BLACK KITE

EBOOK

What You Need To Reduce Third-Party Risk

Learn how your teams can reduce third-party risk without breaking the budget or introducing additional resource strain

There's a Lot More to Third-party Risk Management Than Meets the Eye

In a survey of executive risk committee members, Gartner found that 84% said third-party breaches interrupted operations across supply chains, and 66% said they caused significantly adverse financial consequences. Many organizations agree that third-party risk incidents are a pressing threat — and yet, third-party risk management (TPRM) "misses" hit organizations hard.

A major source of these "misses" is the fact that traditional third-party risk management (TPRM) programs typically display an overreliance on subjective scores that don't paint a full picture of risk. Unfortunately, risk scores are just the tip of the iceberg, and a codependence on them has led to malicious hackers breaking in.

We all know how well thinking about only the tip of the iceberg went for the Titanic. To effectively reduce third-party risk, security professionals must build their defense strategies from a multi-dimensional view of risk that incorporates compliance, ransomware susceptibility, risk quantification, cyber threat intelligence, and other critical components.

TPRM Is About Processes, Not Platforms

Deloitte reports that only 36% of organizations believe they have a high capability of managing and responding to incidents arising from global supply chain issues — and 21% believe their capability is “low.”

That’s due to the fact that traditional TPRM methods don’t allow for the flexibility that organizations need to address fast-moving and mounting threats. Security teams need to be resilient in today’s digital landscape to withstand, prevent, and adapt to the avalanche of threats that come their way.

When organizations build third-party risk programs around strict prevention of any change, they open themselves up to a greater risk of attack. Security teams need to move through, not against, changes in the threat landscape to mitigate risk in a multitude of scenarios — and that includes scenarios around third-party risk.

It’s time for security teams to adapt to change by reframing their view of risk with the following pillars:

- Cyber risk intelligence.
- Compliance engines.
- Risk quantification.
- Ransomware susceptibility.

Agility Is A Must — Take It From SolarWinds

The SolarWinds breach (and the third-party fallout that followed after it) should have been a major wake-up call to organizations everywhere about the potential reach and impact of third-party incidents in any sector.

This incident demonstrated a clear need for security teams to be agile and readily shift gears when an attack is actively in progress. It also displayed what can happen when organizations don’t have a specific response plan in place for potential incidents, even if they haven’t happened yet.

Make Cyber Risk Intelligence the Bedrock of Your TPRM Program

The bedrock of any TPRM program worth its salt is cyber risk intelligence. Cyber risk intelligence provides organizations with the information they need to make the right critical decisions around security. Additionally, with access to cyber risk intelligence, security teams can identify the vendors that have the potential to hit their organization the hardest should a breach occur — which allows companies to make better third-party risk decisions.

It's critical for organizations to understand the difference between cyber risk intelligence and cyber threat intelligence in this case. Whereas cyber threat intelligence is the act of gathering information on potential threats and threat actors, cyber risk intelligence entails putting that data into the context of each organization's specific needs, goals, and risk appetite to determine the right response.

For security teams to maximize their cyber risk intelligence, they must start off with high-quality data. Some examples of the data that should inform cyber risk intelligence include information from social media sites and hacker forums, news reports on relevant cyber incidents, and activity on the dark web.

However, not all data is made equal. Security professionals must verify that the data they're collecting is both accurate and relevant to their organization's needs by leveraging the right tools and solutions that allow for customization of the controls that determine what information gets flagged. This more targeted approach to information gathering helps improve an organization's true cyber resilience, which in turn reduces third-party risk.

Black Kite FocusTags™

The Black Kite platform comes with FocusTags™, a fast and easy way for organizations to track the high-profile cyber events that matter to them (e.g. ransomware events, Log4j updates, Clop attacks) and identify which critical vendors and partners have been affected.

Compliance Engine

Fines from failing to meet compliance can get pretty hefty. Take Amazon, which is paying out $887 million in GDPR fines for privacy violations. Even if a company internally is crossing its T's and dotting its I's with regulations and standards, it still can be liable for major compliance missteps taken by its third-party vendors and partners.

To reduce third-party risk, organizations need tools equipped with a compliance engine to ensure their third-party vendors, services, and partners are consistently meeting regulatory requirements. A compliance engine is a tool that helps automate and streamline the process of vetting third parties' maintenance of regulatory standards.

When equipped with a compliance engine, a TPRM program can help organizations identify the compliance requirements that are important to them and the vendors that put them at risk of violating them. This can additionally inform what standards are critical to include in any contractual agreements with potential third parties. By establishing compliance expectations up front, companies can avoid the difficult (and usually costly) conversation around liability should any violations occur.

When security teams keep tabs on how well their third-party vendors and partners maintain compliance, they can proactively establish both their expectations for adherence to regulations and mitigate compliance risk.

$887M

GDPR fine that Amazon is paying due to privacy violations

The Black Kite Parser Streamlines Procurement

Immediacy and accuracy are especially important in the procurement process, which often demands speedy — but well-informed — decisions. A compliance engine in a third-party risk management tool can help facilitate the procurement process when it has a strong foundation of AI. That's why we built the Black Kite Parser to automate the collection and contextualization of compliance data based on each organization's unique controls.

As a result, security teams can rest assured that they'll get the compliance data they need, when they need it.

Risk Quantification

Black Kite research shows that 68% of CFOs agree that real-time financial data models are critical in enabling better business decisions. When security teams can quantify risk, they can put a concrete dollar value to the money they might lose in working with a vendor or partner that's likely to get attacked. When decision-makers can see risk in such practical terms, it makes it a lot easier for the whole team to get onboard with the right security strategies.

That's where risk quantification comes in. Organizations need a strong understanding of the probable financial impact of potential incidents to better communicate about risk and make smart, collaborative decisions.

Companies equipped with financial knowledge about risk can identify where they're most vulnerable (AKA — where to allocate their resources) and reduce third-party risk by focusing on the weaknesses that pose the greatest potential fiscal, reputational, or operational damage. Additionally, putting risk into financial terms makes security goals and needs easier for executives to understand, which in turn helps gain fuller company alignment on risk reduction strategies.

How Black Kite Gives Risk A Dollar Value

At Black Kite, we use the Open Fair™ model to calculate the probable financial impact a potential cyber breach would likely have on your organization. We use Open Fair™ because:

- It's transparent, which means security professionals will know exactly how we're getting our numbers.
- It's the only international standard Value at Risk (VaR) model for cybersecurity and operational risk.

68% of CFOs agree that real-time financial data models are critical in enabling better business decisions.

Ransomware Susceptibility Indexing

Ransomware attacks are quickly becoming a bad actor's method of choice. Our 2023 Third-Party Breach report found that ransomware accounted for 27% of all reported third-party incidents. That's over a quarter of third-party breaches stemming from a single mode of attack.

Security teams must leverage strategies and methodologies that help them both identify pressing ransomware risks and vulnerabilities, as well as determine which of their vendors are likely to be successfully targeted with ransomware.

One successful strategy is utilizing an index that measures ransomware susceptibility. This index typically measures and analyzes common indicators of ransomware risk, such as leaked credentials, stealer logs, weak email security, and vulnerabilities with remote code execution. Once analysis is complete, organizations can see in clear, concrete numbers how probable it is that one of their vendors will get hit with ransomware.

When organizations have an index against which to measure ransomware risk, they can more effectively avoid the potential reputational, financial, and productivity fallout that comes with a successful attack.

Vet Your Vendors with RSI™

The Black Kite platform includes a Ransomware Susceptibility Index® (RSI™) that allows for fast and accurate assessment of how likely a particular vendor or partner is to fall victim to a ransomware attack.

In fact, our 2023 Ransomware Threat Landscape Report found that 70% of vendors with confirmed ransomware attacks had an RSI value above the high-risk threshold.

Reduce Third-Party Risk With Cyber Experts

Reducing third-party risk is an ongoing journey. However, it doesn't have to be a journey that security teams embark on alone. Every company in any industry can benefit from the knowledge of dedicated cybersecurity experts who live and breathe navigating the changes of the threat landscape.

At Black Kite, our platform is built on the expertise of seasoned security professionals dedicated to reducing third-party risk and, most importantly, clearly explaining and demonstrating how we're doing it.

With components that account for cyber risk intelligence, compliance, risk quantification, and ransomware susceptibility, our solution helps security teams gain the multi-dimensional view of risk they need to keep bad actors at bay.

NOT YET CONVINCED? SEE THE BLACK KITE DIFFERENCE AND HOW WE MEASURE UP NEXT TO OUR CLOSEST COMPETITORS.

BLACK KITE