# CYBER RISK WITHOUT BORDERS: MANAGING EXPOSURE IN A CONNECTED ECOSYSTEM

## Navigating Global Exposure Across Customers, Partners, and Suppliers

In today's business landscape, borders matter less than ever. Companies operate across continents, engage with partners in multiple jurisdictions, and rely on complex international supply chains. While this global interconnectedness fuels growth and opportunity, it also introduces a new reality: cyber risk is no longer local, it is systemic, borderless, and increasingly unpredictable.

As digital ecosystems expand, so does the attack surface. Organizations are no longer exposed only through their own infrastructure, but also through every external relationship they maintain. In a world without frontiers, assessing cyber risk means assessing the entire network of partners, customers, and suppliers.

## The New Nature of Cyber Risk: Interconnected and Amplified

The rapid growth of global trade, digital platforms, and connected technologies has created an environment where interdependence is both a strength and a vulnerability. A single weak link can expose an entire ecosystem.

Recent analyses highlight that the world's increasing interconnectivity is driving a convergence of technological, geopolitical, and operational risks, making cyber threats more complex and widespread. At the same time, the expansion of digital ecosystems and reliance on shared infrastructures have significantly increased the "attack surface" available to threat actors.

This means that cyber risk is no longer confined to IT departments, it has become a strategic business risk affecting operations, reputation, and revenue.



© 2026 CRIF s.p.a. - All rights reserved

# CYBER RISK WITHOUT BORDERS: MANAGING EXPOSURE IN A CONNECTED ECOSYSTEM

## Evaluating Partners, Customers, and Suppliers: A Critical Imperative

For organizations operating globally, one of the most critical challenges is evaluating the risk profile of third parties.
Every new relationship introduces potential vulnerabilities:

- Customers may expose companies to fraud, data misuse, or compliance risks
- Business partners may operate under different cybersecurity standards or regulatory frameworks
- Suppliers can become entry points for cyber-attacks, especially in interconnected supply chains

In many cases, companies rely on third-party vendors for essential services such as cloud computing, logistics, or data processing. This dependency on external entities increases exposure to breaches and operational disruptions, especially when security practices are inconsistent across regions.

Additionally, regulatory landscapes differ significantly from country to country, making it harder to ensure a uniform level of protection. As a result, companies must adopt a risk-based approach to international relationships, combining financial, operational, and cyber due diligence.

## The Hidden Threat: Supply Chain Disruption

One of the most critical, and often underestimated, dimensions of cyber risk is its impact on supply chain continuity.

In an interconnected environment, a cyber incident affecting one supplier can quickly cascade across multiple organizations. Recent events have demonstrated that disruptions to a single system or provider can lead to widespread operational failures across industries, highlighting the fragility of interconnected infrastructures.

Cyber-attacks targeting supply chains are particularly dangerous because they exploit trust relationships. Attackers may compromise a smaller or less-protected supplier to gain access to larger, more secure organizations.



© 2026 CRIF s.p.a. - All rights reserved

The consequences can include:

- Interruption of production or service delivery
- Delays in logistics and distribution
- Financial losses and contractual penalties
- Reputational damage and loss of customer trust

Moreover, as global supply chains become more digitalized, even non-IT disruptions, such as outages in communication systems or cloud platforms, can have significant business impacts.

## The Role of Digital Dependency

Modern organizations rely heavily on digital infrastructures, from cloud services to IoT devices and AI-driven platforms. While these technologies enable efficiency and scalability, they also introduce new vulnerabilities.

The increasing reliance on interconnected systems means that failures can cascade across borders and sectors, potentially affecting critical services such as finance, healthcare, and logistics.

This level of dependency makes resilience a key priority. Companies must not only prevent cyber incidents but also ensure they can respond quickly and maintain continuity when disruptions occur.

© 2026 CRIF s.p.a.  - All rights reserved

# CYBER RISK WITHOUT BORDERS: MANAGING EXPOSURE IN A CONNECTED ECOSYSTEM

## Building a Global Cyber Risk Strategy

To navigate cyber risk in a borderless world, organizations need to move beyond traditional security models and adopt a holistic, ecosystem-driven approach.

Key priorities include:

*1. Third-Party Risk Management*

- Conduct thorough due diligence on partners, customers, and suppliers
- Monitor ongoing risk exposure, not just during onboarding
- Integrate cyber risk into supplier evaluation and selection processes

*2. Continuous Monitoring*

- Implement real-time monitoring to detect changes in risk profiles
- Leverage global data sources to identify emerging threats
- Use predictive analytics to anticipate disruptions

*3. Supply Chain Resilience*

- Diversify suppliers to reduce dependency on single points of failure
- Develop contingency plans for critical suppliers
- Test business continuity and incident response scenarios

*4. Global Compliance and Governance*

- Align with international cybersecurity standards and regulations
- Ensure consistency in security practices across regions
- Strengthen contractual requirements for third-party cybersecurity

*5. Collaboration and Intelligence Sharing*

- Share threat intelligence across ecosystems
- Collaborate with partners to improve overall resilience
- Adopt a collective approach to cybersecurity

Together to the next level

SKYMINDER BY CRIF

© 2026 CRIF s.p.a. - All rights reserved

# CYBER RISK WITHOUT BORDERS: MANAGING EXPOSURE IN A CONNECTED ECOSYSTEM

## From Risk to Opportunity

While the challenges are significant, companies that effectively manage cyber risk can turn it into a competitive advantage. By demonstrating strong governance, resilience, and transparency, organizations can build trust with customers and partners worldwide.

In a world without frontiers, trust becomes a critical currency and cyber resilience is its foundation.

## Conclusion

Cyber risk is no longer a technical issue confined within organizational boundaries. It is a global, interconnected challenge that reflects the complexity of today’s digital economy.

For companies operating internationally, success depends on their ability to understand, monitor, and manage risk across their entire ecosystem, from customers to suppliers and beyond.

In this new reality, the question is no longer whether a cyber incident will occur, but how prepared organizations are to anticipate, absorb, and recover from it.

In today’s global business landscape, assessing a partner solely on financial performance is no longer enough. Organizations need to understand in advance whether a partner, or potential partner, is vulnerable to cyber-attacks, as these risks can quickly translate into operational disruption, financial loss, and reputational damage.

To address this growing need, **SkyMinder, CRIF’s global business information platform**, designed to evaluate B2B trade risks across international markets, offers the KYND Cyber Risk Report, adding a critical new dimension to partner assessment.



© 2026 CRIF s.p.a. - All rights reserved

# CYBER RISK WITHOUT BORDERS: MANAGING EXPOSURE IN A CONNECTED ECOSYSTEM

Powered by KYND's pioneering technology and expertise, the report transforms complex cybersecurity data into clear, easy-to-understand insights, enabling businesses to quickly identify and quantify cyber exposure. KYND, a UK-based cyber risk specialist with CRIF as a major shareholder, brings advanced capabilities to make cyber risk visible and actionable.

- Suitable for any type of business
- Fast and easy, requires only a company name and website
- Immediate visibility into cyber vulnerabilities


The KYND Cyber Risk Report is seamlessly available via SkyMinder, which delivers comprehensive information on companies worldwide, covering over 230 countries and territories. From credit and financial risk to anti-money laundering, anti-bribery, and cyber risk, SkyMinder provides a complete 360° view—empowering organizations to make informed decisions and protect their global business ecosystem from emerging threats.

About KYND
Founded in February 2018 and headquartered in London, KYND is a new breed of cyber company. KYND makes complex cyber risks simple to understand and manage for every organization, regardless of size, means or industry sector.

CRIF
Together to the next level

SKYMINDER
BY CRIF

© 2026 CRIF s.p.a. - All rights reserved