BLACK KITE

EBOOK

Keep Calm and Collaborate:

How To Approach Vendors During High-Profile Security Events

Get the Info You Need — Without Burning Any Bridges

Nobody likes to be told that they're doing something wrong. Unfortunately, that's the message a lot of vendor security teams receive when their partners reach out about high-profile security events. At the same time, security teams can feel ghosted by vendors when they reach out about security concerns following a high profile incident.

However, the usual radio silence or touchiness are not personal failings on either side. Feelings of defensiveness or frustration are a symptom of a greater disease plaguing fast incident response to high-profile security events.

That disease would be poor communication.

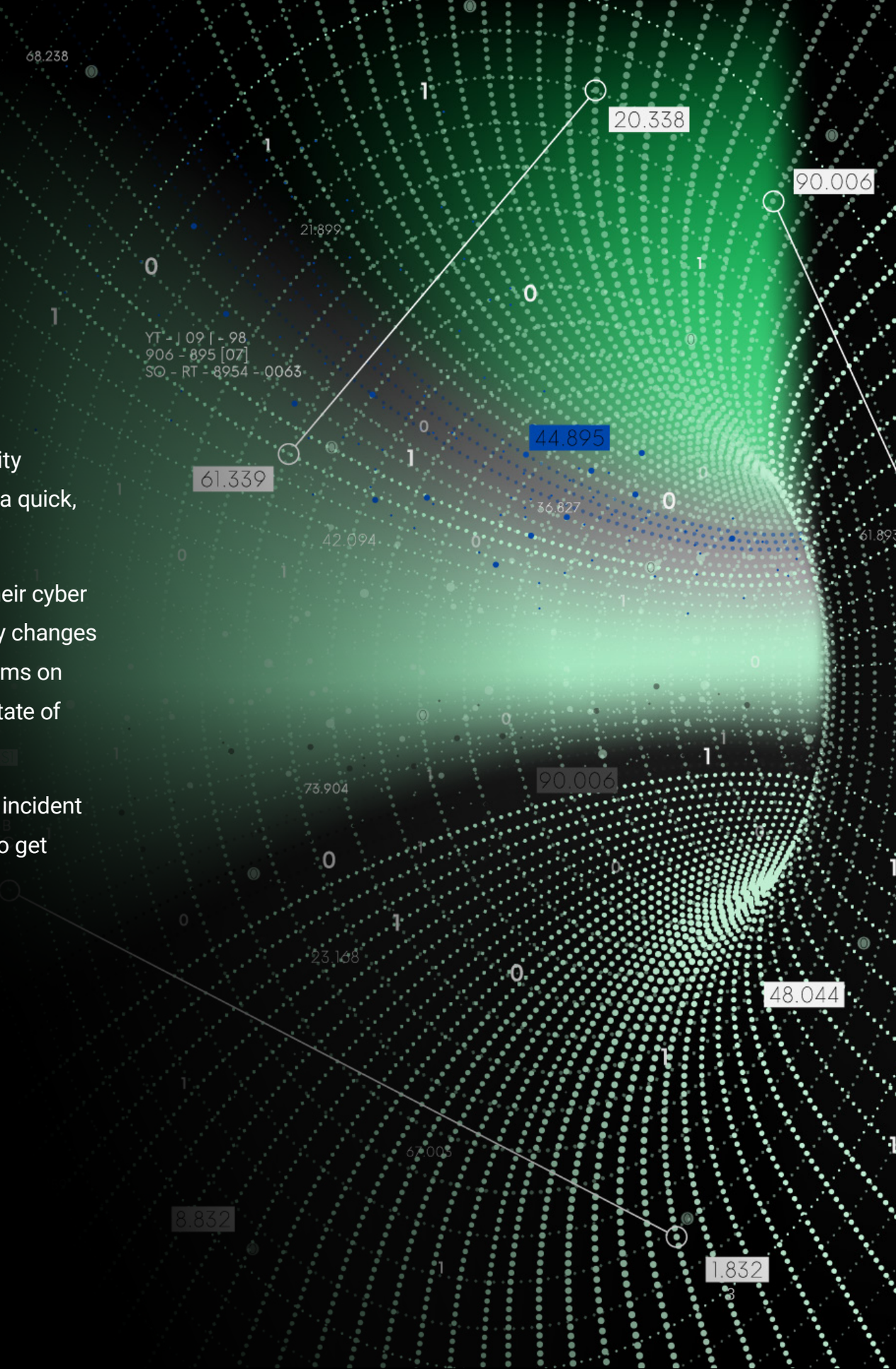
Intentional, collaborative, and empathetic communication is the key to effectively working with your vendors in the wake of a high-profile security event. Through more conscientious communication strategies that treat vendors as partners rather than liabilities, organizations can more successfully mitigate the effects of these events within their ecosystem.

The Real Problem With Current Approaches to Vendor Communications

The biggest challenge security teams face in the wake of a high-profile security event is gathering the risk intelligence and information needed to implement a quick, comprehensive incident response plan.

For example, many security teams have a tendency to approach vendors in their cyber ecosystem, demanding that these third parties make specific internal security changes to suit their concerns as soon as possible. Unfortunately, this puts vendor teams on the defensive and does not account for nuances in their bandwidth, current state of resources, and specific security strategies.

That's why a strong and collaborative communication strategy is essential to incident response: It helps build up the relationships and rapport organizations need to get information from their vendors in a timely manner.



Black Kite – Keep Calm and Collaborate: How To Approach Vendors During High-Profile Security Events

THIS COMMUNICATION STRATEGY SHOULD CONSIST OF:

Defining what high-profile security events are relevant to your organization.

Identifying the right vendor security personnel.

Prioritizing affected vendors.

Sharing clear, concise requests.

Establishing an ethos of partnership and collaboration.

When security professionals establish a robust incident response process that incorporates the aforementioned steps, they increase their chances of effectively monitoring and mitigating the blowback of high-profile cyber events on their critical servers, data, and systems.

Step One:

Identify Relevant High-Profile Security Events

First and foremost, organizations must define for themselves what constitutes a relevant high-profile security event. While high-profile security events by definition have a widespread impact, every single event won't affect or pose a risk to every single organization.

Defining what constitutes a relevant high-profile security event can both save security teams time and resources — as well as preserve vendor relationships. Alert fatigue is a major reason why risks around high-profile security events never get addressed (or get addressed too late).

As such, security teams should take measures to identify and focus on their critical processes, systems, and vendor relationships that must be protected to ensure productivity, security, and performance. Organizations should identify the critical points of their cyber ecosystem and create appropriate risk scenarios that establish what types of high-profile security events could pose a threat to their systems.

Your teams should only move forward with vendor outreach if the high-profile security event in question impacts your risk profile — rather than reaching out to all vendors for every single blip on the radar. This approach can help you maintain good standing with your vendors, as they also likely face the challenge of cutting through the noise to address only relevant customer concerns.

What Is a High-Profile Security Event, Anyway?

Our experts define high-profile security events as cybersecurity incidents that create a ripple effect across industries — typically those that make news headlines and dominate security conversations post-boom.

These are the major breaches, leaks, vulnerabilities, and threats all organizations must pay attention to and assess for potential risks. Think **Okta**, **Target**, **SolarWinds**, and the **Colonial Pipeline** breach.

Step Two:

Find the Right Vendor Security Contact

More often than not, an organization's main point of contact with a vendor or third party will be a sales, product, or customer service representative. These are not the people that security teams should reach out to regarding high-profile security events, as these contacts will likely not have the information or capabilities security teams need.

As such, security teams need to identify other security personnel working for their critical vendors and create effective communication pathways with them. Reach out to sales teams or other relevant vendor representatives ahead of time to schedule an intro (and build a working relationship) with these security contacts.

The more history you build with them, the more likely they will respond to your requests for information when you need it. The best way to build that history is to proactively initiate conversations around communication processes during contract negotiations. Better yet, organizations can even make clear security contacts a requirement within contracts.

Once organizations identify their vendors' appropriate security personnel, they should establish clear communication channels and processes in anticipation of any need to communicate about security incidents or events. These processes should designate clear security contacts, establish what secure communication platforms contacts will use, and set expectations for communication frequency, response times, and escalation procedures.

Step Three:

Confirm that Contacting a Vendor Is Appropriate

Your security team's goal should be to only reach out to vendors when you feel confident that you can work together to improve your company's security. Reaching out to a vendor when something is out of their power to fix will only cause unnecessary tension and potentially sour a good working relationship. **Before contacting a vendor in the wake of a high-profile security event, be sure your team asks the following questions:**

1. **Is this vendor critical to my operations? Do we share sensitive data with them that could result in business disruption or reputational harm if breached?**
2. **Is my vendor actually using the software, tools, or services that were impacted by this high-profile security event?**
3. **Do I know if my vendor has already taken steps to remediate the issue? Or am I making an assumption?**
4. **Do I have access to enough data to ensure what we're asking for is clear?**
5. **Are my requests reasonable and within my vendor's power to enact?**

Asking these questions prior to engaging with vendors can ultimately save all parties a lot of time and effort — as well as mitigate the potential emotional strain of having tough conversations.

Contacting a vendor should be a last resort. Take time to prepare your teams with all the critical data and risk intelligence you need before reaching out — it can go a long way in maintaining a respectful working relationship.

Step Four:

Reach Out to Vendors with Clear, Concise Requests

When organizations reach out to vendors to follow up on the impact of a high-profile security event, it's not enough to simply send a broad list of questions and expect to get impactful information. The key to working with vendors quickly and effectively is to be clear, concise, and specific.

First, your security teams should emphasize to vendors why you're reaching out now. If you're reaching out due to a potential ransomware susceptibility increase, it's best to come right out and say exactly that. If you're reaching out about a possible vulnerability, be as specific as possible about which vulnerability and in what software. Share the susceptible asset so it's not a wild goose chase.

Next, ensure that your outreach clearly outlines a collaborative approach to mitigating the security issue at hand. If your vendors need to remediate a vulnerability, offer them a chance to connect with your security teams to discuss what steps to take.

Engaging in a collaborative back and forth on how to resolve issues caused by the high-profile security event helps preserve and strengthen the relationship with your third parties while jump-starting actionable steps towards remediation.

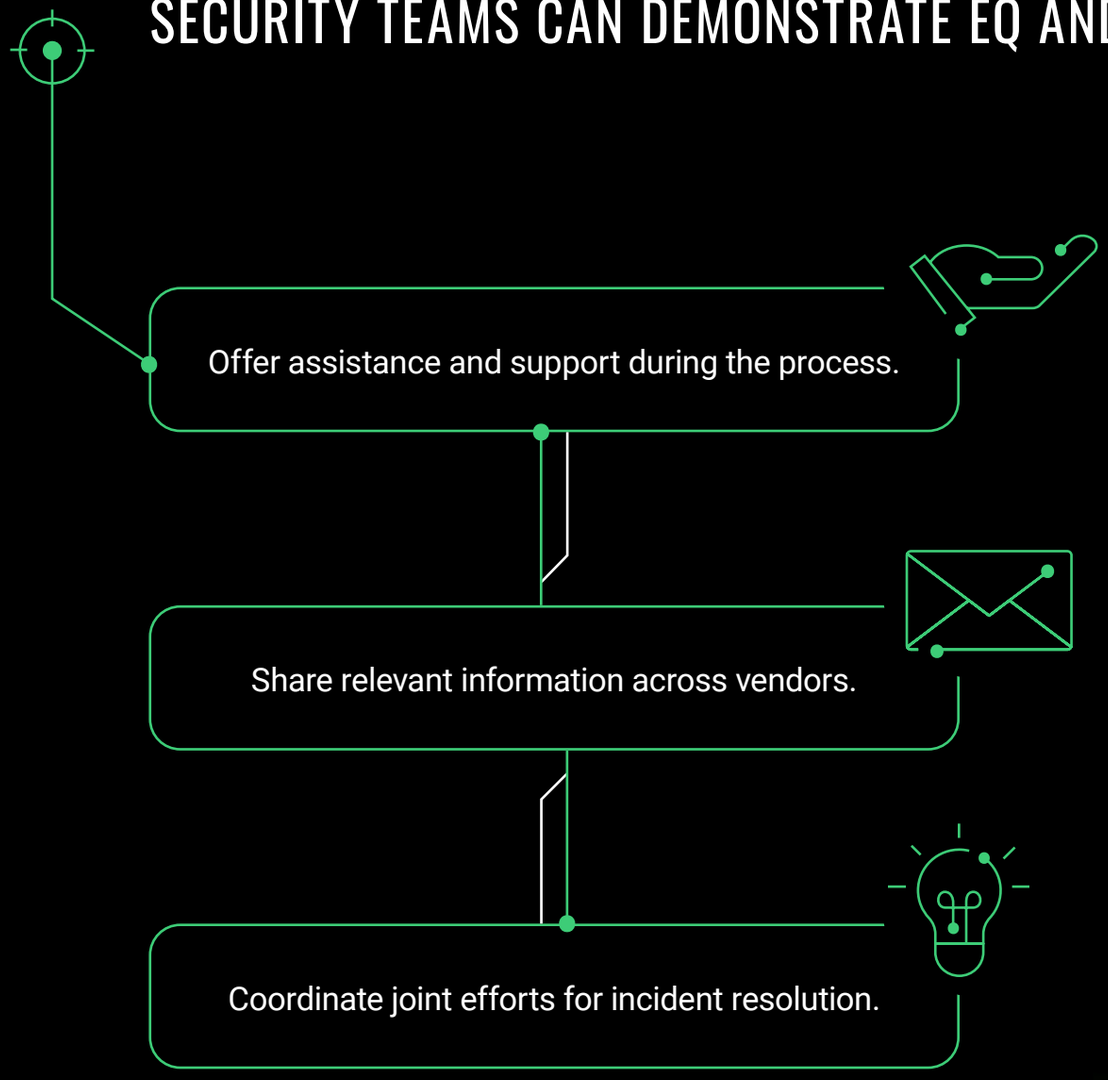
Step Five:

Establish an Approach of Partnership and Collaboration

It's critical for security teams to consider the emotional quotient (EQ) when they reach out to their vendors, even with hyper-specific questions. Even the most strategic communication styles can fall flat if they fail to consider EQ. Furthermore, partnering with vendors on incident response requires team members who are capable of staying aware of the human element at play here — which helps prevent burned bridges.

Here's what we mean by EQ: Lead with compassion so your vendors don't feel like they're being attacked when they're asked about their cybersecurity posture around high-profile security events. As such, your communication plan should be built on a firm understanding of compassion, curiosity, and collaboration when it comes to each incident.

SECURITY TEAMS CAN DEMONSTRATE EQ AND BUILD TRUST WITH VENDORS BY:



Additionally, organizations should regularly perform healthy reassessments on who from their security teams should take charge when reaching out to vendors. This person should have a strong EQ and naturally approach difficult situations and conversations with a foundation of compassion, empathy, and understanding — all while being a problem-solver.

At the end of the day, no one wants to be the victim of a high-profile security event. That's why it's essential for security teams to recognize and acknowledge their vendors' existing security efforts while working together to address any new risks or concerns. Avoid assuming the worst. Depending on each vendor's size and budget, they may have considerable resource challenges and limitations when responding to security incidents.

How FocusTags™ Facilitate More Effective Vendor Relationships

Black Kite FocusTags™ are a fast and simple way to quickly identify vendors in your supply chain affected by high-profile security events. Simply customize and define your security controls to hone in on the incidents that materially affect your organization — and introduce your teams to major savings on time, money, and resources.

FocusTags™ leverage the power of AI and automation to empower security teams with the knowledge they need to effectively communicate with vendors. With FocusTags™, your teams will have access to:

- Automated continuous monitoring. Automated monitoring systems can significantly enhance the efficiency and effectiveness of vendor risk management. These systems can continuously monitor critical vendors for indications of risk within their environments.
- Real-time alerts. Automated alerts help ensure security teams are promptly notified of any suspicious or concerning activities detected within the vendor's infrastructure — and only those that materially have an impact. This allows for rapid incident response, reducing third-party risk.

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.