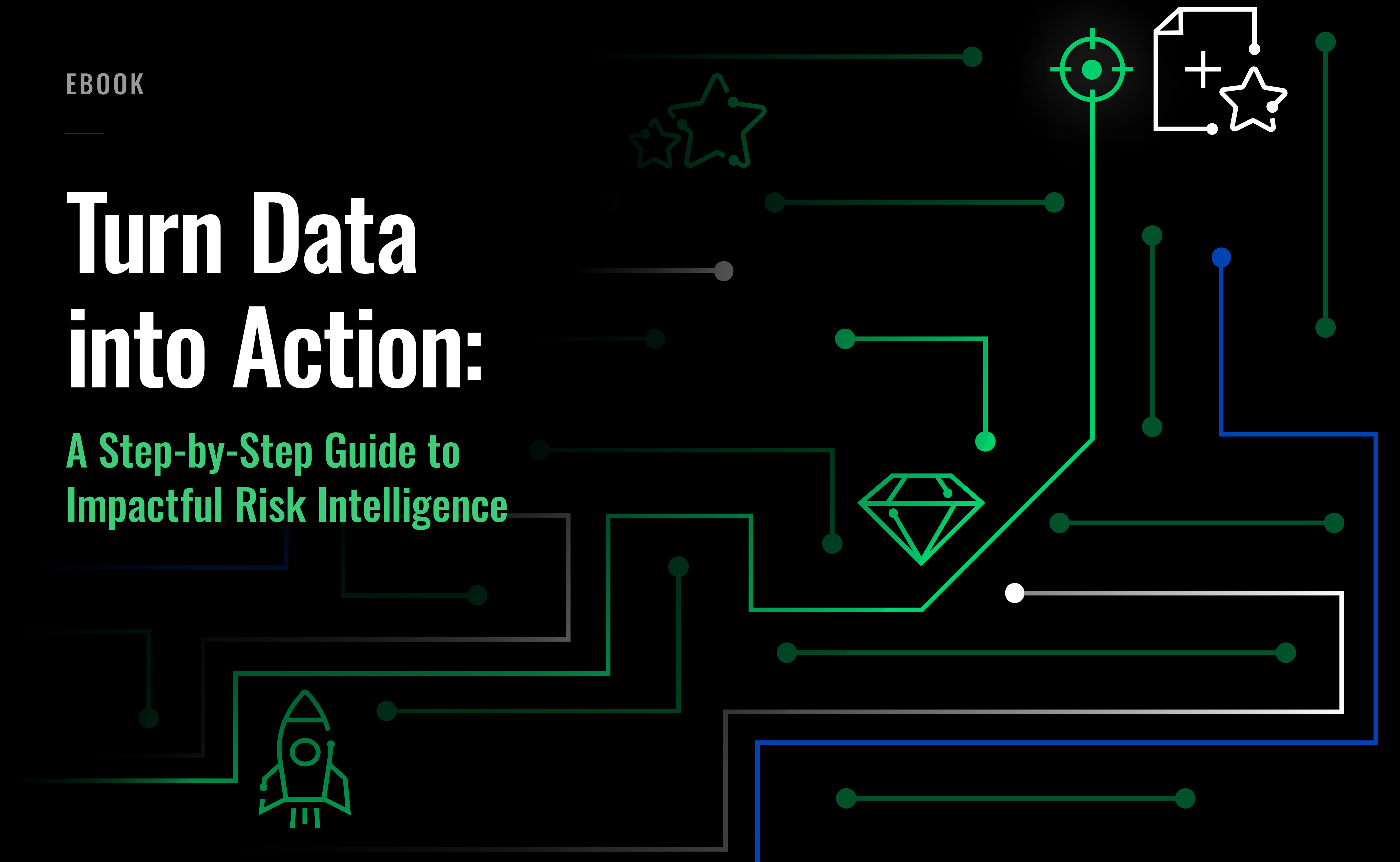
BLACK KITE

EBOOK

Turn Data into Action:

A Step-by-Step Guide to Impactful Risk Intelligence



Level up your cybersecurity strategy and build a more resilient organization with robust risk intelligence.

Many organizations struggle with a lack of visibility into the risks they face, especially those presented by third-party vendors, which leaves them vulnerable to attack. The good news is that with the right tools, security professionals can turn complex risk data into action to more strategically mitigate high-priority risks.

The key? Impactful risk intelligence.

By leveraging cyber risk intelligence, security professionals can gain the clarity they need, develop a data-driven approach to risk management, and, ultimately, safeguard their organization's critical assets.

In this eBook, we'll cover how to:

- Define your objective
- Gather, analyze, and prioritize your risk data
- Identify relevant stakeholders
- Make an action plan

What Is Risk Intelligence?

Risk intelligence is data-based insights that guide your cyber risk management strategy. It provides both a comprehensive and nuanced view of your risk profile, with enough detail to effectively guide prioritization and remediation efforts.

Risk intelligence comes from the collection, contextualization, and analysis of raw risk data, such as:

- Security incident and event management (SIEM) tools
- Vulnerability assessments and/or pentesting reports
- Third-party vendor assessments
- Open-source intelligence (OSINT)
- Industry reports and benchmarks
- Legally mandated data breach reports
- Government agency publications

Benefits of Robust Risk Intelligence

Security professionals who grasp the art of analyzing and using risk intelligence will be better equipped to:

- **Practice data-driven decision-making:** Make decisions around risk prioritization, resource allocation, and risk mitigation strategies with confidence, tracking progress over time, and adjusting strategies.
- **Facilitate communication and collaboration:** Bring stakeholders into the security fold and earn their support by demonstrating the potential impact of risks in cold hard data.
- **Mitigate risks proactively:** Because risk intelligence is predictive, you can identify potential risks before they materialize and take preventative measures.
- **Focus on continuous improvement:** Track the progress of your initiatives, as well as changes in your environment, to continuously refine your organization's protection mechanisms, third-party contract terms, and internal processes.
- **Demonstrate regulatory compliance:** Establish a risk reporting process to easily provide historical risk and control data, ensuring you are ready for any regulatory audit or investigation.

What Risk Intelligence is NOT

Security professionals should be wary of equating risk intelligence with threat intelligence. Threat intelligence is the strategic collection of information on cyber threats and attack methods. This is one vital piece of the risk intel puzzle, but it doesn't offer the analysis and company-specific insights that come with risk intelligence.

It's important to also be aware of the limitations of legacy risk intel tools, like security ratings and manual questionnaires, when seeking risk intel. Security ratings, while helpful for a quick, high-level view of a vendor's risk, don't encompass all the necessary information. Lengthy questionnaires are time consuming, influenced by human bias, and often geared toward compliance. Your cyber ecosystem is evolving too quickly, with new vendors, new threats, and an ever-increasing amount of sensitive data, to rely on these limited methods.

Learn more about the difference between "threat" and "risk" intelligence in this blog.

4 Steps to Using Risk Intelligence Effectively

Impactful risk intelligence is generated through an iterative process of gathering, analyzing, and prioritizing your risk data. This process is different at every organization, but the foundation is the same. Here is a four-step process that will help optimize the way you use risk intelligence.

Step 1: Define Your Objective

Define a clear objective to give your team the focus it needs when collecting and analyzing risk data. In this way, you can ensure that your risk intelligence provides only the insights most relevant to your organization's current needs.

Maybe your primary goal is risk reduction or speeding up the procurement process. This will inform what data you gather, who you involve in remediation efforts, and more. Collecting data without a specific objective in mind makes it difficult to cut through the noise of the threat landscape and identify (and prioritize) the risks that really matter to your business.

For example:

- If you work at **a hospital**, avoiding business disruption may be one of your top priorities, so understanding ransomware susceptibility in your supply chain would be very important.
- As a **finance organization** protecting customer PII and financial data is of the utmost importance. So, understanding how a breach in your supply chain could cascade to you, the potential financial impact, and any history of breaches from the Data Breach Index (DBI) may be what you are most interested in.
- If you are in a **highly regulated industry**, you may need to investigate whether your suppliers meet your internal and industry compliance standards.

The Cascading Effects of Third-Party Breaches

It's not enough to look at direct threats to your company alone. You must also be aware of the cascading impacts of security threats throughout your cyber ecosystem, including your third-party vendors.

In Black Kite's Third-Party Breach Report 2024, we explored 81 third-party breaches from 2023. Those 81 data breaches impacted 251 companies downstream, for an average of 3.1 victims per breach.

Step 2: Gather, Analyze, and Prioritize Your Risk Data

To identify real and urgent threats to your business, you need to identify the signal through the noise. You must gather risk data, analyze it within the context of your business, and prioritize the most pressing risks to inform your cybersecurity strategy.

ADD CONTEXT TO YOUR RISK DATA

Start by tapping into the sea of data available from internal and external sources. Sift through it to find what is most relevant to your business and remove generalized, incomplete, or irrelevant insights.

The goal is to reduce distractions and create a laser-focused, yet nuanced view of your risk. This allows you to approach the other steps in this process more strategically, keeping your objective in mind at each stage.

Here are some contextual considerations you should keep in mind while sifting through your risk data:

- **Industry-specific factors,** like regulations, standards, and common threats.
- Your **third-party vendors' history** of and **current susceptibility** to attack.
- What **type of sensitive data** your business is using and/or storing.

Weigh the Risks

For example, say the vendor who delivers your office supplies is flagged as having a newly discovered vulnerability. After you review this vendor in context of your business, including what data they have access to and whether you have concentration risk, you discover that they a) Don't have access to your internal systems or data, as you work with another office supplier and b) Do not pose concentration risk. Understanding the full picture of the risk this vendor poses to your business specifically allows you to deprioritize this risk and focus your energies elsewhere.

PRIORITIZE THE RISKS TO YOUR BUSINESS

Once you have an idea of which threats are circling, it's time to figure out which risks are most urgent and likely to evolve into a breach if not mitigated. It's nearly impossible to tackle all of them at once.

First, analyze how each risk interacts with your data, processes, and security measures to pinpoint the highest-priority threats. This analysis might require correlating data across pen-testing results, vulnerability assessments, data from your security incident and event management (SIEM) tool, threat actor analysis, and so on.

The likelihood of an attack and the potential financial impact of that attack are key factors in determining your priorities. Look for the following to pinpoint your highest priority threats — or those that you should take action to mitigate right away:

- There's a clear and present danger to your company.
- A risk poses a significant financial impact to your business.
- A new or evolving risk — such as a vendor whose ransomware susceptibility has recently increased significantly — that requires a closer look.
- A potential vendor needs to be quickly assessed to understand what level of risk they might present to the business before the contract is signed.

Once you've identified your highest priority risks, investigate:

- What has changed to cause this increased risk?
- What sensitive data (if any) this vendor has access to?
- What protections are currently in place to safeguard that data?
- What would the potential cost be to the business?

Step 3: Identify Relevant Stakeholders

It's likely that your risk mitigation strategies will impact resource allocation, processes, technology, vendor agreements, and more. You must take into account overarching business goals, competing priorities, potential operational disruptions, available funds, and more.

To fully understand the potential impact of a risk and also the potential impact of your action steps, you must connect with relevant stakeholders. Effective communication and collaboration with internal and external stakeholders are crucial for turning your risk intelligence into action.

COMMUNICATING WITH INTERNAL STAKEHOLDERS

Internal stakeholders are very invested in your cybersecurity success, but they have KPIs to hit and are being held accountable for business critical initiatives, just like your security team. They also have first-hand knowledge of how an at-risk vendor is being used and what data or systems it might have access to. Collaboration with these stakeholders is key for information gathering, weighing next steps, and executing them.

Internal stakeholders you may collaborate with include:

- **Executives and board members:** These stakeholders have the power to determine the business's highest priorities. If you want them to release funds or send reinforcements, you'll have to present a compelling argument with extra emphasis on the cyber threat's potential financial impact.
- **Internal business unit owners:** This colleague heads up the department that's using the tool or software that is exposing the business to risk. It's highly likely that mitigation efforts will disrupt their operations, so ensure they understand how the risk could impact their day-to-day work.

Even Industry Leaders Have Blind Spots

A well-known, multinational bank reportedly spends $1 billion per year on cybersecurity, yet it recently suffered an attack that exposed around 57,000 customers had their sensitive data — including social security numbers, bank account numbers, and more.

Previously, the financial institution also suffered another attack that exposed over 30,000 customers' sensitive data.

How is this possible?

In both cases, it wasn't the bank itself but rather a third-party vendor that fell prey to an attack, allowing threat actors to access data in the bank's ecosystem. This emphasizes the need for more robust risk intelligence processes, especially in the third-party risk management space.

COLLABORATING WITH EXTERNAL STAKEHOLDERS

If you're unable to mitigate or transfer risk to an acceptable level with internal resources alone, it's time to involve external parties (although this should be a last resort). Similar to the internal stakeholders, these organizations will have limited resources and many competing priorities, so you'll have to demonstrate why they should care.

At-risk third-party vendors: These vendors need to know what is at stake for them. Are they at risk for a damaging attack due to a vulnerability they simply haven't spotted yet? Will they lose your business — and potentially other clients — if they choose not to cooperate?

TIPS FOR COMMUNICATING RISK INTELLIGENCE WITH STAKEHOLDERS

While security professionals are expert data analysts, translating complex risk insights into practical guidance for non-security audiences requires a different skill set.

These communication strategies will be essential:

- **Audience Awareness:** Understand your stakeholders' priorities and tailor your message accordingly. This includes using jargon-free language and anticipating potential concerns.
- **Impact Quantification:** Don't use generalized or dramatic language. Instead, quantify the potential impact of inaction, including financial impact, reputational damage, or operational disruptions — all framed within the context of their specific goals.
- **Data Visualization:** Your audience doesn't need to know everything that you know. Provide clear, concise visuals, like graphs or charts, that demonstrate the validity of your conclusions.
- **Practical Guidance:** In addition to highlighting the problem, you also want to provide solutions. Empower stakeholders by sharing specific suggestions for mitigating the risks you've identified.
- **Reasonable Timelines:** Work with stakeholders to establish a realistic timeline for remediation efforts. Consider the risk severity, required resources, and stakeholders' existing workload to find a mutually agreeable time frame.
- **Encourage Collaboration:** Clear communication and open discussion is key to creating and executing on a cohesive risk mitigation strategy.

It's Only a Matter of Time

According to Gartner, nearly half of all organizations will face a cyberattack on their software supply chain by 2025.

Step 4: Make an Action Plan

The next step is to explore mitigation strategies and their potential financial cost. With these findings, you can make a data-driven decision to accept, transfer, or reduce the level of risk. Focus your resources on the highest risk vendors first, and develop a practical third-party risk program. Your action steps might include:

Strengthening internal IT security controls.

Improving your vendor onboarding process, paying special attention to the risk new vendors could present to your business.

Allocating more resources toward security audits and penetration testing for high-risk vendors.

Negotiating more robust contractual terms regarding data security and breach notification.

Seeking a redundant solution to serve as back-up to a mission-critical vendor that's presenting a significant risk.

Make Cyber Risk Intelligence Scalable with Black Kite

Black Kite's risk intelligence platform puts real-time risk intelligence at your fingertips, illuminating potential risks in your cyber ecosystem, assigning priority levels, and providing remediation guidance. Our tool also calculates each risk's potential financial impact, ensuring you know which risks present the greatest danger to your business.

Black Kite's FocusTags™ make this process more scalable by automatically highlighting vendors affected by a high-profile cyber event. They can also be customized to help you filter your vendor ecosystem, highlighting vendors who have access to critical systems or sensitive data, for example.

To round out this comprehensive view of your cyber ecosystem, Black Kite also provides automated compliance assessments and a Ransomware Susceptibility Index®. With these tools, you'll have visibility into any changes in your vendors' compliance level, as well as their susceptibility to falling victim to a ransomware attack.

"Utilizing Black Kite, we can get an **instantaneous overarching view of our third-party vendors** and their security posture. It really speeds up the process of assessing vendor risk for sure. Also, being able to identify new weaknesses that pop up on the fly is extremely helpful in **keeping patient data safe.**"

– Cybersecurity Analyst at [University of Kansas Health System]

"I was able to demonstrate and show the VP of IT that Black Kite was the only platform offering both a **Ransomware Susceptibility Index™** and **quantified risk amount with FAIR™**, setting Black Kite far apart from the competition."

– Director of Information Security at [Scantron]

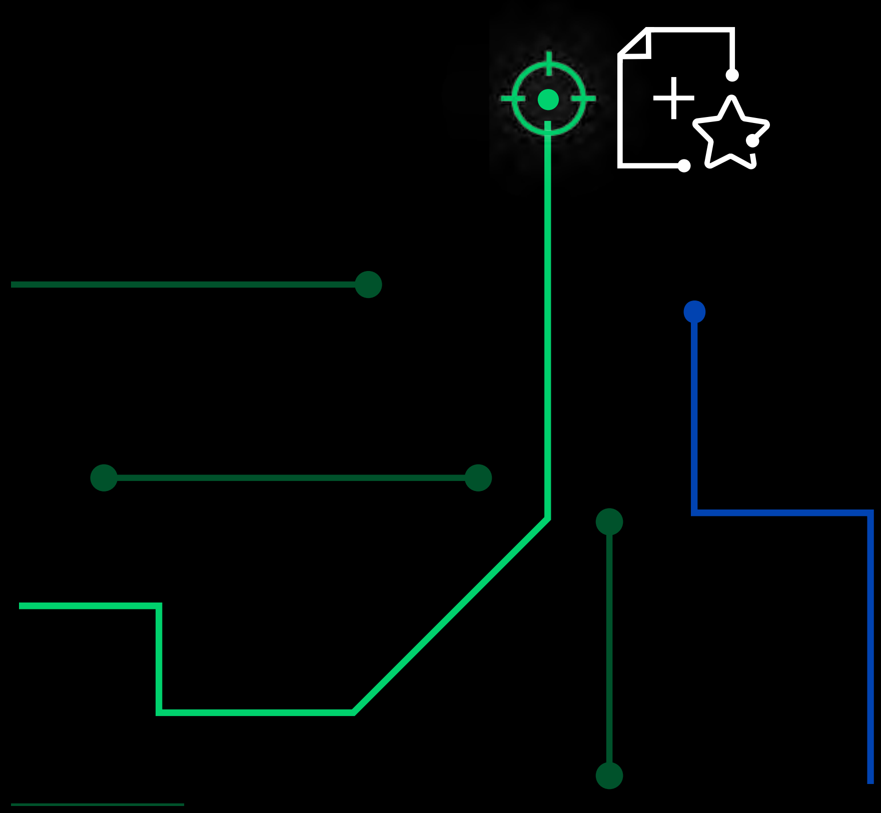
Talk to a Black Kite cybersecurity expert today about establishing your own risk intelligence process before a breach in your supply chain impacts your organization.

BLACK KITE

Put the Partnership in Third-Party Risk Management

When devising approaches to working with third parties to mitigate risk from high-profile cyber events, it can be helpful for security teams to implement a little game theory: What's best for each organization security-wise is likely mutually beneficial across the cyber ecosystem. Security teams should look at communicating with vendors about risk as an opportunity to build upon a partnership — not a trap leading to a charged conversation.

When security teams know what high-profile events matter to them, can efficiently identify their affected vendors, and get straight to the point with compassion and empathy, they open up a new world of vendor communications that plays an essential role in significantly reducing risk.



OUR SOLUTIONS HAVE THE POWER TO TRANSFORM BOTH YOUR SECURITY PROFILE AND YOUR VENDOR RELATIONSHIPS. **GET IN TOUCH** WITH US TO LEARN MORE.

BLACK KITE