Telefónica Tech

NextDefense

Supply chain protection

Keys to cyber resilience

Effective cyber security strategies for third-party risk management. Anticipating threats and protecting your critical assets.

Summary

Over the last year, 60% of companies have reported a supply chain security breach, exposing organizations to unseen risks. This paper addresses a critical and overlooked aspect: protection against third- and fourth-party cyber threats.

The digitalization of processes and the expansion of business and organizational operations expand the attack surfaces, increasing risks and vulnerabilities. If not properly managed, remote suppliers, subcontractors and common digital components become risk vectors. We introduce the FPRM (Fourth-Party Risk Management) approach to address this challenge, which anticipates cascading effects of indirect actors, integrating into cyber security strategies to protect each level of the supply chain.

This document proposes a practical framework for action that combines visibility, traceability, and collaboration. It includes practices such as extended audits, sector drills, continuous monitoring and contractual clauses under recent international regulations, including NIS2, DORA and the Cyber Resilience Act, which redefine cyber security standards globally.

In addition, we also explore solutions such as Telefónica Tech's **Third-Party Risks**, which enable automated, data-driven risk assessment as well as risk mitigation. This comprehensive approach connects advanced technology, robust processes and a committed organizational culture.

In this document you will find the keys to protecting your critical assets, reducing your exposure to breaches and building a resilient supply chain prepared for today's digital challenges.

INDEX

1. Introduction

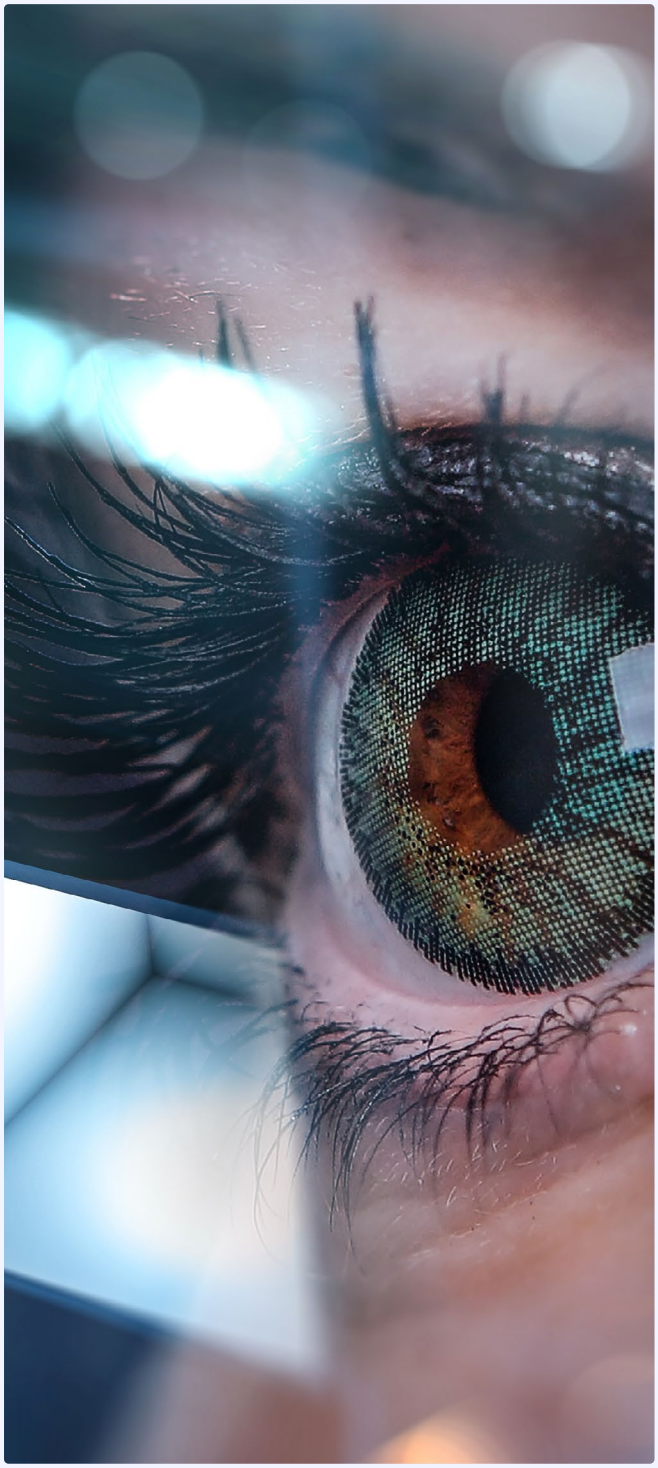
Cyber resilience is no longer optional. It is indispensable for business continuity in an interconnected world.

The massive digitalization of critical industrial and operational processes has transformed the landscape of modern organizations. This change has enabled advances in efficiency, productivity, and connectivity, but it has also expanded the attack surfaces, generating risks that transcend physical and digital boundaries.

Threats are no longer limited to the internal environment of businesses. They extend to a digital ecosystem of third parties and external actors that can introduce vulnerabilities. In this context, cyber security becomes a strategic pillar to ensure operational resilience, regulatory compliance and trust among partners, customers, and citizens.

Supply chains are vulnerable to sophisticated attacks due to their distributed and transnational nature. This document analyzes current risks and offers tools and strategies to protect sensitive assets, anticipate risks, and foster a culture of cyber resilience.

We invite you to explore ways to protect your sensitive assets, anticipate third- and fourth-party risks and develop a culture of cyber resilience with strategies that strengthen your digital defenses and foster collaboration among all stakeholders.



2. Current landscape: threats, impacts, and trends

Digital threats are a daily reality that evolves faster than conventional defenses.

Today's threat environment is characterized by more sophisticated attacks, exploitation of new technologies, and a fragile digital ecosystem.

Organizations face risks in the following areas:

TECHNOLOGY THREATS

- **0-day vulnerability attacks:** unknown breaches that are exploited before patches are developed.
- **Adaptive and polymorphic malware:** malicious software programs that change to evade traditional defenses.
- **Data exfiltration through API interfaces and IoT devices:** unauthorized access to sensitive information through poorly secured integration points.
- **Attacks on AI models (data poisoning, inference, model stealing):** vulnerabilities affecting the security of AI and Generative AI systems.

HUMAN THREATS

- **AI-driven hyper-realistic phishing:** fraudulent messages created with AI that mimic legitimate senders.
- **Deepfakes and digital identity theft:** creation of fake multimedia content to impersonate and manipulate identities.
- **Vulnerable or compromised vendors:** actors with low cyber security maturity that become backdoors to better protected organizations.

REGULATORY AND SYSTEMIC THREATS

- **Risks of using third-party software:** integration of tools that create new attack surfaces if not properly audited.
- **Systemic cyber threats and cascading effects:** attacks that originate in a remote link of the chain and quickly escalate to the rest of the ecosystem.
- **Regulatory and geopolitical impacts:** operating globally adds legal complexity and exposes to trade restrictions or political tensions.

These risks could affect the availability, integrity, and confidentiality of essential services, impacting businesses and economic and social stability.

Fourth Party Risk Management (FPRM)

In an interconnected digital ecosystem, risks do not end with your direct suppliers, they extend to actors outside your control.

The aforementioned threats do not only impact organizations. Their complexity and evolution can propagate through indirect actors in supply chains. Here the **cascading effect** becomes a danger: a vulnerability in a remote supplier or subcontractor can quickly escalate, compromising the stability of multiple connected organizations.

Fourth Party Risk Management (FPRM) emerges as a critical response to address threats that, while initially seemingly peripheral, can cause significant disruptions. This approach focuses on identifying, assessing, and mitigating the risks of your suppliers' vendors, actors that operate outside of your direct control but are essential to your digital ecosystem.

Why manage the risk of the fourth parties?

In a context of increasing connectivity and interdependence, it is imperative that organizations take a proactive and expanded view of risk management. This involves auditing direct suppliers, mapping relationships in the chain, continually assessing their security posture and defining clear controls.

Companies are exposed to invisible vulnerabilities that can unleash devastating ripple effects if they do not address these risks holistically. Prevention and active monitoring are strategic to ensure operational resilience and trust.

Organizations must understand that **risk does not end with their direct suppliers**. Identifying, assessing, and mitigating the risks posed by the fourth parties is essential to building operational resilience in an interdependent digital ecosystem.

In the following section we address **how to translate this approach into practice** through cyber security strategies specifically aimed at protecting the supply chain at all levels.

3. From theory to practice: supply chain cyber security

The security of your supply chain depends on its weakest link. Visibility, control and collaboration are essential to protect it.

Threats are not limited to direct suppliers. Every indirect link, the fourth and nth parties, represents a potential entry point for systemic attacks. The main challenges are:

- **LACK OF VISIBILITY ON THE THIRD-PARTY NETWORK:** many organizations are unaware of the suppliers with which their direct partners interact, which limits their ability to assess and monitor
- **LACK OF TRACEABILITY AND MAPPING OF THE DIGITAL ECOSYSTEM:** without clear inventories of technological and relational dependencies, it is unfeasible to identify indirect risk vectors.
- **DIFFICULTY TO AUDIT OR APPLY CONTROLS IN EXTERNAL ENVIRONMENTS:** outsourcing and subcontracting blur the boundaries of responsibility and reduce the effectiveness of preventive measures.
- **DIVERSITY OF MATURITY AND COMPLIANCE IN THE CHAIN:** the heterogeneity of technical and cultural capabilities in cybersecurity prevents a homogeneous defense.
- **REGULATORY AND GEOPOLITICAL RISKS:** operating with international suppliers adds legal complexity and exposes to political tensions, trade restrictions or contradictory legislation.
- **LACK OF COMMON STANDARDS AND SUPPLIER CERTIFICATION MECHANISMS:** lthe absence of universal frameworks for assessing third-party risk makes benchmarking and informed decisions difficult.
- **RESPONSE TIME TO THIRD-PARTY INCIDENTS:** no defined communication channels or visibility into supplier systems, delaying detection and containment.

Case Study

A fictitious pharmaceutical company suffered a critical impact due to an attack on its supply chain. The attack began with a small outsourced transportation company that managed the movement of vaccines. The attackers exploited a vulnerability in that company's logistics software, accessing sensitive routing and warehouse data.

The attackers intercepted a critical shipment and altered logistics data to delay distribution in key regions.

As a result, this company suffered financial losses, reputational damage and regulatory penalties for failures to deliver medical supplies. The company had failed to audit the cybersecurity of this small supplier, underestimating its role in the chain.

The company adopted multiple preventive measures to mitigate future incidents:

- **Implemented periodic cyber security audits** of all suppliers, including those of less operational relevance.
- **Developed incident response drills** specific to the logistics sector, involving direct and indirect suppliers.
- **Adopted continuous monitoring technologies,** such as software that maps supply chain security in real time.
- **Formalized service level agreements (SLAs)** with strict clauses on cyber security, establishing clear responsibilities in case of incidents.

These actions strengthened its security and increased the confidence of its partners, suppliers, and customers. This case highlights the need for a robust strategy to manage risk throughout the supply chain, from the key players to the smallest links.

Comprehensive risk management. The main lesson from this fictional story is that risk management must include rigorous 'onboarding' assessments, continuous monitoring of supplier security, contracts with clear cyber security requirements, and joint incident response exercises.

Even the most protected actors can be made vulnerable by third parties without these measures.

4. Regulations defining the new compliance framework

Regulation is key to building digital trust, anticipating risk, and strengthening organizational resilience.

The regulatory response has accelerated internationally, driving frameworks that integrate cybersecurity into the digital lifecycle.
Notable examples include:

- **NIS2 Directive:** Extends resilience requirements to critical suppliers and requires third-party audits.

  Example: *A European energy company that outsources critical services to an IT firm must implement regular cyber security assessments and report incidents within stricter timeframes, reducing the risk of widespread disruptions.*

- **DORA (Digital Operational Resilience Act)** regulation establishes measures such as resilience testing and ICT risk management, targeting the European financial sector.

  Example: *banks integrating cyberattack simulations into their operations to ensure continuity of service in the event of breaches in technology providers.*

- **Artificial Intelligence Regulation, AI Act (EU):** Classifies artificial intelligence systems by risk levels and establishes requirements.

  Example: *A provider of facial recognition solutions must comply with traceability and human supervision requirements to operate in the European Union..*

- **CRA (Cyber Resilience Act) Regulation:** Applies to products with digital elements, requiring secure design from the origin and continuous security updates.

  Example: *IoT device manufacturers in Europe must provide security patches during the life cycle, reducing vulnerabilities.*

- **China's Cyber security Law** imposes security reviews and data storage in the country.

  Example: *International companies in China have adjusted their data policies, including restrictions on transferring information out of the country.*

- **Executive Order 14028 (U. S.):** Strengthens cyber security requirements for federal government suppliers, promoting SBOMs (Software Bill of Materials).

  Example: *Software contractors to the U.S. government must provide detailed lists of software components to ensure control and absence of vulnerabilities.*

INTERNATIONAL STANDARDS

- **ISO 27001:** Information security management.

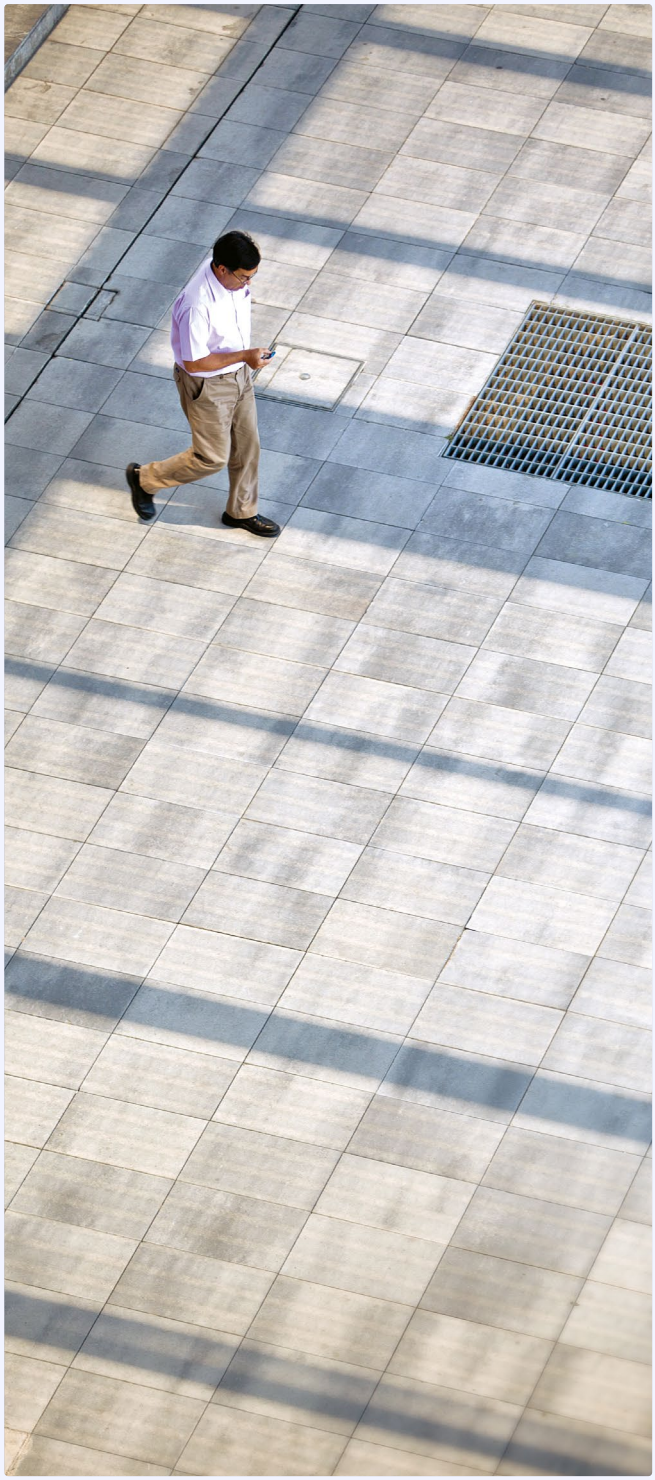
  Example: *A multinational company adopts this standard to structure and document its security policies and facilitate external audits.*

- **ISO 22301:** Business continuity.

  Example: *A pharmaceutical supplier uses ISO 22301 to minimize disruptions in the production of essential medicines following a cyberattack.*

- **NIST CSF:** Framework to identify, protect, detect, respond, and recover.

  Example: *A U.S. telecommunications company implements NIST CSF to strengthen security governance in its critical infrastructure..*



Compliance and data privacy

Compliance and data privacy are pillars of modern risk management, especially with evolving laws and regulations. Telefónica Tech helps companies adopt a comprehensive approach to ensure alignment with key regulations such as GDPR and other international legislation, minimizing legal and reputational risks.

Our solutions enable companies to implement security standards that meet regulatory requirements and strengthen the trust of customers, partners, and parties. Our proactive approach includes data traceability, protection of sensitive information and adaptation to new regulatory requirements, ensuring the resilience and operational sustainability of organizations.

These regulations should not be seen as a bureaucratic burden, but as a strategic opportunity to improve the cyber maturity of organizations. Security can be aligned with innovation, legal risks can be minimized, and the trust of customers, regulators, and partners can be strengthened by proactively adopting these standards.

5. Solutions and best practices for effective defense

An effective defense is not built on isolated technology, but on the synergy between smart tools, solid processes, and committed people.

An effective cyber security strategy is built on three pillars: technology, processes, and people. They must be integrated in a coordinated way to deliver a holistic and resilient defense.

TECHNOLOGY

- Zero Trust Architecture: implements the "never trust, always verify" principle, restricting access to only authenticated and authorized users at every point in the network.
- Network segmentation: isolates IT, OT, and third-party environments to contain threats and minimize lateral movement.
- Tools such as Clean Email (protection against spoofing and malicious emails) and Security Edge (control and visibility of remote and cloud access).
- Detection and response systems (EDR/XDR): monitors endpoints and networks with automatic response.
- Threat Intelligence platforms: anticipates threats through contextualized and actionable information.

PROCESSES

- Define policies and procedures: establish clear protocols for managing access, updates, backup, incident response, and supplier evaluation.
- Ongoing third-party risk management: performs regular assessments, commitment tracking and audits of key suppliers.
- Secure DevSecOps: integrates security from design into software development cycles. DevSecOps combines development (Dev), security (Sec) and operations (Ops), ensuring that security is integrated from the early stages of development through implementation and ongoing operations.
- Secure MLOps: applies security principles to the development, deployment and operation of machine learning models. MLOps (Machine Learning Operations) ensures that AI models are reliably managed, protected against risks such as data manipulation, model leakage and algorithm misuse.
- Cyber incident drills: rehearses critical scenarios to validate the responsiveness of all actors

PEOPLE

- Awareness and continuous training: trains employees and suppliers on best practices, new threats and their role in defense.
- Clear governance: defines responsibilities, security committees, and incident escalation lines.
- Security culture: promotes responsible and proactive behavior at all levels of the organization in the face of digital risk.

When these three components are aligned, organizations improve their security posture and strengthen their ability to resist, recover, and adapt to cyber threats.

The goal is to consolidate a resilient security posture through a coordinated approach that integrates advanced technology, robust operational processes, and an organizational culture focused on threat prevention, detection, and response.

6. Suggested strategy: integrated approach

An isolated strategy is vulnerable. Only a systemic vision can withstand current and future threats.

Addressing the cyber security of infrastructures and their supply chains requires a comprehensive strategy that considers the interdependence of risks, the dynamics of threats as well as the diversity of actors. A holistic approach can fill the gaps that individual solutions fail to address, prioritizing resources and accelerating incident response.

Key elements of a comprehensive strategy

1. Clear and effective governance: Adopt frameworks such as GRC (Governance, Risk and Compliance) to structure responsibilities and align security policies with business objectives. Uses tools to map risks, automate controls and streamline decision making.
2. International collaboration: Participates in multilateral initiatives and cooperation forums to address global threats. Adapts internal processes to global regulations such as NIS2, CRA or DORA to facilitate compliance in various markets.
3. Public-private partnerships: Establish collaborative networks that share intelligence and resources to prevent and mitigate cyber threats. For example, integrate into Threat Intelligence platforms that provide early warnings.
4. Continuous training: Invest in training and promote a culture of cyber security throughout the organization to minimize human risks. Conduct periodic simulations to measure and improve cyber-incident preparedness

A comprehensive strategy is not a sum of disconnected solutions. It is a coordinated framework that anticipates risks, optimizes resources and strengthens resilience to any attack. Those who adopt this vision will be better prepared to lead and resist in the digital environment.

7. Road to cyber resilience

Prevention is not an expense; it is a strategic investment. Preventing today avoids a crisis tomorrow.

Key Actions

1. Diagnose the current state of cyber security: Conduct technical audits and simulations to assess vulnerabilities in the organization and supply chain.
2. Strengthen governance: Establish security policies, defined roles and decision flows aligned with strategic objectives.
3. Develop a continuity and recovery plan: Implement strategies to maintain critical operations in contingencies.
4. Formalize cyber security agreements with suppliers: Include security clauses in contracts, audits and incident management.
5. Promote a culture of cyber resilience: Train employees and partners in best practices and digital threat awareness.
6. Collaborate with industry networks and intelligence platforms: Participate in initiatives that share information on new threats.
7. Embrace disruptive technologies for automated trust: Incorporate blockchain and smart contracts to strengthen traceability and transparency in the supply chain. These technologies automate key processes, reducing risks of manipulation or human error, and ensure the integrity of shared data.

Services such as Telefónica Tech's **Third-Party Risks** can complement these efforts. This service enables continuous monitoring of the level of cyber security in your supply chain in a non-intrusive and automated way.

You can identify and prioritize the most critical risks by integrating solutions like this, optimizing resources and strengthening security.

Time to act

Cyber resilience is not achieved with promises, but with vision, commitment, and sustained execution.

Telefónica Tech knows that the cyber resilience of infrastructures and their supply chains is key to the success of any organization.

Business ecosystems are becoming increasingly interconnected, creating opportunities as well as new risks.

Reliance on third parties remains a critical and multifaceted risk vector. According to Bitsight, 59% of companies have reported a data breach caused by a third party. It further reminds that "there are 'hidden pillars' in the supply chain, with few suppliers concentrating much of the systemic risk."

This risk extends to specific threats such as ransomware, which has increased by 25% in the last year, intensifying its attacks against smaller companies, according to the State of the Underground (2025) study.

That's why at Telefónica Tech we offer capabilities to protect you against new threats. Our solutions such as Third-Party Risks, backed by our partner ecosystem and the professional services of our global DOC, enable you to:

- **Constantly monitor** the safety of your suppliers.
- **Measure and mitigate** supply chain risks through data.
- **Quantify and communicate** risks in terms accessible to all organizational levels.

The integration of technologies such as blockchain can also be key to increasing trust between actors and ensuring the security of the digital ecosystem.

Telefónica Tech helps you assess your security, identify vulnerabilities, and apply advanced solutions that boost your operational resilience and digital confidence.

Our team of experts will work with you on a comprehensive strategy adapted to your needs. Together we will protect your assets, strengthen the trust of your customers, suppliers and partners, and ensure the sustainability and competitiveness of your business. The time to act is now.

Telefónica Tech