The Risk of Doing it Yourself

DIY vs Managed Cyber Risk Service

KEY POINTS

- Time to Value
- Service Execution
- Knowledge and Expertise
- Scalability

An increasing reliance on third parties to perform a variety of operational business functions has generated a growing demand for business leaders to understand the external risks and security postures of every vendor they engage for business. A majority of critical and non-critical vendors have direct access to sensitive data. Cybersecurity is no longer limited to monitoring internal security posture, it now incorporates the need for understanding and addressing the cyber risk posture of the supply chain and future business partners.

Traditional approaches to managed risk utilize security questionnaires, on-site reviews, information from attestations, and certifications for assessments. These all have resource review limitations, especially when hundreds or even thousands of vendors are involved.

According to Gartner, 73% of efforts devoted to risk identification are allocated to due diligence and recertification efforts with only 27% of effort reserved for identifying risks over the course of the relationship.

Typically, this limit of risk identification can be attributed to a lack of resources and expertise to consistently monitor vendor relationships. To manage resources effectively, some organizations opt to monitor top vendors only, relying on one-time questionnaires and recertifications to vet the rest of their ecosystem. The drawback to this approach is that their top vendors are the most likely to have protection in place, whereas the lower vendors represent the real risks.

Senior leaders and boards are under enormous pressure to gain a better understanding of cyber risk and how to manage it. To make things more manageable, some organizations leverage security rating solutions to provide continuous, real-time scoring for internal assessments, procurements, partnerships, and M&A activities. While effective, these solutions can cause information overload and make risk professionals feel more like data analysts than proactive risk mitigators.

Each third party relationship comes with a unique set of risks. Those unique risks pose new challenges that organizations must manage and effectively resolve. A continuous, iterative approach is needed to fully protect businesses from third-party risk. Risk management leaders must weigh the cost/benefit ratio of building, staffing, and managing their own program, or partnering with a managed risk service provider, like BlueVoyant.

Can you *effectively* DIY, or should you engage a managed cyber risk service?

Here are four elements to consider before making the choice to do it yourself or outsource.

- **Time to Value:** Is there an immediate need? How soon can you be monitoring vendors?
- **Service Execution:** Do you have the resources and systems in place to onboard, assess, and continuously monitor?
- **Knowledge and Expertise:** Do you possess the resources and expertise to triage? How will you retain that talent in-house?
- **Scalability:** Can you protect and grow along with your business's needs?

Time to Value

CSO Online found that over 94% of executives had low to moderate confidence in their third-party risk management tools and software. Current approaches are typically subjective, labor intensive, and only offer point-in-time insight. This snapshot view can either help or hurt your chances of getting the funding needed to build it in-house.

To DIY, begin by conducting a review of your existing processes. Once you identify your problem areas, start to develop a plan to improve upon your existing program and continuously monitor vendor risk.

Next, finding a scoring vendor to easily integrate into your current processes and systems. You'll have to go through the evaluation process to see which vendor is right for you, both with current data and interoperability. Once that's out of the way, you'll then need to onboard your third-party vendors and organize them by operational importance.

After you've identified how many vendors you have, use a numerical score for each vendor by outlining the risks associated with each. From here, you can rank each vendor accordingly and begin to interact with them to fix their security posture.

Your work should be focused around which vendors scored below your set threshold and the areas they need to address to meet your acceptable risk range.

Be prepared that this entire process can take 6 - 12 months to stand up. Interacting with vendors to remediate issues can take even longer. While effective in-house solutions can be developed in a reasonable time period, it's not uncommon to exceed both a planned timeline and an estimated budget.

Lastly, you'll want to assess whether or not you can change your leadership's opinion on risk and gain their confidence in the solution you've built.

Faster & Better Value

BlueVoyant Cyber Risk Management Services can be integrated in days, exponentially speeding up deployment and giving you the confidence inherent in identifying risks quickly. You'll be able to speed
up review of vendor risk profiles and immediately report on risks to your executives.

BlueVoyant Risk Analysts will triage any findings and work directly with your vendor to remediate issues.

You and your executives can rest easy knowing BlueVoyant will continuously monitor vendor security postures based upon the security standards you set. You can rely on BlueVoyant to reduce sensitive data vulnerabilities and protect everyone in your ecosystem.

Service Execution

An effective risk program needs to be continuous. It needs to consistently monitor vendor risks, notify you when problems arise, triage notifications, and interact with your vendors to remediate issues. It must ensure enterprise security standards are met while concisely reporting relevant information to your leadership.

As you build out your feature sets and continuous monitoring capabilities, you'll need to ensure you have the staff to interpret the data collected, and more importantly, articulate the data findings to engage directly with vendors and remediate any issues that arise.

Ask yourself, "can my team effectively interpret what was found? Do they know the actual risk associated with what they're seeing?"

You'll also need a tracking program in place to tabulate cases and responses to ensure mitigation is done effectively. This should also include an evaluation process for a post-action review of mitigation steps taken by your analysts and your vendor.

Will you be able to confirm that the vendor did indeed rectify the problem? Next, assess your internal bandwidth and ask, "how many vendor issues can we effectively investigate at once?"

Communication during this time is key. You'll need a process that provides internal and external updates, as well as a database for historical tracking purposes. You'll also need a way to report findings to executives.

24/7 and Always Ready

BlueVoyant Cyber Risk Management Services help mitigate security risks with third-party vendors by continuously monitoring their security posture to ensure they meet your enterprise security standards.

Upon signing up, customers go through an onboarding process, filling out a security profile and setting up vendor parameters. Vendors are then onboarded, scored, and ranked using BlueVoyant's proprietary scoring system.

Initial assessments and new alerts are triaged by expert analysts to eliminate false positives and remediate effectively.

You're able to review data in real time and download reports that can assure your executives the problem is under control.

Knowledge and Expertise

Just like cybersecurity, the risk management sector is experiencing a talent shortage. According to a survey from RIMS (the Risk Management Society), 94% of respondents believe risk management professionals will need to develop new skills to meet future challenges, yet just 32% believe they are prepared to make the changes needed. What's more, only 16% of respondents think there will be enough graduates to fill open positions in risk management by 2025.

On top of that, 40% of companies believe they have sufficient resources allocated to their third-party risk management program. Most programs are point-in-time-based, can you confidently say you have the resources in-house to effectively monitor and remediate vendor issues? Consider the following questions:

- Do you have the right talent? Performing a comprehensive view of the vendor's attack surface requires engineering and security expertise.
- Who will monitor and manage digital risks alerts and take action when issues are discovered?
- Do you possess the resources and expertise to determine critical vs. non-critical?
- Most security ratings platforms focus on publicly accessible, external data sources to assess and benchmark vendors. While good, this information can lead to an incomplete picture or a high rate of false positives. Do you have the right talent to analyze this data and fill in the blanks? Do you have the time to?

In today's data-driven world, ensuring you have the right technology and set of expertise in place to protect your data from internal and external risk is the best decision you can make. You must be confident you have the right measures in place.

Trusted Experts

BlueVoyant Cyber Risk Management Services are built on BlueVoyant's core capabilities and business line expertise. Our team of expert world-class, former cyber attackers and defenders review and evaluate findings and provide remediation recommendations. This curation function allows you, the client, to effectively review our findings from monitoring, evaluation, and remediation activities.

By codifying our cybersecurity expertise into our risk offerings, BlueVoyant is able to integrate the knowledge we've gained through actively investigating and remediating cyber attacks across our entire client base into our risk services as they occur.

Scalability

Ponemon Institute research found that, on average, companies share their data with **583 third parties.** While Fortune 100 organizations with vendor counts in the tens of thousands push that average up, **58%** of organizations still say they share information with more than **100 third parties**, further illustrating the point that it is increasingly difficult to extend and enforce your enterprise security controls to hundreds of other companies while keeping up with other day-to-day responsibilities.

Manual questionnaires take months to complete; multiply that by a number of vendors. Then factor in how many alerts you might need to investigate for each vendor. You have to determine how many are false positives and how many need investigation. You must determine how many vendors you can effectively continue to monitor for changes in their security posture.

To effectively DIY, you have to consider the vendor lifecycle - onboarding and offboarding. How will you handle new vendors or new organizational requirements? Do you need to worry about compliance?

If you've followed our advice, you'll no longer need to rely on vendor surveys and attestations. You've built your program to keep up with the complexity and volume of work required to accurately measure and monitor the security program quality of all your third parties.

The reality is, you need to cover your bases today, but look towards the future. You've built out your program to have the best foundation of technology and expertise - now prepare it to scale so you can maintain your posture and adapt to the changing risk landscape.

Flexibility & Relevance

BlueVoyant Cyber Risk Management Services help you tackle the threat landscape. The evolution of threats and the changes within your business affect your threat posture. That's why it is important to seek out new data sources to keep ahead of vulnerabilities.

At BlueVoyant, scalability is a top priority. We continue to invest in finding new and innovative data sources that empower our experts, products, and services with the breadth and visibility needed. We are ready to help as your needs change.

Managing vendor risk is not easy. There is a major risk of doing it yourself. Can you afford to take that chance?

Managing Cyber Risk with BlueVoyant

BlueVoyant Cyber Risk Management 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 Cyber Risk Management Services include:

Vendor Risk Management

BlueVoyant Vendor Risk Management helps organizations obtain clear visibility into cybersecurity risks across their organizations by proactively identifying, prioritizing, and remediating cyber risks posed by business partner and supply chain relationships.

Cyber Risk Management for Investors

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

For more information visit: www.bluevoyant.com
Secure your business today: contact@bluevoyant.com