WHITE PAPER

BlueVoyant®

Best Practices to Assess and Mitigate Third-Party Cyber Risk

"Criminals do not stand still when it comes to trying to exploit computer systems... it's their day job to do this."

– JIM BIEDA, SENIOR ADVISOR, BLUEVOYANT

Introduction

With more than 63% of breaches today caused by third-parties, organizations are starting to realize the need to gain a better understanding of how effectively their business is managing third-party risk.

The current average cost of a data breach is $3.92 million, and with third-party breaches, that number can climb substantially beyond the usual financial, regulatory, and reputational damage.

These days, it's just as critical to know what outside risks are affecting your organization —and the best ways to manage those risks—to ensure your most valuable assets are protected.

Traditional security defenses are designed to protect assets that exist within your network—whether at the network edge or within the server and on the endpoint. Unfortunately, sometimes even the most advanced defenses deployed to protect your data might not be enough to keep you safe. You also need to protect your valuable assets from intrusions that extend beyond your perimeter, including your supply chain.

Organizations increasingly rely on vendors and partners to conduct business every day, often granting third-parties direct network access that connects them to sensitive areas of their business. This opens up an entire spectrum of risks that you can't directly control. In short, the overall security of your data and systems is dependent on the security controls put in place by your vendors. Do you understand what controls are in place to protect unauthorized access to your network? How confident are you that they deploy the same level of security defenses that are in place on your own network?

It's important to understand and ensure your data is protected. But where should you begin?

Understanding Your Security Posture

Organizations should start with understanding their own defenses to gain a better understanding of the risks and vulnerabilities associated with their business. Having a strong security posture in place not only means that your network is protected with the right defenses, but it also ensures you have an effective plan in place to respond. This plan should also include identifying and mitigating third-party security risks.

TO GET THINGS STARTED, YOU SHOULD:

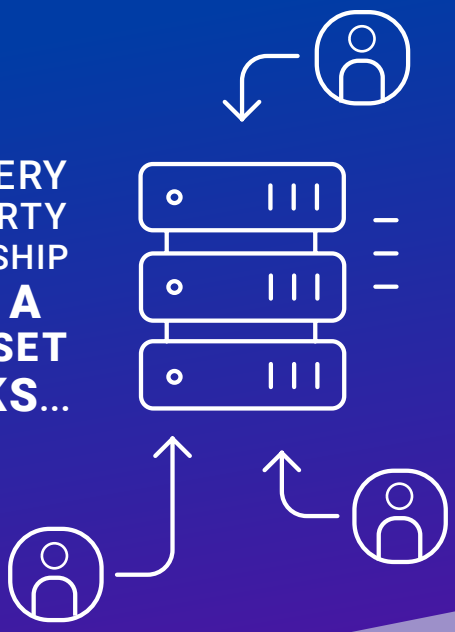
Establish a Baseline: What are the most valuable assets that need protecting? Who has access to that data? Understanding the assets that need to be protected are key.

Identify Risks: Highlight the areas in your network that are most vulnerable to attack to ensure sensitive data cannot be accessed. Ensure your most valuable assets are protected to limit the risks.

Respond Effectively: Minimize the damage and reduce response time by ensuring you have the right incident response plan in place.

Once you understand the strength of your own security defenses, you can begin to focus on understanding the cyber risks associated with your vendors and implement the most effective ways to help mitigate those risks.

WITH EVERY THIRD-PARTY RELATIONSHIP COMES A UNIQUE SET OF RISKS...



Effectively Identifying Vendor Security Risks

Collaboration is one of the key components of any effective vendor risk management program. According to a recent study by Gartner, the compliance and legal departments are typically the primary owners of third-party risk management, but many other functions have a stake in improving risk management and business outcomes, including security teams. Senior leaders and boards are under enormous pressure to gain a better understanding of and managing cybersecurity risk.

With every third-party relationship comes a unique set of risks with which organizations are challenged to effectively respond. Unfortunately, the siloed nature of risk management, especially in larger organizations, can lead to inconsistent application of set standards and validation methodologies that can be ineffective.

Organizations need to take a collaborative approach to more readily and accurately identify and manage outside risks created through third-party relationships.

The Changing Landscape

Vendors have more direct access to organizational data than ever before. Chances are, they're also working with their own third-parties, which increases the size and complexity of identifying and managing cyber risks.

Most organizations use a point in time approach to managing vendor risk, relying on questionnaires as they perform due diligence or recertification on third-parties.

In fact, in a recent report, Gartner states that only 27% of organizational resources are dedicated to ongoing monitoring efforts of third-party risk.

Gartner's research also states that to improve the identification and monitoring of third-party risk, leaders should take an iterative approach, and we at BlueVoyant agree.

By continuing to understand threats outside your organization, along with your monitoring your vendors' security posture, you're able to quickly identify the most critical risks targeting your organization in real-time and work directly with your vendor to resolve and remediate those issues.

According to Gartner's research, to improve the identification and monitoring of third-party risk, leaders should take an iterative approach.

Make an Impact with Your Approach

Organizations need to establish internal guidelines to effectively implement an iterative, continuous approach and overcome the associated challenges. To achieve the desired results and make an impact, organizations should:

STEP #1: ASSESS

When you looked at your security posture, you most likely were able to understand what makes your organization attractive to attacks. Now, apply those same questions to your third-party environment. What information do you collect and store? What data is most valuable? Where is it stored and who has access to that data? How is it protected?

Assessing the level of security in place and how your most valuable data is protected can help you gain a better understanding of where your most vulnerable areas lie. You can then begin to assess your vendors and identify which ones have access to that data and dive deeper into their security posture to gain an understanding of how safe your data is.

STEP #2: RANK

Attackers don't stand still when it comes to trying to exploit computer systems or gain access into an organization's data and information. You shouldn't either. By keeping up to date with the threat landscape, you'll gain an understanding of the latest trends in attacks and the different levels of severity and impacts they can have on your company.

By continuously monitoring the security posture of your vendors, you'll understand which ones are doing a good job of protecting themselves and your data, enabling you to effectively prioritize third-party risks based on ratings and severity.

STEP #3: MONITOR

It's important to understand risks in real-time, for yourself and all of your vendors. Utilize monitoring tools to understand the latest cyber risks in your environment and pinpoint where your vulnerabilities are. Implementing real-time threat detection and response capabilities can also help to identify fraud attempts and other malicious activities originating from third-parties.

STEP #4: ENFORCE

Ensure your security control standards are enforced across your entire ecosystem. Set security level baselines that all vendors must meet and work directly with them to ensure those levels are met. By understanding the performance and service-level metrics for each third-party product and service, you'll be able to ensure that each engagement is being delivered in accordance with your expected level of security.

STEP #5: RESPOND

Once you understand the potential areas that could be targeted, you can prioritize how to resolve the weakest areas in your supply chain and put together a response plan in case of a breach. Work directly with your vendors to remediate risks quickly and effectively. By taking a collaborative approach, you're not only able to better manage risk for yourself, but your vendor as well

Managing Cyber Risk with BlueVoyant

Managing third-party security risks is not easy. **Attackers are increasingly targeting smaller businesses to gain access to larger organizations.** As organizations put more resources into security and breach prevention, it's critical that your suppliers are protecting your data in a safe, well-controlled environment.

BlueVoyant 3rd Party Cyber Risk Services help protect organizations by identifying, assessing, and remediating security risks posed by third-party relationships. BlueVoyant utilizes our powerful, proprietary datasets to expertly identify and measure third-party risk, integrating people, processes, and technology to tailor solutions to an organization's needs.

BLUEVOYANT 3RD PARTY CYBER RISK SERVICES INCLUDE:

3rd Party Cyber Risk Services for Vendor & Supply Chains

Managed risk service that helps organizations proactively identify and remediate third-party security risks by continuously monitoring vendor security posture to help reduce exposure to outside security risk.

3rd Party Cyber Risk Services for Investors

Helps identify and mitigate cybersecurity issues throughout the investment process, enabling investors to assess, quantify and remediate cyber risks associated with a potential transaction or an investment portfolio.

"Risk changes over time, attacks change over time, and we'll see that because we're actively operating defenses for people and investigating what seems to be nefarious activity all the time. What we learn through our managed security services and threat intelligence translates immediately into BlueVoyant risk services."

– JIM BIEDA, SENIOR ADVISOR, BLUEVOYANT

About BlueVoyant

BlueVoyant is an expert-driven cybersecurity services company whose mission is to proactively defend organizations of all sizes against today's constant, sophisticated attackers and advanced threats.

Led by CEO Jim Rosenthal, BlueVoyant's highly skilled team includes former government cyber officials with extensive frontline experience in responding to advanced cyber threats on behalf of the National Security Agency, Federal Bureau of Investigation, Unit 8200 and GCHQ, together with private sector experts. BlueVoyant services utilize large real-time datasets with industry-leading analytics and technologies.

Founded in 2017 by Fortune 500 executives and former Government cyber officials and headquartered in New York City, BlueVoyant has offices in Maryland, Tel Aviv, San Francisco, London, and Latin America.

BlueVoyant®

To learn more about BlueVoyant, please visit our website at **www.bluevoyant.com** or email us at **contact@bluevoyant.com**