Re-assess supply chain security

Ensure operational continuity

KPMG Smart Government
Catalyse digital progress

Executive Summary

No government is immune from third-party risk.

Cyberattacks have become so commonplace they rarely shock us anymore. Perpetrators often use an organisation's third parties as points of entry to conduct these cyberattacks.

Almost 50,000 UK government ministers and civil servants were vulnerable to cyber-attacks until March 2020, because the Government Communication Service (GCS) website posted their personal information.[1]

Digital transformation is happening for all government departments, and the security of third-party systems that underpin that transformation determines risk, which can be huge. With such significant change in the landscape of digital, third-party security must be a preeminent consideration.

Knowledge is power—and the law

What government leaders and team members do not know about third parties can have a deep impact to their organisation.

National mandates require that government organisations appropriately manage and protect their own information as well as data for which they are stewards.

At the department level, these mandates extend to any third- party product or service.

The KPMG approach to prevent third-party breaches

Our four-step approach:

- **Program development.** Define and implement, or evaluate and enhance, your third-party risk management program.
- **Third-party assessments.** Evaluate ways of monitoring risk to align with program goals.
- **Control monitoring.** Identify continuous controls monitoring up front.
- **Risk reduction and failed control remediation.** Address third-party contractual security, operational requirements, and risk remediation.

[1] Alex Scroxton, "UK's Labour Party hit by third-party data breach," Computer weekly, November 3, 2021

Managing third-party risk with automation and AI

Cybersecurity threats show no sign of slowing down—in fact, they're getting smarter and more advanced. This means government departments must be proactive in monitoring and improving their third-party risk management to stay ahead of intensifying threats.

KPMG works with government clients using a risk-based approach that provides intelligence to help proactively manage third parties and minimise risk.

Our method helps organisations:

- Connect enterprise applications and analytical engineering with a user-friendly front end as a holistic interface between operations, security, compliance, and the third party
- Manage risk using advanced analytics and standard third-party assessments
- Use automation and AI to automate less complex tasks and identify any behaviour outside of scope with third parties
- Track contracts with visibility into security provisions and data sharing
- Gain visibility into third-party environments across regions, languages, and assessors
- Accelerate digital transformation as a solution framework that delivers, teaches, and elevates organisations to transform into a human-accelerated, AI-enabled organisation

Breaking down the numbers

97%

of 300 UK respondents suffered a cybersecurity breach because of weaknesses in their supply chain or third-party vendors in the past 12 months, in 2021[2]

25.8%

rise over the previous year in average number of breaches experienced over the past 12 months (from 2.6 to 3.5)[2]

Only 57%

of large UK companies have cybersecurity incident response processes in place[3]

A ransomware attack on the Irish Health Service Executive (HSE) accessed sensitive information of

520 Patients[4]

34%

of remote UK employees admitted to using their work gadgets for personal purposes[5]

[2] "Managing Cyber Risk Across the Extended Vendor Ecosystem (UK)," BlueVoyant, December, 2021

[3] Dan Swinhoe, "UK cybersecurity statistics you need to know," CSO, May 6 2020

[4] Lindsay Ward, "Ireland's Health Service Executive ransomware attack (2021)," Cyber law, May 13, 2021

[5] Sandra Vogel, "What are employers' responsibilities when we use personal tech to work from home?," IT Pro, January 25, 2021

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

kpmg.com/uk

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 endeavour 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.

CREATE | CRT145789B | May 2023

Document Classification: KPMG Public