KPMG

Third-Party Security Service

KPMG Cybersecurity

KPMG China

kpmg.com/cn

Mitigating Third-Party Risk Is A Top Security Priority

Organizations across all industries are subject to increasing amounts of legislative, regulatory, and even their own internal corporate requirements to show they are appropriately managing and protecting not only their own organization's information, but their clients' information as well. As organizations enter and operate in new markets, they are likely to rely on third parties, many of whom operate in locations far from the organization's headquarters, and conduct business in a foreign language and with different local customs. As recent headlines continue to confirm, cyber-attacks are clearly growing in scale and incidents continue to be on the rise. As a result, regulators are making it a high priority for organizations to police such third-party relationships, and when something goes wrong, the penalties can be significant to the organization.

According to Forrest survey of security decision makers, third-party incidents were the cause of 17% of confirmed breaches in 2017 This highlights the cybersecurity posture of business partners and third parties as a crucial vulnerability In fact, 65% of security technology decision makers rated ensuring that their business partners and third parties comply with their internal security requirements as a high or critical priority.

Third-Party Security Challenges

Senior Management (e.g. Board of Directors, IT Management)

- What are the greatest risks brought into our organization through our third parties?
- How do we compare to other similar institutions?
- What could take our business down?
- How effective is our third-party oversight capability?

Chief Risk Officer

- Do we have a clear understanding of our risk posture as it relates to third parties?
- How do we measure progress in risk reduction due to improvement in our third parties' security controls?

Chief Information Security Officer

- How effective are our third parties' controls?
- Where are the third parties' high risk areas and how are they being remediated?
- Are we assessing our third parties to the extent necessary?
- What is our third parties' level of compliance to our policies, standards and regulatory requirements?
- How do we measure risk inherent to the use of these third parties?
- What compensating controls may I be asked to implement in order to reduce risk in certain third parties?

Office of General Counsel

- Are our third parties able to recover from issues arising from cyber security or internal breaches?
- Do our contracts include the appropriate level of protections against cyber security and data breaches?

The Third-Party Security Risk Management (TPSRM) Program focuses on seven primary areas of third-party management, each interconnected, and each incorporating security risk management throughout the third-party life cycle.

Source: 1. Forrester Analytics Global Business Technographics ®Security Survey

Third-Party Security Risk Management Program

Potential Benefits of a Third-Party Security Risk Management Program

Third-Party Selection

- Understand the inherent risks present in using the third party
- Understand the readiness of the third party to combat a cyber attack
- Gain actionable intelligence around the threats introduced to the business from third parties

Contract Negotiation

- Obtain clear definition of responsibility and liability in contractual obligations with third parties in the case of a data breach
- Obtain clear assignment of responsibilities for key cybersecurity control domains such as access administration, website security, DR/BCP, etc.

Ongoing Monitoring

- Validate the effectiveness of the third party's controls
- Understand the readiness of the third party to combat a cyber attack
- Gain actionable intelligence around the threats introduced to the business from third parties
- Gain awareness around how risk is being monitored, tracked and remediated

Termination of Third Party

- Gain confidence that sensitive data has been disposed of or archived appropriately, per contractual or policy standards

How KPMG Helps

Program Assessment

KPMG professionals perform an independent assessment of a client's existing Third-Party Security Risk Management Program and provides gaps against a generic Target Operating Model (TOM), which is based on leading industry practices, KPMG's experience with clients, and guidance found within industry regulations on managing third-party risk.

Program Developmentt

For clients, KPMG professionals can design and help the client implement a full lifecycle TPSRM program. The work can include developing supporting artifacts such as a TOM, third-party risk analysis scorecard model, and assessment questionnaires. KPMG professionals can develop the workflows and processes for conducting the security assessments, evaluating responses, weighting responses, and gathering third-party management responses

Global Assessment

KPMG professionals can stand up a KPMG Project Management Office (PMO) and deploy KPMG global assessment teams to conduct onsite security assessments. They will generate detailed reports specific to each third party, including recommendations for remediation and the third-party's scorecard based on client's risk ratings criteria. As part of the KPMG's PMO services, KPMG will provide logistics management, assessment status reporting, and risk reporting.

Remediation Oversight

After security assessments have been performed, KPMG professionals can provide on-going oversight of remediation progress by third parties clients. They can provide executive reporting to summarize analysis of assessment results across the third-party portfolio. KPMG professionals can also provide continuous improvement and alignment as business priorities and third-party partnerships change.

Contact us

Henry Shek
KPMG China
Cybersecurity
Partner
Tel: +852 2143 8799
henry.shek@kpmg.com

Richard Zhang
KPMG China
Cybersecurity
Partner
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

Quin Huang
KPMG China
Cybersecurity
Director
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

Danny Hao
KPMG China
Cybersecurity
Director
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

Brian Cheung
KPMG China
Cybersecurity
Director
Tel: +852 2847 5062
brian.cheung@kpmg.com

Frank Wu
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

Jason Song
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3306
jason.song@kpmg.com

Jason Li
KPMG China
Cybersecurity
Associate Director
Tel: +86 (10) 8508 5497
jz.li@kpmg.com

John Chiu
KPMG China
Cybersecurity
Associate Director
Tel: +852 2847 5096
john.chiu@kpmg.com

Kevin Zhou
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3149
kevin.wt.zhou@kpmg.com

Kevin Fan
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 2200
kc.fan@kpmg.com

Olive Wang
KPMG China
Cybersecurity
Associate Director
Tel: +86 (10) 8553 3630
oh.wang@kpmg.com

Andy Yuen
KPMG China
Cybersecurity
Associate Director
Tel: +852 3927 4697
andy.yuen@kpmg.com

William Xu
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 4633
william.q.xu@kpmg.com

kpmg.com/cn/socialmedia

For a list of KPMG China offices, please scan the QR code or visit our website:
https://home.kpmg.com/cn/en/home/about/offices.html