KPMG

Cybersecurity during Covid-19

Critical questions in supplier assurance

May 2020

During Covid-19, procurement and third party assurance teams face unprecedented change in the supply chain, with existing suppliers changing the way they operate and prioritize, and new suppliers being rapidly on-boarded to help keep operations flowing. How to adapt?

As pandemic containment measures escalate, insight into the operations and controls of suppliers can be a daunting task. Not only are existing suppliers adjusting how they work, potentially rendering previous risk assessments obsolete, but new suppliers are rapidly being on-boarded to plug supply chain gaps and provide redundancy during these uncertain times.

Traditional third party assurance processes can often be too cumbersome to adapt to the changing needs of the business, leaving them open to unknown risks.

To help tackle these challenges, here's a checklist of issues to consider.

What challenges are suppliers facing?

— Are operating models changing to adapt to the pandemic; if so are trade-offs in risk being made which could affect your business?

— Are services in high demand now or being used in ways not previously envisioned?

— Are suppliers facing cash flow and financial resilience challenges that may affect staffing and/or long term viability?

— Are the remote access capabilities secured?

— Are the acquired systems allows you to access your data safely?

Proactively reaching out to critical suppliers to understand how they are adapting operating models, can provide the insight needed to make key decisions.

How does that change suppliers' risk?

— What's the impact if suppliers don't meet service-level agreements (SLAs), or fail entirely?

— Are reviews needed of previous supplier risk ratings in the light of Covid-19 stresses on the supply chain and the changing business dependency on new and existing suppliers?

— What are the expectations of the local regulators in the Kingdome to evidence assurance and due diligence activities during the pandemic period?

How to get the needed assurance?

— Is there a view on the top cyber security and privacy risks that need focused attention in the short term for assurance purposes?

— Can new and existing suppliers be rapidly prioritized according to the urgency of their services, or the risk they pose by the nature of their services and the data they access?

— How can at least a limited degree of assurance be provided over the steps taken to manage cyber security (and privacy) risks?

— Can existing third party assurance processes be adapted to provide that assurance, if necessary, limiting dependence on on-site assessments?

— Is it possible to rely on assurance work done by peers or industry groups, or cyber security rating agencies for lower risk suppliers?

What are your organizations alternatives?

— What contingency plans are in place if a supplier is unable to continue providing services, or presents an unacceptable level of risk?

— Can procurement mechanisms adapt and provide a streamlined process if an alternate supplier is needed at short notice?

How have suppliers changed their working practices, and does it change their risk profile?

— What infrastructure changes have been made to allow for remote working? Is staff able to operate effectively and efficiently from their homes?

— How are they managing the secure provisioning and configuration of IT devices to staff? Have the security risks of working from home been assessed? What guidance has been provided to staff to address concerns?

— Have arrangements to deal with the potential insider threat and changed control environment associated with remote working been put in place?

— Has there been high staff turnover during this pandemic period? How are joiners, movers and leavers controls being managed, especially for third party contractors?

— How is compliance being monitored to secure working procedures?

What business continuity and disaster recovery arrangements have suppliers made?

— Are business continuity (BC) and disaster recovery (DR) plans in place to address remote working at scale and allow for potential infrastructure failures?

— Do BC/DR plans allow for disruption to data center and other key site operations due to travel limitations, site lockdown or major staff absences?

— How are security teams coping with the heightened cyber threat landscape?

— What incident response (IR) plans are in place to deal with the volume of new phishing and ransomware attacks? Do IR plans still work in the current environment, where on-site support may be affected?

What changes have suppliers made to their service delivery and infrastructure?

— What changes have been made to service or product delivery models? What approaches have been taken to security processes (securing DevOps) and handling of sensitive data in a remote working environment?

— How has service infrastructure scaled in relation to demand (either increased or reduced), including server / data center capacity, personnel availability and hardware?

— What effect do these have on agreed SLAs — can suppliers still guarantee the same level of controls over privileged access, data handling, response processes and use of break-glass procedures?

— How are suppliers managing the use of shadow IT in their organization — can they ensure data won't be transferred over insecure channels?

How confident are suppliers on their supply chain?

— What steps have been taken to gain assurance over their supply chain? Have they applied similar principles, as outlined here, to their supply chain risk assessment?

— Have mapping and contingency plans been made for any single point of failure or significant dependencies?

What happens in the worst case?

— What step-in rights does your organization have regarding any services provided, including access to key data required by the business?

How can we support each other to ensure it doesn't happen?

— How can the due diligence process be tailored to the supplier, making it as efficient as possible?

— How do we efficiently and effectively communicate mutual stresses and promote an open and transparent approach to supply chain management?

— Are there areas to support suppliers to improve resilience and reduce the risks to businesses?

— Are new ways of thinking needed to work together with suppliers and potentially with peers who also depend on supplier services?

Contacts

Tariq Dreiza
Head of Technology
KPMG in Saudi Arabia
E: tdreiza@kpmg.com
T: +966 55 388 9928

Ton Diemont
Head of Cybersecurity
KPMG in Saudi Arabia
E: antondiemont@kpmg.com
T: +966 56 860 8393

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

kpmg.com/sa

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 Al Fozan & Partners Certified Public Accountants, a registered company in the Kingdom of Saudi Arabia, and a non-partner member firm of the KPMG network of independent firms affiliated with KPMG International Cooperative, a Swiss entity. All rights reserved.