Andrew MacKenzie is managing director of Systemwide and FEP Cybersecurity at the Blue Cross Blue Shield Association.

Comments and opinions expressed by interviewees are their own and do not represent or reflect the opinions, policies, or positions of McKinsey & Company or have its endorsement.

Principle 3: Collaborate and make fallback plans

Real resilience is built on twin pillars: trusted relationships and viable fallback measures. When disruptions happen, collaboration and ready-made plans can be the difference between chaos and continuity.

— *Action:* Foster executive-level ties (CEO to CEO, chief information security officer [CISO] to CISO) to accelerate threat intelligence sharing and collaboration with critical third parties. Develop fallback strategies for critical supplier disruption. This may mean identifying secondary providers, standing up in-house failover capacity for the most critical workloads, or designing manual work-arounds (for example, batch processing, paper-based fulfillment) that keep critical support flows running. Incorporate real-time alerts so small issues are flagged and can be addressed quickly. This integrated approach will ensure nth-party risk management is a practical shield against real-world failures.

— *To get started:* Invite the CISOs of the most critical suppliers to a collaborative risk roundtable. Focus on identifying potential single points of failure/concentration risk, agreeing on escalation channels and scheduling joint-incident response drills.

In a world where supply chain vulnerabilities frequently make headlines, being prepared is not just a "nice to have"—it's an imperative. Decision-makers who speedily identify high-priority areas, clarify contractual obligations, and establish deeper collaborations with their most critical suppliers not only embed resilience into their most critical operations but also create competitive advantage. Moreover, the process doesn't need to be onerous. Leading companies have shown that a risk-based approach can significantly improve third-party risk resilience in less than 12 weeks, as they move from merely identifying risks to actively mitigating business-critical risks across the organization.

Charlie Lewis is a partner in McKinsey's Connecticut office, **Justin Greis** is an alumnus of the Chicago office, **Lamont Atkins** is a partner in the Dallas office, **Emily Schenck** is a principal lead II in the Denver office, and **Jacob Faria** is a consultant in the New York office.

Designed by McKinsey Global Publishing