BEST PRACTICES

Managing Cyber Risk

Organizations Need to Take a Continuous Approach to Managing Cyber Risk

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 are dependent upon the security controls put in place by you 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?

Best Practices to Assess and Mitigate Cyber Risk

1. Assess
Determine extent of your third-party ecosystem

2. Rank
Identify most critical vendors

3. Monitor
Continuously monitor key risk factors to assess risk tolerances

4. Enforce
Ensure security controls are maintained

5. Respond
Develop a response plan to remediate quickly and effectively

1. Assess

Assess the level of security you have in place to determine how your valuable data is protected and who has access to gain a better understanding of where your most vulnerable areas lie.

2. Rank

Determine which vendors have access to that data and are the most critical to your business to dive deeper into their security posture to gain an understanding of how safe your data is.

3. Monitor

Utilize real-time threat detection and continuous monitoring tools to understand the latest cyber risks in your environment to pinpoint where your vulnerabilities are and identify malicious activities originating from third-parties.

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.

5. Respond

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 risk 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. Find out how BlueVoyant Cyber Risk Management Services can help.

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**