



The extended enterprise — securing the future

**Charting the course towards a more
secure third party ecosystem**

KPMG International

home.kpmg/cybersecurity



Contents

Foreword	03
Closing the door to open innovation threats	04
Managing security risk in the new ecosystem	06
Supplier risk is expanding to the Nth-degree	08
Forging closer collaboration and connections	10
Let's make smarter choices on data security and privacy	11
Regulators now have a timely opportunity to drive progress	12
Working together to evolve ecosystems	13
How KPMG can help	14
Our authors	15
Contacts	16

Foreword

The need to secure new and increasingly complex supplier ecosystems in the digital age is rapidly rising up the agenda of CEOs around the globe. Since the beginning of the global pandemic, supply chain risk has risen to become one of the top four growth risks facing today's organizations, as noted in the *KPMG 2021 CEO Outlook Pulse Survey*.

Make no mistake — traditional approaches to third party assurance are no longer fit for purpose in today's new reality. While third party risk management, monitoring and innovation will not be new to your organization; a sharp focus on emerging threats amid accelerating digital transformation, cloud adoption, software-defined infrastructure and new models of working has become critical.

The pandemic has brought into stark relief the need for complex digitally enabled ecosystems that will reliably and securely meet ever-evolving customer and business demands. Our thinking must evolve to match today's incredibly fast-paced, connected and rapidly changing world.

Organizations once concerned with merely managing third parties are now working in a vast new risk-charged world — managing fourth, fifth and even sixth parties. These parties include a mix of cloud and IT providers, partners and affiliates that define today's modern extended enterprise.

The new reality pushes the boundaries and pace of digital transformation. Unlocking new ways to enhance supply chain capabilities and security in the digital era will likely spell the difference between success and failure.

In collaboration with KPMG cyber professionals working with their firms' clients around the world, this paper examines today's challenges and the emerging solutions that promise to help businesses implement modern supplier ecosystems that: reduce risk, build trust, improve privacy, drive ongoing innovation and manage compliance.



Jonathan Dambrot
Global Third Party
Security Leader
KPMG in the US

Closing the door to open innovation threats

Understanding and effectively managing the third party ecosystems supporting today's businesses has become more challenging than ever amid the rapid proliferation of new, digitally enabled, open innovation models.

KPMG professionals are seeing back doors being written into critical commercial and open-source software that, once embedded, unlock dangerous opportunities for bad actors to deploy malware into otherwise secure infrastructures. Those back doors can lie dormant, appearing benign, until activated by an attacker. Polymorphic malware that changes its identity features to evade detection, typically introduced by a subverted security or management tool, can quickly undermine even the most hardened security environment.

To compound that challenge, gaining clear visibility into today's increasingly broad and complex supply chains via legacy third party risk management is becoming extremely difficult.

Historically

An organization might become aware of a potential supplier related incident and use external security monitoring tools to identify and respond to indicators of compromise. The affected organization might be inundated along the way by requests from anxious clients seeking to confirm that their data is secure. This unfolding process can often overwhelm the victimized business, resulting in a lack of timely action and guidance to clients.

Currently

Techniques in third party security are being developed to address such threats. Security ratings and monitoring companies are starting to help organizations utilize more relevant data based on need. Also, the use of artificial intelligence and machine learning can advance the monitoring of anomalous behavior. These tools can integrate multiple data sources, which can then be used to learn what risks may persist beyond those provided by a single analyst.

In addition, the US National Institute of Standards and Technology and others are developing capabilities like the [Open Security Controls Assessment Language \(OSCAL\)](#) to enhance communication, standardization and automation of security control data. Initially created to support the US government, this framework is now being used commercially to deliver better visibility and frequency of critical assessment data.



Case study

Unlocking the power of higher risk-visibility

Working with a financial services client, KPMG in the US recently used its Continuous Assessments and Monitoring model to explore how best to move from point-in-time assessments to a more proactive, risk-based approach to third party security. In our proof of concept, near real-time security control data collection was configured between the client and a third party, standardized using OSCAL and tested for compliance against Service Level Agreements (SLAs). The model demonstrated the power of increased risk visibility, how it can enhance the client's risk posture understanding, and how they could automatically address issues as they arise.



Managing security risk in the new ecosystem

Today's typical enterprise is being inundated with vast volumes of confidential data and intellectual property traversing its ecosystem. Of course, understanding the flow of data moving across a supply chain has always been critical to gauging supply chain risk. But in today's ecosystems, those data flows are becoming increasingly complex and opaque. Amid rapid advances in technology, the variety and number of threats and vulnerabilities to business data is growing, and amongst that, third party incidents are on the rise.

As challenging as it is today, identifying ecosystem risk is critical to understanding the potential threat to your organization. Clarity on the following is critical:



Your organizations place in the ecosystem

The first step in the risk management process is understanding where your organization is situated within the ecosystem. The organization must understand its internal and external environments and determine its mission-critical information assets, where they exist and how they flow across this system. This will enable a risk-based approach that's solidly focused on protecting all critical information.



Data sharing

With threats and risks in this model being significantly different, one supplier's impact on clients, upstream or downstream, can now mean a loss of service, integrity or data. These data supply chain dependencies mean we need to aggressively understand connectivity, data sharing and relationships with every ecosystem partner. This includes understanding the ongoing level of data sharing between businesses and suppliers. Smart ecosystem stakeholders are now having deeper conversations about fourth parties and concentration risk, for example.



Cloud security

The ongoing migration to cloud services, which has been dramatically accelerated in response to the pandemic's disruptive impact, also increases the potential for internal and external threats. Attacks compromising business email, for example, can now more easily invade clients and suppliers. But the shift to cloud infrastructure has put businesses in an unusual position. The ability to gain assurance of major cloud providers' security architecture remains limited, yet business users are accountable for lost or compromised data if cloud services are breached.

In general, the cloud has modified the risk landscape in the supply chain and is forcing businesses to be creative in their methods to gain assurance or re-evaluate their risk appetite. Given the proliferation of cloud hyperscale providers, the issue of cloud security risk may be something that only a regulator can address at a systemic level.



Intersection of risks

In addition to cyber and data risk, organizations are looking more closely at the intersection of several different types of risks in the ecosystem. For instance, does financial resilience potentially indicate future cyber risk? Advanced analytics and machine learning models are starting to identify such potential risk scenarios and reveal significant potential issues downstream. As risk models, better access to ecosystem data, and improved technology become part of the third party security toolkit; management will enhance their risk visibility and ability to make cyber risk-enabled decisions.

Supplier risk is expanding to the Nth-degree

The fourth party risk topic continues to resonate among regulators and clients as organizations struggle to understand where their data is being shared beyond their immediate vendors. Primary client data in the data supply chain can now raise new concerns regarding fifth and sixth parties and beyond — today's so-called Nth parties. KPMG's *Third Party Risk Management Outlook 2020* report notes that 72 percent of businesses we surveyed said they urgently need to improve how they assess fourth party suppliers.

The challenge has been agency, visibility and practicality — and its growing complexity concerns business leaders across all industries. Additionally, the increasing concentration of suppliers in the fully cloud-based ecosystem raises concerns about the impact of outages hitting such service providers, mainly as some businesses are now entirely dependent on them.

As it stands, most industries have yet to piece the expanding supplier puzzle together to define a consistent solution to the challenge. But the very fact that individual industries are talking about the subject with regulators and, as a community, gives hope to seeing an effective new approach. While we don't have the answers yet, it will likely involve a combination of sector-wide initiatives that include:



A new mindset on regulatory scrutiny

Regulators in the financial services sector have commissioned reviews into fourth party risk, but a key challenge is that many fourth party suppliers and beyond are small to medium-sized organizations. Imposing regulations on them may prevent them from innovating in ways that their buyers require today.

However, we already see a shift in mindset. The European Commission recently proposed in its Network Information Security 2 Directive the inclusion of a requirement that digital infrastructure (DNS, TLD, cloud services, search engines, social media) adhere to cyber security and incident reporting requirements. These providers make up a large portion of the fourth/Nth parties historically left out of supply chain security approaches.



Greater collaboration is the way forward

In some industries, such as financial services and oil and gas, major players rely on a common set of suppliers. Could the major organizations in an industry, as the dominant set of buyers, influence suppliers to adopt similar third party security approaches with their suppliers? Could sectors gain a new view of fourth party risk by working together and sharing threat intelligence? There is hope. And community led initiatives around training and awareness could also enhance the role of fourth parties themselves in securing today's expanding ecosystems.



Plugging into security rating and monitoring capabilities

We've already mentioned that security rating and monitoring organizations are evolving their capabilities to give organizations more relevant data when they need it. Organizations should take advantage of this and plug fourth parties into these capabilities to determine risk exposure. Obtaining visibility of fourth, fifth and sixth parties remains the biggest challenge here, however.



Managing cloud-bound data

Organizations have a new glimmer of hope as they continue to embark on enterprise-wide cloud transformation. Post-cloud transformation, they could gain an enhanced — and encouraging — ability to control how their extended suppliers access and use their data. Rather than transferring data between multiple parties, suppliers may simply get access rights to data stored in the cloud, thus giving cloud providers the power to implement data security and access controls tailored to each supplier.



Forging closer collaboration and connections

The ability to innovate and collaborate in the new reality requires an ability to more easily integrate data and suppliers into the ecosystem without significant disruption. Data drives innovation in the modern economy, and open architectures and open application programmable interfaces (APIs) are at the heart of this. Acting as the bridges that connect organizations to third parties and their wider ecosystems, APIs have become crucial for the future of commerce.

Open banking

In the Open Banking era, APIs have helped create stronger, more dynamic links between banks and customers and have opened up the European market to so-called challenger banks. With market competition increasing, APIs are now pivotal to quickly innovate and meet customer demand. Some banks implement APIs to encourage collaborative innovation and data sharing with third party partners, suppliers and other businesses. One set of banks developed an API marketplace to collaborate with various stakeholders, including fintechs, on new online banking concepts, customer data, credit cards, payments and accounts.

To help address such timely questions and identify principal security issues when managing API integration, the [Open Web Application Security Project \(OWASP\)](#) has published the API Security Project. We encourage security leaders to explore this to understand how to address any potential security issues.

As open API infrastructure becomes more widespread, we're likely to see strong vertical integration of the supply chain — opening up significant considerations for ecosystem security governance. An organization's data environment may now extend outwards to the Nth party. As a result, questions to consider include:

01

How do organizations then capture customer data movement as it flows fluidly through a supply chain?

02

What do the data-flow diagrams of the future look like?

03

How do organizations monitor customer behavior for fraud prevention or marketing purposes when they're potentially intermediated by layers of third party APIs that act as an air gap?

Let's make smarter choices on data security and privacy

While innovation and collaboration influence our ability to secure the ecosystem, consumer data's vastly increased flow and accessibility are also creating significant new privacy challenges. Amid growing privacy, security and ethical concerns and regulatory scrutiny in the wake of the pandemic, the importance of understanding your data environment becomes a central focus. Nowhere does this play out in the privacy arena more clearly than in the area of data subject rights (DSR).

Under a growing number of regulations across the globe — Europe's GDPR, California's Consumer Privacy Act, Brazil's LGPD, to name a few — consumers and in some cases employees have gained legal rights to increased visibility, transparency and control of data that companies have collected or purchased. Meanwhile, the EU Court of Justice's recent [Schrems II](#) case ruling will likely have a major impact on the transfer of personal data between the EU and the US.

From a consumer perspective, privacy advocates and laypeople alike are being enabled to make better choices about the companies they deal with and how effectively their data is being managed. From a corporate standpoint, timely and accurate fulfillment of such rights, especially at scale, has proven tremendously difficult. This is largely driven by two factors.



It's extremely difficult

Proactively building and maintaining a program and systems to manage and secure personal data across a large, complex ecosystem that encompasses a wide array of suppliers and stakeholders can be extremely difficult. For many industries, we have seen limited progress on enhancing visibility to personal data, or on data subject right request fulfillment. However, with the continued global emergence of privacy and data protection regulations, now may be an ideal time to 'bite the bullet' and build a best-in-class data management and protection program.



Culture and policy

Cultural norms, in some cases enforced by policy, have only exacerbated the problem. Take, for example, data retention practices. In the era of cheap data storage, many companies still suggest or require that employees retain business records perpetually, regardless of business circumstances. Setting aside legal discovery concerns, the volume of data this approach generates makes creating an inventory to support DSR next to impossible.

A framework for understanding how data flows throughout the ecosystem, dependencies on its use and protecting customer privacy throughout the ecosystem is becoming imperative. This will likely require a different level of cooperation among participants, as well as stricter enforcement downstream.

Regulators now have a timely opportunity to drive progress

The regulatory landscape on third party risk management and security is evolving at pace. New regulations are being implemented at regional and country levels. These include the California Consumer Privacy Act, the EU's General Data Protection Regulation, Australia's CPS 234 Regulation and more, all of which aim to provide guidance and clarity on third party risk management.

One of the roles among regulators is to apply a strategic lens to market challenges. The pandemic has forced organizations, sectors and nations to question fundamental assumptions about the interconnectedness of our global market ecosystems, their dependence on technology, and their resilience in the face of cyber attacks. More than anything else, the pandemic has revealed the need for governments and regulators to take a step back and gain a holistic view of how we identify single points of failure in industry ecosystems and how we make sectors resilient to catastrophic cyber attacks.



Key to success — action at the industry level

Input from critical industries will be crucial to understanding the most effective approach. Action to drive such behaviors would represent significant intervention on behalf of governments — tying in with efforts to drive ecosystem-wide active defense models to target cyber, fraud and organized-crime threat groups. For example, The UK National Cyber Security Centre's active defense program is now in its fourth year, offering a range of protective services to the UK public sector and beyond.

Industry input is key to ensuring that regulation of cyber third party assurance stays current, productive and advantageous to market ecosystems as a whole, ultimately ensuring buy-in from those they're seeking to protect. Our current approach to cyber third party assurance is no longer suited to today's bold new reality. This decade, regulators have an opportunity to embed an uncommon combination of resilience and agility into governance and to drive true efficiency enhancement.

Working together to evolve ecosystems

We need to consider methodologies that can better scope assessments, provide more continuous data and monitor those controls that are critical to the proper functioning of the service. However, KPMG's *Third party Risk Management Outlook 2020* report identified that only 26 percent of businesses believe they have all the data needed to carry out required assessments. In addition, 37 percent of respondents cited technical barriers, such as incompatible systems, as obstacles to sharing third party data across the enterprise.

The role of modern technologies

The new third party risk assessment model requires modern technologies that can ingest, process and learn from internal and vendor data and systems. Until the ecosystem starts to build security visibility, remediation and resiliency into our open-innovation model itself, it won't be easy to move at a speed necessary to solve these challenges. Fortunately, innovations in continuous controls monitoring, threat intelligence and machine learning have opened new doorways for businesses to address them.

Improved legal and regulatory frameworks

This new ecosystem driven cyber environment will likely require improved legal and regulatory frameworks that reduce agency considerations that often lead to lower visibility and increased liability. Several federal governments have started to break down silos hindering speed in cyber adoption and visibility. Building machine readability, shareability and risk-driven models into our assessments are also beginning to help.

Organizations should look to some of these models commercially and enable better ecosystem frameworks to support interoperability, reduced liability and lower regulatory hurdles to meet security objectives.

By working together, building a risk management, regulatory, privacy, resilience and technology framework, we can continue to evolve our ecosystems and reduce risk. We look forward to a new reality that allows much-needed innovation and progress to move at the speed of business.

How KPMG can help

At KPMG, our global organization of cyber security professionals offers a multidisciplinary view of risk. We help you carry security throughout your organization, so you can anticipate tomorrow, move faster and get an edge with secure and trusted technology.

No matter where you are on your cyber security journey, KPMG firms have expertise across the continuum — from the boardroom to the data center. In addition to assessing your cyber security and aligning it to your organization's priorities, we help you develop advanced solutions, implement them, monitor ongoing risks and help you respond effectively to cyber incidents.

KPMG brings an uncommon combination of deep technical expertise, strong business insights and creative professionals who can help you secure your third party relationships and realize the value of your third party security investments — positioning you to confidently grow your business. Together, let's create a trusted digital world, so we can push the limits of what's possible.



Our authors



Jonathan Dambrot
Global Third Party Security Leader
KPMG in the US



David Ferbrache
Global Head of Cyber Futures
KPMG



Orson Lucas
Principal, Cyber Security Services
KPMG in the US



Mark Thompson
Director, Cyber Security Services
KPMG in the UK



Rangana Guha
Director, Cyber Security Services
KPMG in the US



Pratiksha Doshi
Director, Cyber Security Services
KPMG in India



Jackie Hennessey
Director, Cyber Security Services
KPMG in Ireland



Sebastiaan Pronk
Manager, Cyber Security Services
KPMG in the UK

Contacts

Jonathan Dambrot
Global Third Party Security
Leader
KPMG in the US
E: jdambrot@kpmg.com

Gordon Archibald
KPMG Australia
E: garchibald@kpmg.com.au

Leandro Augusto M Antonio
KPMG in Brazil
E: lantonio@kpmg.com.br

Hartaj Nijjar
KPMG in Canada
E: hnijjar@kpmg.ca

Henry Shek
KPMG China
E: henry.shek@kpmg.com

Vincent Maret
KPMG in France
E: vmaret@kpmg.fr

Wilhelm Dolle
KPMG in Germany
E: wdolle@kpmg.com

Atul Gupta
KPMG in India
E: atulgupta@kpmg.com

Dani Michaux
KPMG in Ireland
E: dani.michaux@kpmg.ie

Luca Boselli
KPMG in Italy
E: lboselli@kpmg.it

Atsushi Taguchi
KPMG in Japan
E: atsushi.taguchi@jp.kpmg.com

Min Soo Kim
KPMG in Korea
E: mkim9@kr.kpmg.com

Rommel Garcia
KPMG in Mexico
E: rommelgarcia@kpmg.com.mx

Koos Walters
KPMG in the Netherlands
E: walters.koos@kpmg.nl

Daryl Pereira
KPMG in Singapore
E: darylpereira@kpmg.com.sg

Marc Martinez Marce
KPMG in Spain
E: marcmartinez@kpmg.es

Matthias Bossardt
KPMG in Switzerland
E: mbossardt@kpmg.com

Martin Tyley
KPMG in the UK
E: martin.tyley@KPMG.co.uk

Timothy Wood
KPMG in the Middle East
E: timothywood@kpmg.com

Kyle Kappel
KPMG in the US
E: kylekappel@kpmg.com

home.kpmg/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 on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit home.kpmg/governance.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, "we", "KPMG", "us" and "our" refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

Designed by Evalueserve.

Publication name: The extended enterprise — securing the future

Publication number: 137397-G

Publication date: April 2021