Whitepaper

Supply Chain Defense

What a Board Needs to Know

BlueVoyant
Terrain: SCD™

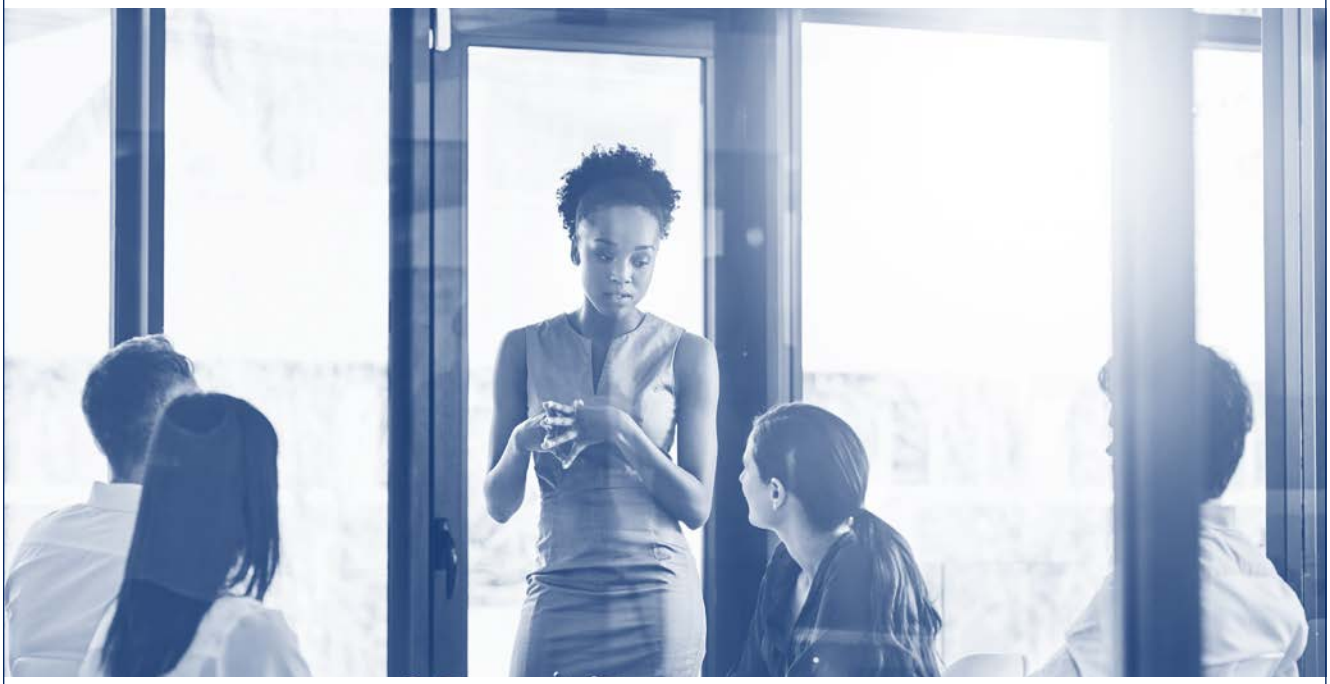
BlueVoyant

Executive Summary

Supply chain cyber risk has rapidly become one of the most prominent and pervasive risks faced by today's organizations. Third party connections, which include suppliers, partners and service providers, can distribute an organization's operational and business risk among multiple thousands of critical vendors. With the growing attention and expectations of investors, partners and regulatory agencies around cybersecurity, board members across all industries should care more than ever about supply chain cyber risk.

A board's view of their organization's cybersecurity risk posture is incomplete if it does not consider the third-party connections that make up their supply chain and extended ecosystem. In order to be effective, a board needs to have oversight over supply chain cyber risk, timely and relevant updates on the changing state of the organization's risk posture, and assurances of action relating to their risk management program. As an organization's highest level of oversight, it is the responsibility of the board to be actively involved in cybersecurity in general and supply chain cyber risk specifically.

One of the most prominent challenges for security executives in keeping their organizations safe from cyber attacks is having the resources and buy-in from executive leadership teams and their board of directors. It is therefore critical that executive cyber risk owners (whether they are a CISO, CRO, or other) know how to bring to light the importance of this topic to a board that may lack awareness. This whitepaper will outline best practices to frame and achieve the goals of broader board involvement, both for cybersecurity-owning executives speaking to them, as well as individual board members seeking to track the progress of their cyber risk programs within their organizations.



Supply Chain Cyber Risk

What Board Members Should Know

Among the many strategic challenges that a modern board of directors must contend with, cybersecurity, and specifically cyber risk attributable to third parties and the supply chain, has dramatic implications on an organization's financials, business operations, and brand reputation. While your organization may have its internal network's security covered, it is critical that you and every other leader at your organization know that your digital attack surface (i.e. all of the points where cyber threat actors can try to breach an IT perimeter) is much larger and more complex than many realize. At the same time, it's imperative to understand how your organization will be impacted either directly by a cybersecurity breach, or indirectly by vulnerabilities within your supply chain from a business continuity and trust perspective.

While they may appear separate, the vendors, suppliers, and partners that make up your third-party ecosystem contribute to your organization's security posture. Because of the inherent data connections and trust-based relationships that exist between a primary organization and its third parties, your operational risk may actually be distributed among perhaps thousands of vendors, partners, and suppliers. Information ranging from customer lists, to product plans, to core intellectual property can be found in many places outside a company's own IT environment, and third-party relationships can offer easily exploitable ways to infiltrate the networks of even the most well defended organizations.

Put another way: every organization is only as safe as the weakest link in its supply chain, which offers vulnerable targets to attackers. Most companies work with anywhere from 500 to 10,000 third parties, which can represent high levels of compounded risk.

So what does your extended attack surface actually look like?

Historically, a company's attack surface was viewed as limited to its own assets (endpoints, IPs, domains, etc.), rarely concerned with or addressing the exposure of their external vendors. Today, creative threat actors' relentless efforts to find weaknesses in networks have taken advantage of this. Recent high profile supply chain breaches, such as those that affected Solarwinds, Accellion, and Kaseya, have garnered the attention of executives responsible for the continuity of their company's operation, as well as their company's reputation and financial security. A security incident that occurs at any stage of the supply chain will have effects upstream, downstream, and laterally on the entities that rely on it, and can impact even more than just a given sector.

In certain business contexts the security of a third-party ecosystem might require as much attention as that of an internal network. From the perspective of a threat actor, supply chain targets represent an ideal union of two approaches they can take: the path of least resistance and the path that leads to most access. Rather than expend resources trying to breach a primary target's hardened outer perimeter, an attacker can achieve their goal by using access previously granted to a trusted but less secure third party. To make third parties even more appealing targets to threat actors, a single critical supplier in a given industry will often work with multiple enterprise organizations that can be compromised via the third-party breach. If an attacker is able to compromise one such critical supplier they may gain access to various high profile customers. This is what occurred during the Solarwinds breach, where a trusted software update was compromised by attackers[1] and used to push malicious code into the networks of hundreds of unsuspecting customers.

What does Supply Chain Risk Mean for Your Organization?

Supply chain risk can represent varying concerns to different organizations and industries. In general, when looking at third-party cyber risk, it can be defined as the potential for a primary organization to suffer a data breach or disruption, or be negatively impacted and indirectly compromised, via digital connections to external organizations and entities.

Vendor and supply chain risk management is important from both a brand protection and security perspective, as many high profile third-party breaches result in brand damage for the primary organization. Because of this, and due to the increasing complexity of supply chains across virtually every industry, many organizations are increasingly trying to create third-party cyber risk management (TPRM) programs that can address this problem.

As an executive involved in overseeing cyber risk exposure, are you aware of how your organization addresses third-party risk and confident in its mitigation program? To maintain an effective third-party cyber risk program, it is critical to get stakeholder buy-in in order to ensure the program is sufficiently funded and will grow as needed. Additionally, it is vital to build partnerships with business units, as they likely control vendor relationships and the governance around onboarding and offboarding.

"To maintain an effective third-party cyber risk program, it is critical to get stakeholder buy-in in order to ensure the program is sufficiently funded and will grow as needed."

Liability

It is sensible to think that a vendor would be the entity liable following a data breach or other cyber incident, but often this is not the case. If one of your third parties is affected by a cyber incident, it now becomes a major problem for your organization from the perspective of fiduciary responsibility. Therefore, in order to understand and manage risk, everything you are responsible for must be measured.

In the case of a third-party breach, liability depends on the contractual make-up of the third-party agreement. Typically, those agreements contain limitations and often will not meet the fiduciary obligations to manage such liabilities in the event of a substantial security incident impacting your organization. Ultimately, regardless of the amount of liability that may be shifted to a third-party, your organization and your brand is responsible.

Given these implications for an organization, board members have an obligation to ensure duty of care and shareholder protections. It is critical not to rely on contracts alone as comprehensive assurances that the company is protecting its brand and its assets. In the event of negative impact to your organization, the responsibility belongs to a company's executive risk-owners, and not something that can be shifted to a third-party partner. It is imperative to be able to measure the risks associated with third-party engagements, what they may represent to the organization's risk profile, and govern how those suppliers are monitored.

Investor and Compliance Implications

As a result of the enormous threat posed by cybersecurity incidents, investor interest and concern has risen as it relates to how organizations manage their risk postures. The fact that third-party cyber risk is now a diffuse problem means that investors want to know how your organization is specifically managing that kind of risk. The more traditional practice of macro reporting and generalized statements will no longer meet the needs and requirements of many investors, particularly those institutional investors who continue to become more educated regarding the ancillary risks associated with third-party arrangements and connections.

This has increasingly become clear to regulators in addition to investors. Recently, government oversight agencies around the world have increasingly established rules and regulations that govern third-party relationships across a highly diverse set of industries.

In the United States, the Securities and Exchange Commission in 2022 put forth a new proposal[2] requiring that any cyber breach must be included in periodic disclosures, and any "material" incidents (i.e. something that reasonable shareholders would consider important) must be reported within just a few days of occurrence. This includes breaches and compromises through third-party connections, regardless of whether those third-parties were considered first or second tier in terms of criticality.

New proposed requirements by the SEC would also require every public company to name a cybersecurity expert on their board, and require board involvement in the review, assessment, and implementation of cybersecurity policies and procedures. This makes it incredibly important for board members to have high fidelity in the data they are provided by the management team, including on third-party risk, supply chain and partner health, etc.

In terms of implementation, these regulations could follow how the Sarbanes-Oxley Act (SOX)[3] was enacted, through which members of the board are required to attest and "personally" sign off on the fact that standards and details are accurate. How can a corporate director or board member carry this out without a degree of assessment data? This is where a successful TPRM program can provide the level of detail and efficacy needed to either assess, attest or remediate.

Rule making will more than likely conclude in early 2023 for implementation in 2024 – leaving 2023 an opportunity for companies to address gaps and prepare for the requirements the SEC is looking to implement. Third-party risk is currently a large gap for many organizations and, at minimum, measurable visibility and reporting will be a key competency companies will need to address in order to fulfill the large set of proposed cybersecurity disclosure requirements.

How a Board can Ensure Better Supply Chain Defense

How often should Executive Briefings and Board Updates Occur?

It Is imperative for the board to receive periodic updates from the leader of the cybersecurity function in an organization, whether it be a CISO, CIO, CRO or other. In some cases, updates should be carried out quarterly or bi-monthly. In other cases, it might be acceptable for updates to come through meetings with subcommittees, with the minimum of a bi-annual read out to the entire board. These updates should focus on the overall status, trends, and metrics of their respective cybersecurity program and initiatives. Each industry will have specific risks that should be the focus of their cyber risk programs, and so should be reflected in these updates.

For their part, board members should make sure that updates and briefings are scheduled, and be prepared to ask the relevant questions associated with the risks of their respective industry and business processes in order to ensure that there is oversight and visibility at the highest level. The potential risks inquired upon should include third-party arrangements, which typically are reported and less scrutinized instead of being properly monitored and mitigated. Of course, it is just as important to have assurances of action and results tracking related to supply chain risk, so all briefings should establish practical next steps and goals to be validated at the next briefing.

Complementing board verification, executive cybersecurity owners should ensure that they have the opportunity and the right method to disclose and share the ongoing challenges and successes of cyber risk management programs. Individuals in this position may already have ways of keeping track of and reporting on different aspects of security, but not third-party cyber risk.

Planning for the Next Board Meeting

What questions should the board be asking and should every executive risk-owner be able to answer? Board members should be asking key questions and executive risk-owners should be able to answer those key questions. Of course, the extent of the depth of those questions will be relative to the resources and attention already invested in a TPRM program. Keep in mind that relying only on surveys and contracts to govern third-parties is not enough, so consider the following two tiers of example questions to ask depending on your organization's maturity:

Initial baseline questions

1. What assets or data matter to your company most and why?
2. Where are they stored and how can one find them?
3. How are you protecting it?
4. Where are we most vulnerable and at risk? What third party arrangements do we have that place us at risk?
5. What response plan do we have in place for if an incident were to occur?

Secondary advanced questions

1. What frameworks do we use to manage risk, and how do we benchmark ourselves using these frameworks?
2. How are we evaluating our partners and suppliers within our ecosystem? Specifically, those that have access to our network, our data and/or our transactional platforms? How is this measured and monitored?
3. What types of threat actors are interested in attacking us, what are they motivated to do so and how do we defend ourselves against the specific techniques they would likely employ?
4. How much friction do we add to the customer and user experience through our risk mitigation practices?
5. How do we discover our own sensitive data located outside our network, and how do we protect it?
6. Do you have the resources you need to be successful?

Best Practices for Improving Supply Chain Security

So where does that leave you in practice? There are a number of best practices you can advocate to be implemented across the organization in order to shore up supply chain defense and move yourself towards an improved risk posture for your extended ecosystem. The supply chain defense experts at BlueVoyant have identified the following:

1. **Identify and prioritize** vendors to monitor and secure, focusing on their criticality to production, access to critical systems and data, as well as importance to business operations.
2. **Consider additional "cyber" risk factors** related to network/endpoint resource utilization, user install base, and popularity among user groups with privileged access such as human resources, legal, IT, and finance.
3. **Continuously monitor** the extended vendor ecosystem, using contextual analysis to prioritize Zero Tolerance and critical findings mitigation. Traditional solutions like questionnaires and point-in-time scans are useful, but not sufficient for for comprehensive supply chain defense.
4. **Build out governance processes** and work with procurement - ensure security checks are included into your organization's procurement process to ensure you are discovering security gaps up front and work required by the third party can be baked into the cost of the current contract reducing the likelihood of unexpected cost increases (To include offboarding). Make sure there is a process and that everyone is aware of it
5. **Report regularly and effectively,** ensuring that business leaders have a clear view into supplier risks that inform decision making and risk acceptances.
6. **Maintain response readiness** by assessing your organization's ability to detect and investigate attacks within the supply chain and by adding failure scenarios to your regular table top exercises and wargames. Ransomware events, emerging risks and zero day vulnerabilities are increasing in frequency and can suddenly impact your supply chain. (Reporting on unexpected events, you need to be able to respond readily and report on what is not in scope when asked by leadership)
7. Finally, **leverage platforms or solutions** that proactively track how critical vendors are addressing externally visible misconfigurations, and that will work with the vendors directly to reduce risk across their exposed attack surface.

How a Partner Solution can Help

In order to jumpstart the TPRM maturity of an organization, solutions are available that can begin to immediately ensure active cyber risk mitigation in your supply chain. Leverage platforms or solutions that proactively track how critical vendors are addressing externally visible misconfigurations, that utilize continuous monitoring and can track instances of emerging vulnerabilities (including zero-day vulnerabilities) in your supply chain.

In order to reduce the strain created between your organization and its third parties, look for solutions that can remediate and address risk by directly communicating with and supporting suppliers. BlueVoyant's Terrain: Supply Chain Defense provides a comprehensive and easily implementable solution to rapidly increase risk mitigation and defend suppliers and partners up and down the value chain of your business operations. BlueVoyant delivers the ability to not only alert to externally detectable vulnerabilities with suppliers and partners, but also to continuously monitor these third- and fourth-parties and quickly remediate any issues.

Sources

1 https://www.bluevoyant.com/resources/what-does-a-third-party-breach-look-like
2 https://www.sec.gov/rules/proposed/2022/33-11038.pdf
3 https://www.techtarget.com/searchcio/definition/Sarbanes-Oxley-Act

Rock-solid cyber defense you can trust

BlueVoyant converges internal and external cyber defense capabilities into an outcomes-based, cloud-native platform called BlueVoyant Elements™. Elements continuously monitors your network, endpoints, attack surface, and supply chain as well as the open, deep, and dark web for vulnerabilities, risks, and threats; and takes action to protect your business, leveraging both machine learning-driven automation and human-led expertise. Elements can be deployed as independent solutions or together as a full-spectrum cyber defense platform. BlueVoyant's approach to cyber defense revolves around three key pillars — technology, telemetry, and talent — that deliver rock-solid cyber defense capabilities to more than 700 customers across the globe.

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

BlueVoyant