BOSTON CONSULTING GROUP

White Paper

Protecting Digital Value with Third-Party Cyber Risk Management

Nadya Bartol, Matthew Doan, Jeffrey Ng

November 2020

As companies fight their way to a post-COVID-19 future, their executives are accelerating digital transformation efforts. Simultaneously, they are increasingly relying on third-party suppliers to develop and manage the digital platforms and capabilities that deliver transformative value to the business. Yet each additional third party presents new cybersecurity risks. In fact, many of the significant publicly disclosed cyber incidents in recent years were caused by the poor cybersecurity practices of suppliers. The most notorious global cyber attack, NotPetya, originated from infected third-party software and ultimately caused over $10 billion in damages.

To minimize this threat and protect the business's digital investments, companies must integrate third-party cyber risk management directly into the digital transformation process. Boards, CEOs, and CROs should be at the forefront of the effort, creating a strategy and approach for dealing with cyber risk, embedding appropriate cybersecurity at the beginning of each third-party relationship, and forming a strong multidisciplinary team to manage the initiative—ensuring that the topic becomes a mainstay of the business strategy and the enterprise risk agenda. Our approach, developed in partnership with the National Institute of Standards and Technology (NIST), offers businesses a powerful chance to reach their digital transformation goals while remaining resilient in the face of today's continuously evolving cyber risk landscape.

Complex and Growing Third-Party Cyber Risk

Companies across the globe are accelerating their digital transformations as they work to improve the bottom line, boost revenues, and build resilience. While third-party relationships have always been essential to such efforts, the growing scale of their use and the resulting risk to the businesses they serve are creating a challenging new reality. Many businesses now comprise an extensive ecosystem of interlinked companies dependent upon their own constellation of third parties. The result is a dizzying web of high-risk business connections, making third-party risk management an increasingly complex and sophisticated problem.

Ensuring a Well-Architected Program

In the past, businesses introducing new digital technologies have typically prioritized cost reductions, deadlines, and performance over managing potential cyber risk. In today's digital landscape, however, they can no longer afford to dismiss cyber risk as a lesser priority. Instead, digital enterprises must address this risk directly and expeditiously if they are to protect the business and fortify it against future shocks.

A well-architected third-party cyber risk management program addresses the following objectives:

1. **Closely manage third-party cybersecurity.** Proactive management of third parties reduces the risk of incidents and their potential cost. Companies need to first ensure that their third parties' cybersecurity controls are aligned with the company's requirements, and second, establish appropriate communications protocols should an incident occur.
2. **Employ proactive cybersecurity analysis during M&A.** A cybersecurity assessment during the due diligence phase will shed light on potential risks from a new entity or its third-party portfolio. During the integration phase, it's important to scrutinize the specific digital connections and supplier relationships before they are allowed.
3. **Ensure vendor security.** Companies continually introduce information technology (IT) and operational technology (OT) into their environment. These technologies can become open attack pathways if technology vendors do not properly secure and maintain them. Organizations must have trust and confidence in the software and devices they allow inside the enterprise, from executives' mobile devices to smart meters and manufacturing systems.
4. **Deploy secure cloud services.** The leading cloud service providers, such as Amazon and Microsoft, are diligent about securing their products and services. The true danger lies with individual cloud services offered by less mature companies that often lack the resources and incentives to fully secure their products. Businesses should focus their time and attention on the cybersecurity of these individual providers, both at the time of purchase and during use, as a part of their ongoing risk management program.

Bringing Third-Party Cyber Risk Management to Life

Companies can achieve these objectives by implementing the following proven framework. The framework contains three simple parts: organize, analyze, and engage.

Our BCG team formulated this content from our work with NIST (see the sidebar "Industry-Leading Resources & Tools") and by infusing it with extensive learnings from our client work.

Industry-Leading Resources & Tools

These resources and tools, created by NIST and BCG, can be used to help establish and run a robust third-party cyber risk management program.

- **2019 Case Studies in Cyber Supply Chain Risk Management** provides findings and recommendations based on interviews with 16 subject-matter experts across a diverse set of six companies in separate industries to explore the best practices in use today.
- **Key Practices in Cyber Supply Chain Risk Management** provides summary recommendations based on case studies, NIST insights, and BCG experience. These key practices aid the design of an effective third-party cyber risk management program.
- **Impact Analysis Tool for Interdependent Cyber Supply Chain Risks** offers a novel method for evaluating the security of an organization's third parties in the context of business criticality.
- **Criticality Analysis Process Model** provides an approach for identifying the systems and components that are most vital and may therefore need additional security.

Organize. Successful third-party cyber risk management starts with alignment. From the CEO and the board down to the staff on the ground, organizations need to thoughtfully embed a new mindset and practices focused on collaborative management of cyber risk and the protection of priority digital investments.

- **Integrate third-party cyber risk management across the organization.** Third-party cyber risk does not belong to a single department. It requires cross-organizational collaboration within the relevant business functions, including procurement, supply chain management, IT, cybersecurity, legal, engineering, software development, R&D, and HR. Organizations should establish both formal and informal communications channels, such as supply chain risk councils or working groups, that cut across the organization to improve the flow of information and promote efficient and effective identification and management of third-party cyber risks.
- **Establish a formal program.** An appropriately sized third-party cyber risk management program establishes the necessary processes and accountabilities to produce efficient and effective remediation of third-party cyber risks. When processes are well-established, they facilitate a uniform approach to prioritizing risk management efforts without compromising business objectives.
- **Plan beyond the initial onboarding.** Once a new third party is assessed and onboarded, companies should establish communications protocols for use during incidents. Businesses should also monitor third parties regularly and consistently as part of their ongoing risk management program. Finally, to prepare for future issues—such as a third party that goes out of business or experiences a crippling cyber attack—it's important to run collaborative exercises across functions and in cooperation with third parties, such as tabletop exercises or war games, to understand these possibilities and implement appropriate contingencies.

Analyze. An organization must have strong situational awareness to continually manage third-party cyber risk. This awareness starts with an inventory and prioritization of the most business-critical suppliers to facilitate an assessment that sheds light where targeted engagement is required.

- **Understand the third-party network.** The better the organization can visualize and interpret its supplier portfolio, the more effective its management of third-party cyber risk will be. This includes understanding the practices adopted by third parties to ensure the security and integrity of their technology environments and products, along with the relationships they hold with their third parties.

- **Know and manage critical third parties.** Critical third parties are those whose business disruption would create a substantial negative impact on the organization. Prioritizing third parties provides the organization with a starting point for third-party cyber risk identification and remediation activities.
- **Continually assess and monitor.** The focus of third-party cyber risk management activities should extend well beyond the onboarding stage. Third-party relationships are continually evolving throughout the relationship and businesses should monitor changes in third-party status and performance and subsequent security implications.

Engage. A successful third-party cyber risk management program involves collaboration to develop mutual trust and understanding. Businesses should work with their third parties to improve their cybersecurity practices and establish a common set of security standards for all parties.

- **Collaborate closely with priority third parties.** Once businesses have prioritized their third parties by criticality, they can partner with those entities to maintain acceptable levels of cyber risk. Businesses can do this by collaboratively discussing industry threat activity or changes in their technology environments, or by assisting third parties with improvements to cybersecurity controls and practices.
- **Include leading third parties in resilience and improvement activities.** Critical third parties are not just an important part of a business's network; they play an essential role in overall resilience and stability. As such, they should be considered and included in the development of business continuity, incident response, and disaster recovery plans, and participate in the tests of those plans.

* * *

Strong third-party cyber risk management is vital to a successful digital business—both in the transformation and the steady-state phases. By elevating and maturing third-party cyber risk management programs, organizations will greatly improve their chances of a secure transformation to a sustainable digital future.

About the Authors

Nadya Bartol is a managing director in the Washington, DC, office of BCG Platinion. She has more than 25 years of cybersecurity technology and management experience across multiple industry and government environments. Nadya is co-author and editor of numerous NIST and ISO documents, including those on cyber supply chain risk management and security measurement. You may contact her by email at bartol.nadya@bcg.com.

Matthew Doan is a senior manager in BCG Platinion's Washington, DC, office. He has extensive global experience in helping companies and government agencies digitally transform to more cost-effective, cyber-secure, and resilient states and has a passion for solving problems at the intersection of technology and human dynamics. You may contact him by email at doan.matthew@bcg.com.

Jeffrey Ng is a senior consultant in the New York office of BCG Platinion. He has advised global clients across multiple cybersecurity domains, including third-party risk management, security strategy and governance, and secure development operations. You may contact him by email at ng.jeffrey@bcg.com.