In February 2020, KPMG hosted a third-party security roundtable for cyber leaders. The objective of this event was to discuss the mission-critical role of managing third-party security. We heard from a diverse range of voices on how third-party security functions are innovating to keep ahead of expectations from the business, affiliates, vendors, regulators, and clients. This paper presents the key themes arising from this event.

Cracks are emerging in traditional approaches to third-party security.
Increasing complexity and integration within digital ecosystems is driving cyber leaders to rethink their approach to managing third-party security. This process has exposed a variety of limitations with traditional approaches to third-party security:

— **Latency:** Typically, reviews are conducted on a one-to three-year cycle. However, the rise of DevOps is driving an exponential increase in technological change. Security leaders need more real-time security information of their third parties.

— **Enterprise focus:** Reviews typically focus on enterprise controls, whereas security leaders are increasingly interested in critical assets and the associated technical controls.

— **Level of effort:** Organizations individually invest significant time and resources in their third-party security programs, and undertaking unique reviews is a labor-intensive process.

— **Inconsistent standards:** Lack of convergence between standards, combined with varied approaches to control evaluation, increases the complexity of vendor reviews. Initiatives seeking to address this include the adoption of utilities and the shared assessment framework.

Regulators are paying increased interest into how organizations manage third-party security.
Regulators are becoming increasingly stringent in their approach to overseeing third-party security programs. Key areas of focus among regulators include supply chain resiliency, strength of the second line challenge capability, and assurance over the quality evidence provided by third parties. In response to this, organizations are actively considering how best to manage regulators’ expectations.

Without a hint of irony, and despite requesting significant amounts of data from organizations, regulators have so far exhibited an unwillingness to be subjected to third-party security reviews.

There is a widening divergence of approaches to risk management between regulated organizations and their third parties.
Nonregulated third parties, with significantly fewer compliance requirements, typically have less mature security oversight functions than their regulated financial services clients. This presents a challenge to security leadership, who are expected to manage their organization’s security at a time when boundaries between the organization and its third parties are becoming increasingly hazy. For example, Software-as-a-Service and Infrastructure-as-a-Service providers typically will not have a second line of defense.

Regulators are seeking to address this by expanding their focus to include the use of systemically significant service providers, such as major cloud providers.

"Responding to demand changes around third-party security is a key priority for cyber leaders. This is driving a wholesale rethink in how risk management is done in an ever expanding supply ecosystem."

—Jonathan Dambrot
Principal
Cyber Security Services
Tensions between third-party security programs and the business remain unresolved. Despite concerted efforts, there has been limited progress in aligning third-party security programs with business agendas. Significant doubts have been cast over whether cyber leaders are empowered to forcibly offboard third parties with inadequate security posture. Indeed, when mitigating a third-party security risk requires a “line stop,” businesses tend to encourage risk acceptance. This is sometimes rooted in a security organization’s struggle to communicate risk in business terms.

Offboarding resistance is particularly apparent for critical third parties. In at least one instance, security leadership was requested by the business to provide remediation support for a business-critical vendor that extended to the provision of hardware. Alongside this, cyber teams often face challenges in quantifying return on investment or (residual) cyber value at risk for their third-party security programs. This creates a challenge when making budget requests of—and reporting back to—executive leadership.

The current maturity of utilities does not provide a “one-stop shop.”

It’s abundantly clear that there is no “one-stop shop” when it comes to the assessment of utilities. Coverage of vendors and their respective focus areas vary significantly. Organizations still need to conduct their own reviews, tailored to their individual risk exposure, and perform extensive analysis on utility reports. Legal concerns increase the complexity when nondisclosure agreements limit information sharing. What’s more, questions remain over how willing regulators are to accept risk programs that rely on utilities.

Organizations are incorporating threat intelligence into third-party security programs.

The sophistication of adversaries’ tools and techniques continues to enhance, and this is driving an evolution of the cyber threat landscape. In response to this, cyber leaders are increasingly considering how risk profile changes may impact their third parties’ security posture. Cyber leaders are acutely concerned by “island hopping,” wherein adversaries can gain access to an organization’s corporate network via a compromised third-party asset.

The trend is leading some organizations to experiment with incorporating open source threat intelligence to help scope third-party security assessments. Some early successes have been proven, with data being used to inform security expectations of third parties’ underlying critical assets.

Organizations are rethinking how they share security information with their clients.

For many organizations, accountability for data security and data use is shared between disparate groups. This limits the degree of control that can be asserted over proprietary data. Security leaders are seeking to address this by investing in technologies that enable them to provide clients with data securely within their own environment and to keep track of which clients have access to what data outside their environment.

Leading technologies seeking to address this issue cover end-to-end data flows including data usage, data monitoring, encryption, access restrictions, multitenant support, and data lineages.

Connect with us. Learn more about KPMG’s innovative third-party security solutions and participate in future third-party security roundtable events.

Matt Miller
Principal
Cyber Security Services
E: matthewpmiller@kpmg.com
T: 571-225-7842

Jonathan Dambrot
Principal
Cyber Security Services
E: jdambrot@kpmg.com
T: 908-361-6438

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.