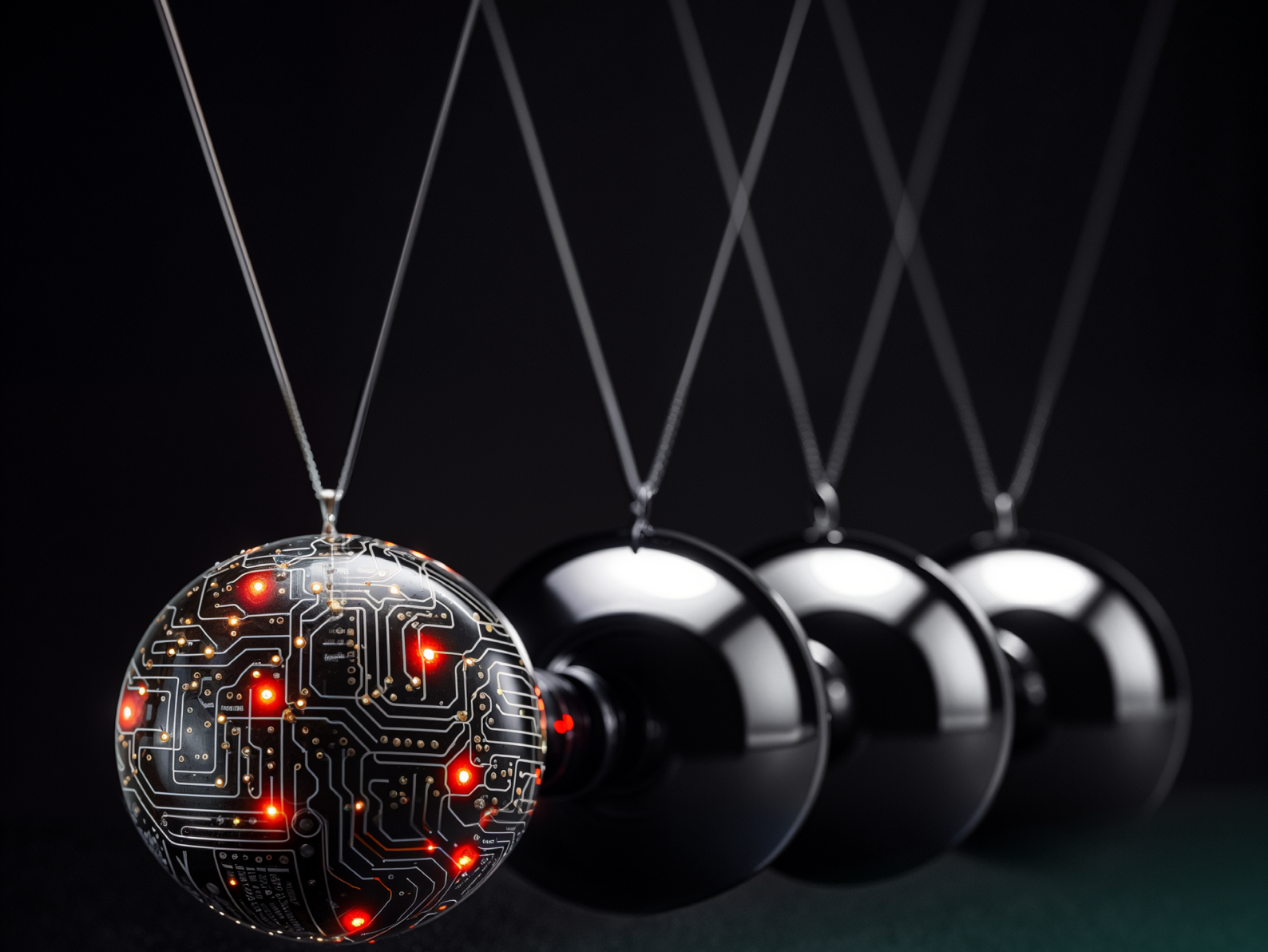


Analytical report

Supply chain reaction: securing the global digital ecosystem in an age of interdependence

kaspersky

Contents

Introduction: Cyber risk in an interconnected world

Enterprise security today is not defined by technology in isolation, but by the collective cyber resilience of an entire ecosystem. Modern organizations operate within a vast and intricate web of trusted relationships, relying on dozens, if not hundreds, of contractors, software vendors and cloud service providers.

This digital interdependency, while driving efficiency and innovation, has created a pervasive and critical weakness: risks of supply chain attacks. By exploiting the trusted relationships between organizations or vulnerabilities in the software used, adversaries can bypass fortified front doors to target the less-secured digital backdoors of partners and suppliers.

This shift has elevated supply chain risk to a top-tier strategic concern for both cyber executives and technical specialists. As highlighted in the World Economic Forum's Global Cybersecurity Outlook 2026, the growing interconnectivity of digital systems, coupled with severely limited visibility into third-party security postures, poses a fundamental challenge to achieving cyber resilience.

It is an ecosystem-level risk that defines the fate of entire industries, where a single vulnerability in a common software component, a widely used cloud platform or a niche supplier can cascade into a global crisis of operational disruption, severe financial loss and irreparable reputational damage.

This interdependence creates a critical vulnerability: an organization's security is directly dependent on that of its external software providers and suppliers, who often have trusted access to its network. A single breach in the extended ecosystem can become a direct pathway for attackers.

To understand how the business world is responding to this complex challenge, Kaspersky presents the findings of a global survey of technical professionals and security specialists, from C-level executives to senior technical experts. It examines the current state of supply chain cybersecurity in large enterprises, with a focus on the growing risks and the evolving strategies to mitigate them.

The Kaspersky research specifically investigates the following:

Risk perception & exposure:

How companies estimate the risks associated with supply chain and trusted relationship attacks, and how frequently they confront these threats in practice.

The protection gap:

The critical factors, from insufficient visibility and resource constraints to a lack of standardized assessment frameworks, that prevent enterprises from addressing these risks effectively.

Evolving mitigation strategies:

The practical methods organizations are employing for protection, including technical controls, contractual security obligations and continuous vendor risk monitoring.

The principle of shared responsibility:

Exploring the pragmatic, yet complex, question of investment by assessing companies' readiness to share contractors' cybersecurity costs to bolster collective defense.

As geopolitical tensions complicate global digital trade and reliance on critical external services deepens, securing the supply chain has become a core business imperative. This report explores the critical data on enterprise preparedness, offering insights into navigating the fragile web of trust upon which modern business depends.

Methodology

For the report, Kaspersky's internal market research center commissioned a survey, questioning technical experts, ranking from C-level employees and vice presidents to team leads and senior specialists, whose work is largely devoted to security issues.

Team leads

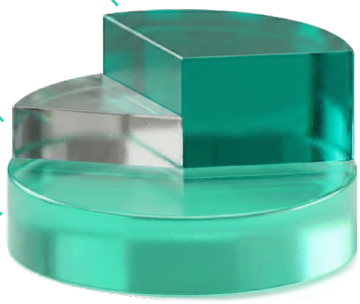
Senior specialists

C-level & VP

56%
Most of the time

30%
Less than half the time

14%
Only IT security



Time spent on IT security issues

16
countries surveyed

Asia Pacific

Europe

META region

Latin America

1,700+
IT security professionals

Size of companies surveyed
500+
employees

kaspersky

Key findings

For the report, Kaspersky internal market research center commissioned a survey, questioning technical experts, ranking from C-level employees and vice-presidents to team leads and senior specialists, whose work is devoted to security issues in certain amount.

Supply chain attacks are at the top of the list of attacks that happened to companies **over the last 12 months (31%).**

Trusted relationship attacks were experienced **by 25% of companies,** putting them fifth among the most common threats.

Companies that believe they are less vulnerable to supply chain/trusted relationship attacks still rate supply chain risks as one of the top three most dangerous threats.

On average, companies have **more than 60 hardware and software suppliers.**

42% of corporations

name the lack of qualified workforce and priority given to other IT security tasks and issues as the main factors preventing them from tackling supply chain risks effectively.

The number of contractors having access to companies' systems varies **mostly from 25 to 99 (44%), the average being 72.**

69% of organizations

confirm their readiness to share security costs with their contractors if that would guarantee invulnerability to cyberattacks.

A quarter of organizations (25%)

already share contractors' cybersecurity costs.

Among other barriers that prevent businesses from addressing supply chain risks effectively, respondents name lack of legal IT security obligations of contractors in their contracts (39%) and lack of understanding of these risks by non-IT security staff (32%).

Chapter 1: Underestimating the most prevalent threat

A clear disconnect lies at the heart of modern cybersecurity. While technical executives are acutely aware of cyber risks, the survey reveals a significant underestimation of the specific dangers posed by supply chain and trusted relationship attacks.

Organizations worldwide are prioritizing threats based on perceived lethality rather than experienced frequency, creating a critical gap in preparedness and resource allocation.

The data presents a contradiction. When asked to classify various threats based on the hazard level to their organization, only 9% of businesses globally put supply chain attacks at the top. Similarly, just 8% named trusted relationship attacks. This low level of concern stands in contrast to the operational reality these same organizations face.

In reality, over the past 12 months, supply chain attacks topped the list of threats actually experienced, with 31% of respondents confirming their organization had been impacted, more than any other type of cyberthreat. The trend for trusted relationship attacks is similarly misaligned, while a quarter of businesses globally dealt with such an attack.

This perception gap extends to potential consequences. A majority of respondents (52%) correctly identified operational disruption as a primary potential outcome of a supply chain or trusted relationship breach.

However, this widespread understanding of severe business impact does not translate into proportional threat ranking, suggesting a dangerous situation where the risk is acknowledged abstractly but not prioritized concretely.

Threats ranked by organizations as the most dangerous

	Share
Advanced persistent threats (APTs)	**14%**
Ransomware attacks	**11%**
Insider threats	**9%**
Supply chain attacks	**9%**
Distributed denial of service (DDoS) attacks	**8%**
Trusted relationship attacks	**8%**
AI-powered attacks	**8%**
Cyber espionage	**8%**
Reconnaissance	**7%**
Malware-as-a-Service	**7%**
Phishing and other social engineering	**6%**
Zero-day threats	**6%**

A broader misalignment in threat landscape views

This underestimation is part of a wider disparity between perceived and actual threat landscapes. Businesses globally cite advanced persistent threats (APTs) (14%), ransomware (11%) and insider threats (9%) as the most dangerous.

In practice, however, the threats they most frequently encounter are supply chain attacks, followed closely by AI-powered attacks (30%) and phishing/social engineering (28%). This indicates that defensive resources may be disproportionately focused on sophisticated, targeted threats while more pervasive, ecosystem-based attacks are causing the daily operational friction.

Threats experienced by organizations over the past 12 months

	Share
Supply chain attacks	**31%**
AI-powered attacks	**30%**
Phishing and other social engineering	**28%**
Cyber espionage	**26%**
Ransomware attacks	**25%**
Trusted relationship attacks	**25%**
Insider threats	**24%**
Malware-as-a-Service	**23%**
Distributed denial of service (DDoS) attacks	**23%**
Advanced persistent threats (APTs)	**20%**

High-exposure enterprises are prime targets

The data further indicates that the threat is not evenly distributed and is acutely focused on the most connected organizations. The highest share of experienced supply chain attacks was among large enterprises (36%). Crucially, this same group reports having the highest mean number of software and hardware suppliers, directly correlating increased ecosystem complexity with a higher likelihood of attack. For these organizations, underestimating the supply chain threat is not a misstep but a failure to address one of the most probable attack vectors.

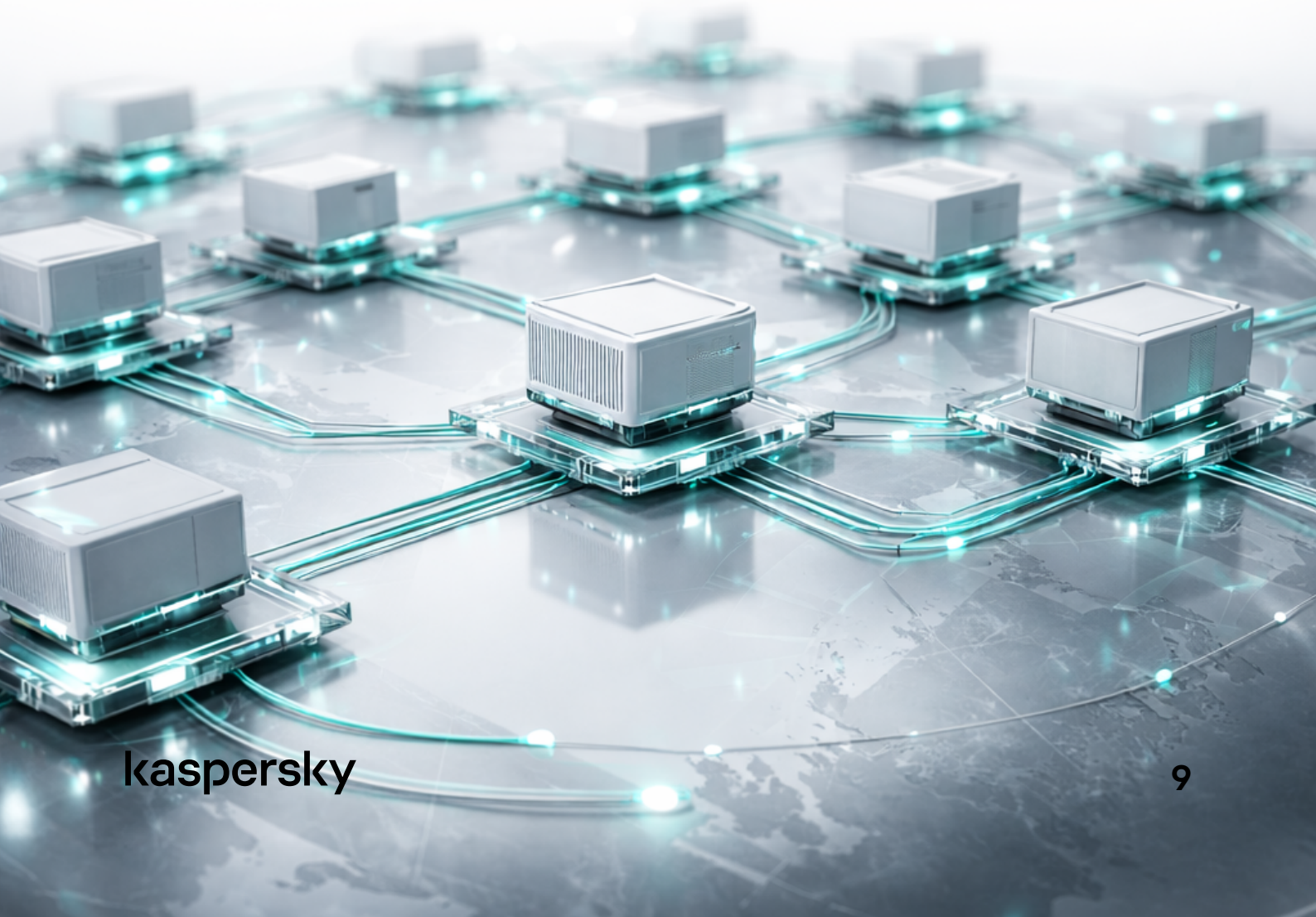
The scale of this exposure is substantial. On average, companies manage more than 60 distinct hardware and software suppliers. Furthermore, access to internal systems is widely granted, with the number of external contractors holding such privileges typically ranging from 25 to 99 and averaging 72. Collectively, these figures quantify the significant external attack surface that organizations must defend.

A telling indicator of overconfidence in effectiveness of protection systems or blind spots is that 21% of organizations claiming low or zero vulnerability to supply chain or trusted relationship attacks cannot even estimate their number of software and hardware suppliers. This suggests a fundamental lack of visibility into their own attack surface.

Geographical variations in awareness

Geographic analysis reveals notable differences in risk perception. Supply chain attacks are ranked among the top three most dangerous cyberthreats significantly more often than the global average by companies in Singapore (38%), Brazil (36%), Colombia (36%), and Mexico (35%).

Furthermore, countries that consider themselves most vulnerable to supply chain and trusted relationship threats include Vietnam (32%), Saudi Arabia (35%), Turkey (41%), Egypt (32%), Germany (34%) and Russia (38%). This suggests that regional threat intelligence, regulatory environments or recent local incidents may be driving a more accurate and heightened assessment of risk in these markets.



Chapter 2: Widespread concern meets fragmented defense

The previous chapter revealed that businesses systematically underestimate the pertinence of supply chain and trusted relationship (SC/TR) attacks. This chapter exposes a corresponding vulnerability in their defensive posture in the absence of universal, robust mitigation strategies.

While awareness of the risk is growing, the survey of businesses globally shows a fragmented and often insufficient approach to protection, creating a dangerous gap between concern and capability.

A patchwork of protections, dominated by basics

The analysis of protective measures reveals no single mitigation technique is employed by a majority of organizations. The most popular measure, the use of two-factor authentication (2FA), is implemented by only 38% of respondents. This foundational security control, while critical, is just a single layer in a defense-in-depth strategy required for complex ecosystem risks.

How organizations protect themselves from supply chain and trusted relationship risks

	Share
Use two-factor authentication (2FA)	38%
Add IT security requirements in our contracts with contractors (such as regular security audits, compliance with organization's relevant cybersecurity policies, etc.)	37%
Regularly check our existing contractors' cybersecurity level	35%
Add contractors to our IT security system	33%
Update software asset inventory regularly	31%
Use secure channels for sharing confidential information with contractors	31%
Evaluate contractors' reliability before working with them	28%
Share our cybersecurity expertise with contractors	28%
Implement the principle of least privilege for all contractors	27%
Implement email encryption	25%

The fact that even these core practices of vendor risk management are not universally adopted underscores a significant maturity gap. Regular checks of existing contractors' cybersecurity level are practiced by only about one-third of businesses (35%), while nearly two-thirds of organizations do not regularly audit their existing contractors' security postures, leaving them blind to evolving risks within their established partner network.

Inconsistent and incomplete due diligence

This inconsistency deepens at the point of vendor onboarding. Only 28% of organizations evaluate contractors' reliability before working with them and only 18% of all companies check contractors' cybersecurity level. Among those who do conduct cybersecurity assessments, there is no standard methodology. Practices range from reviewing incident response plans (58%) and cybersecurity policies (53%) to examining past incidents (51%) and compliance certificates (51%).

How organizations assess contractors' cybersecurity level before working with them

	Share
Request and review their incident response plans	58%
Request and review their cybersecurity policies	53%
Request and review their detected vulnerabilities	52%
Request and review their past cybersecurity incidents	51%
Review their compliance with industry cybersecurity standards (ISO/IEC 27001, NIST, IEC 62443, etc.)	51%
Request and review their penetration tests results	49%
Request and review their own cybersecurity policy of working with their contractors	46%

Notably, companies with prior attack experience demonstrate more rigorous habits. Those hit by supply chain attacks are more likely to request penetration test results (56%), while victims of trusted relationship attacks prioritize checks on compliance with industry standards (56%) and their contractors' own supply chain policies (53%).

This technical due diligence is often absent altogether. A concerning 38% of respondents who vet contractors before a deal do not include IT security checks in their assessment, focusing instead on legal, financial, and reputational criteria alone. This treats cybersecurity as a non-essential attribute rather than a foundational component of reliability.

Resource constraints and structural barriers

This fragmented defense is not for a lack of foresight. An overwhelming 85% of businesses admit their organizations need to upgrade protection against SC/TR risks. The barriers to doing so are clear. The primary obstacle, cited by 42% of respondents globally, the lack of a qualified workforce and competing IT security priorities.

85%
Need stronger protection

42%
Cite lack of qualified workforce as key obstacle

Factors preventing organizations from effectively protecting themselves from supply chain and trusted relationship IT security risks

	Share
Priority given to other IT security tasks and issues	42%
Lack of qualified IT security staff	42%
Lack of legal IT security obligations of contractors in our contracts	39%
Lack of understanding of these risks by non-IT security staff	32%
Lack of solutions allowing to control contractors' cybersecurity	31%
Lack of investment	29%
Lack of support from top management	27%
We don't have any such issues	5%

Beyond resource constraints, structural hurdles dominate regionally: a lack of legal IT security obligations in contracts (highlighted in Vietnam, Turkey, Spain, and Mexico) and a perceived lack of technical solutions to monitor contractors' cybersecurity (a key issue in Russia).

kaspersky

Widespread dissatisfaction and a search for solutions

Unsurprisingly, this diversity of incomplete mechanisms leaves businesses deeply unsatisfied. Globally, only 15% of enterprises consider their current security measures against supply chain attacks effective. This confidence plummets further in key economies like Germany (6%), Turkey (7%), Italy (8%), Brazil (8%), Russia (8%), and Saudi Arabia (9%).

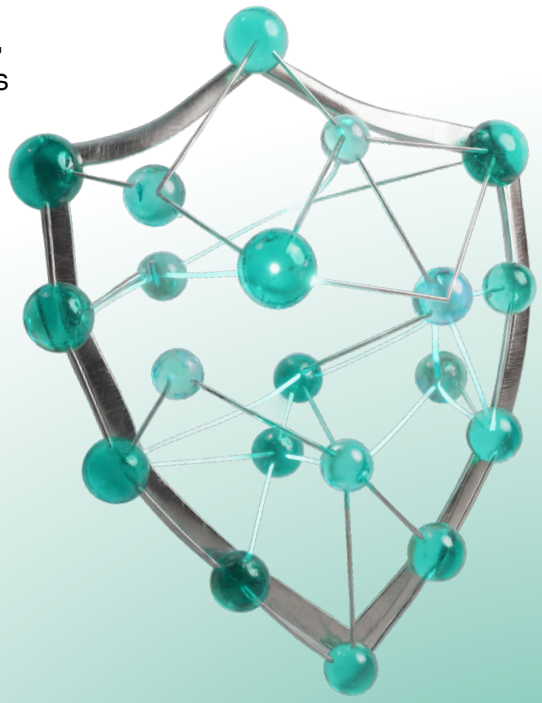
Faced with this reality, organizations are seeking new approaches.

To improve their protection, organizations are ready to consider resource-consuming solutions such as the possibility of sharing contractors' cybersecurity costs, with nearly 70% of respondents ready to help their partners boost their defenses and share respective costs to become more cyber resilient, and a quarter of respondents already doing just that.

This willingness to invest in collective resilience is even higher in India (83%), Indonesia (80%), Russia (80%) and Brazil (76%), signaling a pragmatic understanding that security is only as strong as the weakest link in the chain.

Conclusion: Transforming risk into resilient advantage

This report reveals that while awareness is growing, a widespread perception gap and fragmented defenses leave the global enterprise community dangerously exposed. The most prevalent threats, supply chain and trusted relationship attacks, are among the least prioritized, and the majority of organizations (85%) acknowledge their current protections are insufficient.



However, within this challenge lies a profound opportunity. In a world where operational disruption is the top-cited consequence, robust supply chain security is no longer just a cost of doing business but a direct source of competitive advantage.

Organizations that systematically close their protection gap will achieve superior business continuity, protect their brand reputation and foster stronger, more trusted partnerships. They become preferred, resilient nodes in the global network, attracting clients and partners who value stability.

Achieving this advantage demands a fundamental shift in approach, centered on three imperatives confirmed by the data

Collaboration over compliance

The strong global readiness to share cybersecurity costs (69%) must evolve from willingness to action. Leading enterprises will move beyond one-sided audits to build collaborative defense frameworks, investing in the collective resilience of their critical partners.

Transparency through continuous insight

Replacing point-in-time checks with continuous monitoring is non-negotiable. Organizations must demand and provide greater transparency, leveraging technology to gain real-time insight into partner ecosystems, thereby transforming visibility from a major weakness into a core strength.

Strategic investment in collective defense

Addressing the primary barrier of limited resources requires viewing cybersecurity expenditure differently. Investment must be targeted not only inward but outward, funding shared threat intelligence, co-developed incident response plans and ecosystem-wide training. This elevates security from a technical line item to a strategic enabler of growth and trust.

By embracing shared responsibility, operationalizing transparency and making strategic investments in the health of their entire digital ecosystem, businesses can navigate the fragile web of trust not as their greatest vulnerability but as their most durable asset.

Implementing a layered defense strategy

Deep technological integration throughout the supply chain affords companies unique competitive advantages but simultaneously creates systemic risks. Understanding these risks is critically important for technical executives and experts in the face of growing attacks on trusted relationships and supply chains which can entail significant damage. Only by implementing preventive measures across the organization and approaching partnerships with suppliers and contractors strategically can companies reduce these risks and ensure the resilience of their business.

Organizations should take comprehensive measures to reduce the risks associated with supply chain attacks:

1. Thoroughly evaluate suppliers. It's crucial to assess the security level of potential suppliers before beginning collaboration. This includes requesting a review of their cybersecurity policies, information about past incidents, and compliance with industry security standards. For software products and cloud services, it's also recommended to collect data on vulnerabilities and penetration tests, and sometimes it's advised to conduct dynamic application security testing (DAST).

2. Strengthen network level visibility with advanced NDR tools like Kaspersky Anti Targeted Attack (KATA), which analyzes both northsouth and crucial eastwest traffic to detect suspicious network activity that may indicate a supply chain compromise. Using extended IDS, anomaly detection and integrated sandboxing, KATA enables detailed retrospective analysis and supports more accurate incident investigation and response. As part of a SOC workflow, its events can be correlated with other security systems, helping analysts detect sophisticated attacks with greater precision.

3. Adopt preventive technological measures. The risk of serious damage from supplier compromise is significantly reduced if your organization implements security practices such as the principle of least privilege, zero trust, and mature identity management.

4. Implement contractual security requirements. Contracts with suppliers should include specific information security requirements, such as regular security audits, compliance with your organization's relevant security policies, and incident notification protocols.

5. Ensure continuous monitoring using solutions like XDR or MXDR, which are part of the Kaspersky Next product line, for real-time infrastructure monitoring and detecting anomalies in software and network traffic. Your choice should depend on the availability of in-house staff members capable of carrying out such monitoring.

6. Enhance visibility into third-party risks with services like Kaspersky Digital Footprint Intelligence (DFI), which identifies compromised supplier accounts linked to your organization's assets. With upcoming upgrades, it will also monitor dark and deep web sources for signs of partner-related incidents, including unauthorized publication and sale of confidential data, ransomware activities and website defacements.

7. Develop an incident response plan. It's important to create a response plan that includes supply chain attacks. The plan should ensure that breaches are quickly identified and contained; for example, by disconnecting the supplier from company systems.

8. Collaborate with suppliers on security issues. It's vital to work closely with suppliers to improve their security measures; such collaboration strengthens mutual trust and makes mutual protection a shared priority.

Supply chain attacks often exploit something that is already trusted and allowed inside the organization such as software updates, service accounts, integrations or remote access tools. This means that protection does not depend only on having security solutions in place. It also depends on whether those solutions:

- are properly configured,
- continuously monitored,
- and actively managed.

Even advanced protection can lose effectiveness if policies are misconfigured, alerts are ignored, or monitoring is inconsistent. In supply chain scenarios, small gaps in configuration or oversight can allow malicious activity to blend into normal operations.

Kaspersky Next MXDR Optimum strengthens protection by adding continuous expert monitoring and investigation. Experts validate whether the observed behavior indicates a real incident and help determine severity and urgency.

24/7 expert monitoring validates suspicious activity and confirms whether it represents a real supply chain incident.

Submitting an incident helps to start expert-led investigation and determine the scope and impact of the incident, reducing the risk of incomplete or incorrect conclusions.

Guided or managed response ensures that containment actions are taken correctly and in time, even without in-house expertise.

Learn more:

kaspersky