CLOSING THE VISIBILITY GAP:
5 Questions to Ask Yourself About Your Third-Party Risk

Your business relies heavily on third parties to operate efficiently, innovate ahead of competitors, and deliver value to customers. While critical to continued success, each vendor relationship introduces risk to your organization.

According to an Opus and Ponemon study, the average company today shares confidential information with nearly 600 third parties — that's a lot to keep track of. Unfortunately, most organizations don't. Only 34% keep a comprehensive inventory of these third parties, let alone monitor their risk profiles.

With manual and imperfect third-party assessment practices, organizations only have a limited view of active and emerging threats. However, this is only a part of the reason why third-party risk (TPR) teams struggle to fully understand their partners' risk landscape — and how that risk relates to them. Growing regulatory mandates, a surging skills shortage, ineffectual procurement practices, and dangerous visibility gaps create a perfect storm for security issues. As a result, it's estimated that more than 50% of organizations have suffered a data breach through their vulnerable third parties.

You must fully understand the risk that third parties introduce to your organization before you can effectively defend against it. **Start by thinking critically about these five questions and answering them honestly**.

QUESTION 1
Who Are My Most Critical Vendors?

When it comes to third-party risk, not all vendors are created equal. Consider how critical each vendor's solutions or services are to your business. Then, rank each company by the potential business impact of a breach in terms of revenue loss, business disruption, lack of access to sensitive internal systems, leaked customer data, etc.

Also consider grouping vendors by criteria, such as spend, profit gained, industry, or offering, to track meaningful metrics like key risk indicators (KRIs) and return on investment (ROI). For example, you may want to create a category of vendors who manage your sensitive data because vendor data leaks represent a potentially huge cost to your organization — both financially and in terms of reputational damage to your brand.

This risk-prioritized vendor list will empower your TPR team to focus their efforts by continuously monitoring risk levels for your critical third parties, enabling real-time alerts throughout the lifecycle of those relationships, and implementing strong controls to ensure confidentiality, data integrity, and compliance. They will also be able to deprioritize less critical relationships for efficient TPR management.

Understanding which third parties matter most to your business also enables vulnerability management teams to prioritize patching and application control to safeguard the software that you rely on from critical vendors.

When you conduct the vendor ranking process, be sure to consider your legal and compliance responsibilities as they relate to your third-party ecosystem, as well. See question 2 for more on this.

QUESTION 2
What Am I Legally Accountable For?

Your industry and organization has a unique set of regulatory requirements. When assessing the risks versus the rewards of doing business with a provider, it's important to know your own liabilities and responsibilities in the event of a breach. For instance, GDPR requirements often hold organizations liable for their customer's data in the event of a third-party data breach.

Many organizations rely on GRC systems to tackle third-party compliance challenges. However, traditional GRC systems miss an important piece of the puzzle without contextualized intelligence on active, emerging, and historic threats to each supplier. It's critical to connect those dots with real-time context and a historic view of how each vendor's risk standing has changed over time.

For maximum efficiency, consider solutions that enable you to view this information directly within the GRC system you already use.

QUESTION 3

What Is My Current Vendor Risk Assessment Process?

Manually reviewing a never-ending stack of vendor security questionnaires is a full-time job in and of itself — and TPR teams are feeling the pressure. Yet, security questionnaires only provide a static snapshot of a vendor's security posture. These assessments may be outdated by the time you receive them, and they're useless for tracking your partners' rapidly evolving infrastructures, policies, and risk landscapes over time. Making matters worse, since vendors fill out these forms directly, their answers are usually subjective and potentially biased.

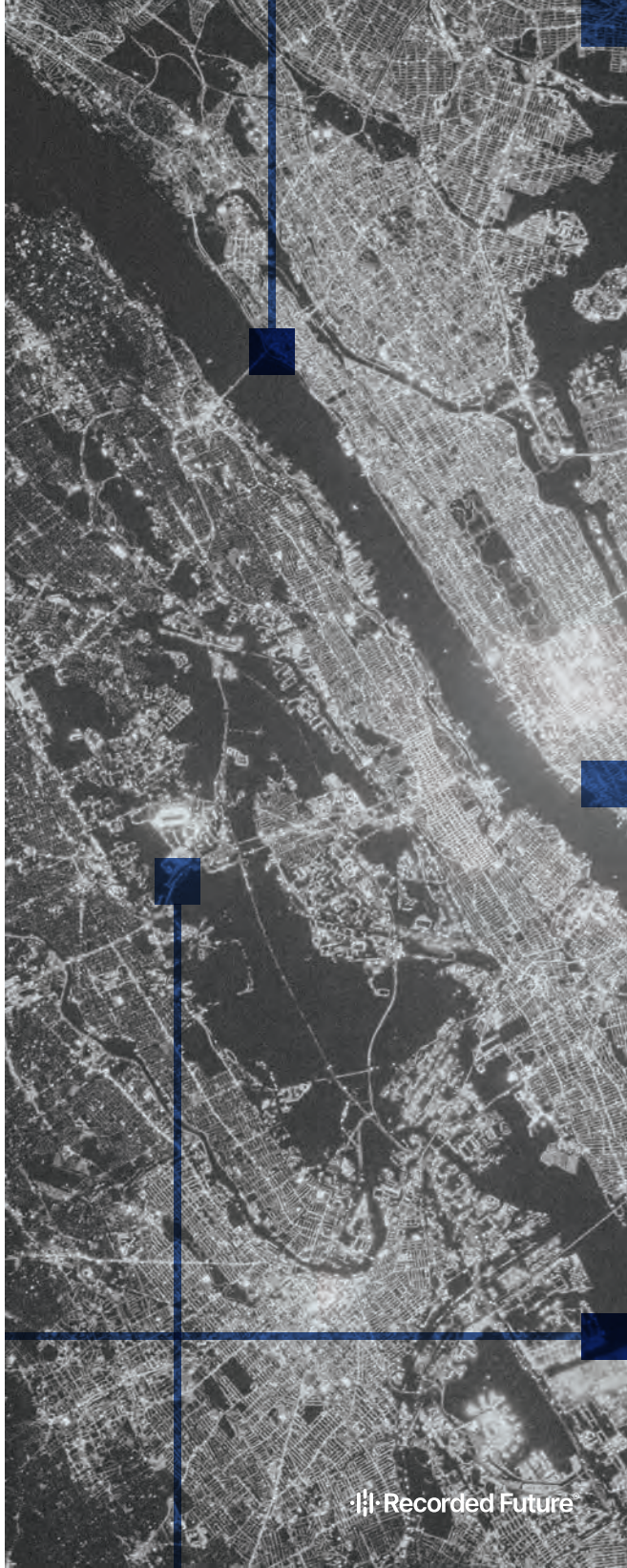
Ask yourself, "what does our procurement and regular reassessment process look like today?" Consider certain criteria you look for and hold your vendors to. Then, identify solutions that provide real-time visibility to close the gap created by point-in-time assessments. Also considers solutions that dynamically categorize, link, and analyze risk information on your current vendors, new potential partners, and even M&A targets.

QUESTION 4
Who Else in My Organization Needs This Information?

As TPR teams focus on assessing risk levels across a growing, interconnected vendor network, cross-functional information sharing doesn't always bubble to the top of their priority list. However, risky applications, vulnerable products, and certain behaviors from third parties have the potential to threaten other lines of your business if you fail to effectively communicate and address them.

To get on the same page, all security teams, from TPR, to vulnerability management, to SecOps and response, need access to the same information.

Consider solutions that empower teams across your organization to break down silos by centralizing and continuously updating third-party intelligence. For example, access to shared information on malware or exploits targeting a critical vendor's applications empowers your incident response team to respond fast and block the attack. Or, real-time context on third-party partners being targeted in the wild or being discussed on the dark web, along with insights into attackers' motivations and capabilities, enables the entire security organization to optimize workflows and amplify their impact.

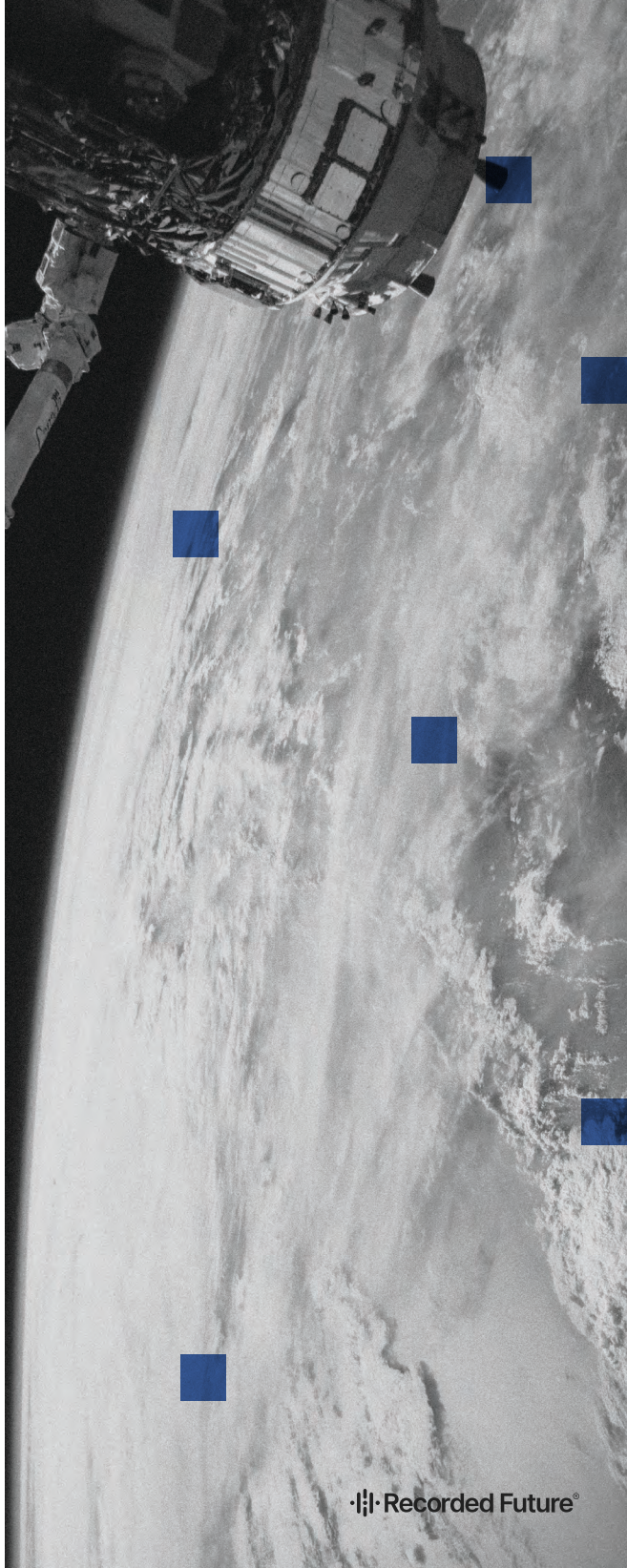


QUESTION 5

How Does the Global Threat Landscape Affect My Partners?

As the business and geopolitical landscapes rapidly evolve, your vendors are often exposed to new risks and potentially dangerous circumstances that could ultimately impact your business. However, manual threat research and monitoring of regional and economic trends across every provider and language is virtually impossible. You need to respond swiftly to protect your supply chain, but you run the risk of being blindsided when intelligence trickles in piecemeal.

Consider solutions that empower you to reduce risk and protect your assets by accelerating critical decision-making with real-time, contextual intelligence on relevant geopolitical threats and trends impacting your vendors.



Elite Intelligence to Close the Visibility Gap

Examining your organization's current third-party risk exposure, coverage, and controls will enable you to define a baseline for improvement, create an action plan, and drive your program's maturity.

Third-party intelligence from Recorded Future empowers you to understand, monitor, and measure your real-time exposure to third-party risk.

REQUEST A DEMO TODAY

Recorded Future®

About Recorded Future

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams by informing decisions in real time with contextual, actionable intelligence. By analyzing data from open, dark, and proprietary sources, Recorded Future offers a singular, integration-ready view of threat information, risks to digital brand, vulnerabilities, third-party risk, geopolitical risk, and more.

www.recordedfuture.com