Re-assess supply chain security

Ensure operational continuity

KPMG Smart Government

Catalyse digital progress

Insight Briefing

No government organisation is immune from third-party risk

Cyberattacks have become so common we are almost numb to the news headlines. A 2021 study found that, **of the 300 UK respondents, 97 percent suffered a cybersecurity breach** because of weaknesses in their supply chain or third-party vendors in the past 12 months. The average number of breaches experienced over the past 12 months increased somewhat from the previous year (from 2.6 to 3.5), a 25.8 percent rise over the previous year.[1] 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.[2] A cyberattack on a third-party data processor resulted in the compromise of data on UK's Labour Party members.[3]

Government organisations, citizens, and employees reap uncountable benefits from digital transformation, but these benefits can come with risk. Organisations rely on third-party tools to add new digital capabilities. Only 57 percent of large UK companies have cybersecurity incident response processes in place.[4] Sometimes these tools open a door to allow cyberattacks. Threats are more frequent and breaches are larger in scope making it a priority for central and local governments to **tighten third-party selection due diligence processes.** This article covers methods that **use automation and artificial intelligence (AI) to lower risk of attacks** via third parties.

Why smart government is important

Government organisations and departments around the world should modernise in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders involved in government modernisation are reviewing their user's experiences to plan what upgrades are needed in their business processes and service delivery models.

This article is one of a series that features how modernising can affect the government workforce and the user experience, improve security and public trust, and accelerate the digital journey. KPMG offers insights intended to help guide governments and public sector organisations in their modernisation efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organisations.

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

[2] "IOTW: Almost 50,000 UK government ministers vulnerable to cyber attacks", Olivia Powell, Cyber security hub, 2023.

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

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

Knowledge is power to prevent third-party-related breaches

Ignorance is not a defence. What government leaders and team members do not know about **third parties** can have a deep and negative impact on their organisation. Regulatory mandates require that government organisations appropriately manage and protect their own information as well as data for which they are stewards. At the departmental level, these **mandates extend to any third-party product or service.**

The UK government has a new executive order that lays out its plan to improve the nation's cybersecurity, including steps departments must take. **Third parties supporting government departments will have to meet requirements** including cybersecurity incident reporting, cloud security principles, and using data encryption and multifactor authentication.[5] The National Offensive Cyber Programme and the National Cyber Force (NCF) were two recent examples of the UK government's major investments in its offensive cyber capabilities. The NCF united personnel from the Government Communications Headquarters (GCHQ), the Ministry of Defense (MOD), and more departments under a single overarching command.[6]

Some **regions are lowering their risk exposure** after constant cyber threats across the industry. For example, in May 2021, a ransomware attack on the Irish Health Service Executive (HSE) accessed sensitive information of 520 patients. After the incident, the HSE declared it would open a cyber security operations center to keep an eye on its networks and put in place a thorough procurement procedure for the building.[7]

With or without laws or regulations, every government organisation needs an active **third-party risk management strategy and program** to evaluate and monitor for risks before, during, and after contracts are in place. We recommend the following critical steps:

Program development: Define and implement, or evaluate and enhance, your third-party risk management program. Segment third parties by which are critical and potentially high risk. Identify which vendors have access to your organisation's critical data, where they store your data, and how they protect it.

Third-party assessments: Take a tailored approach based on the risk profile of the third-parties you are working with as well as ensuring there is a structured approach around exiting third parties when required.

Control monitoring: Look at how continuous controls monitoring can enhance traditional methods.. Tailor the assessment requirements based on the risk profile of the third party.

Risk reduction and failed control remediation: Address third-party contractual security, operational requirements, and risk remediation.

[5] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021.

[6] "Cyber Security Breaches Survey 2022," GOV.UK, July 11, 2022.

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

Third-party risk management can be proactive with automation and AI

Cybersecurity threats will likely not subside, especially considering government organisations' growing reliance on third parties. This means central and local governments must depend on effective **third-party risk management to stay ahead of the intensifying threats.**

KPMG works with government clients using a risk-based approach that provides intelligence to help proactively manage third parties and mitigate risk. The technology-agnostic approach uses AI analytics and engineering as well as AI principles across the third-party security process lifecycle. AI and automation enhance the ability to **identify, evaluate, and respond to threats.** Our method helps organisations:

- **Connect enterprise applications and data** such as contract management and procurement 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:
  - Our third-party security programme assessment and benchmarking service uses standards and security models. These help organisations assess third-party security readiness against peer organisations and recommend improvements.
  - Users can test security program components in our third-party security lab's interactive simulation.
  - Our team helps streamline and automate processes. They use an assessment framework that runs large-scale third-party security assessments in a smarter way and helps organisation leaders realise the value of the managed service.
- **Use automation and AI** to automate less complex tasks such as managing security assessments and add intelligence about each third party, their behaviours, and when they perform actions outside of approved services. Machine learning picks up behaviours from human interaction and also verifies and correlates data in real-time against the organisation's tolerance levels.
- **Track contracts** with visibility into security provisions and data sharing included in them.
- **Gain visibility into third-party environments** across regions, languages, and assessors. Clients have near- real-time visibility into their third parties' security posture with continuous monitoring and assessment that enables a risk remediation culture.
- **Accelerate digital transformation** as a solution framework that delivers, teaches, and elevates organisations to move from a human-powered cyber workforce to a human-accelerated, AI-enabled organisation.

Our third-party risk management approach includes these steps and outcomes:

Identify
Rationalise third-party database; eliminate duplicate entries

Assess
Fast-track assessments and identify priorities and changes in approved services

Evaluate
Present a holistic third-party view across assessors and departments

Recommend
Predict and challenge inherent, residual risks based on historical data

Integrate
Connect enterprise applications for big-picture visibility

Communicate
Deliver consistent, automated messaging across channels and departments

Building resilience in your third-party network

Central and local governments are all targets, and the rise in remote working adds significant risk. In the UK, 34 percent of remote employees admitted to using their work gadgets for personal purposes, 64 percent of whom checked their personal emails and 60 percent of whom admitted to conducting online shopping.[8] Thorough **assessments and continuous monitoring** powered by **automation and AI-powered third-party risk management is the best defence.**

Better cybersecurity can improve trust. One study found 68 percent of UK citizens do not trust their government in terms of personal data management.[9] This response is not a surprise since central governments are usually larger targets. For example, data from the October 2020 attack on Hackney Council was leaked by the Pysa ransomware. It contained personally identifiable information, such as scans of tenancy audit records for occupants of public housing, staff data, and details on community safety, among other things.[10]

Some central and local governments are boosting their cybersecurity legislation and activities to prevent data breaches and ransomware.[11] Private information obtained from fourteen UK schools was posted on the dark web by the ransomware group Vice Society. The leaked information included details on special education requirements, passport scans of students, and staff pay scales going back more than 10 years.[12]

The results of security assessments with continuous monitoring can offer government leaders a **comprehensive, real-time view of their third parties' readiness** to prevent, detect, contain, and respond to information security threats such as these. Whether an organisation is developing or building a program or starting to explore AI and machine learning to enhance it, KPMG third-party risk management government professionals can help.

Outsmart the hackers with indestructible third-party risk management

In a world that becomes more digital each day, risks that your organisation will be hit with a cyberattack grow exponentially, and odds are the attack will involve a third party. Companies and organisations across all industries, including government, seek to lower risk by performing due diligence on any third-party company with whom they work. You have the power to save your central and local organisation's time, money, and reputation by better managing third-party risk across operations.

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

[9] "Most British people don't trust government with personal data," ComputerWeekly.com, Jan 7, 2021.

[10] Alex Scroxton, "Annual costs of Hackney ransomware attack exceed £12m," Computer weekly, October 14, 2022.

[11] Matthew Hodson, "Increased Cybersecurity Mandates Coming for State and Local Governments," Security Magazine, June 11, 2021.

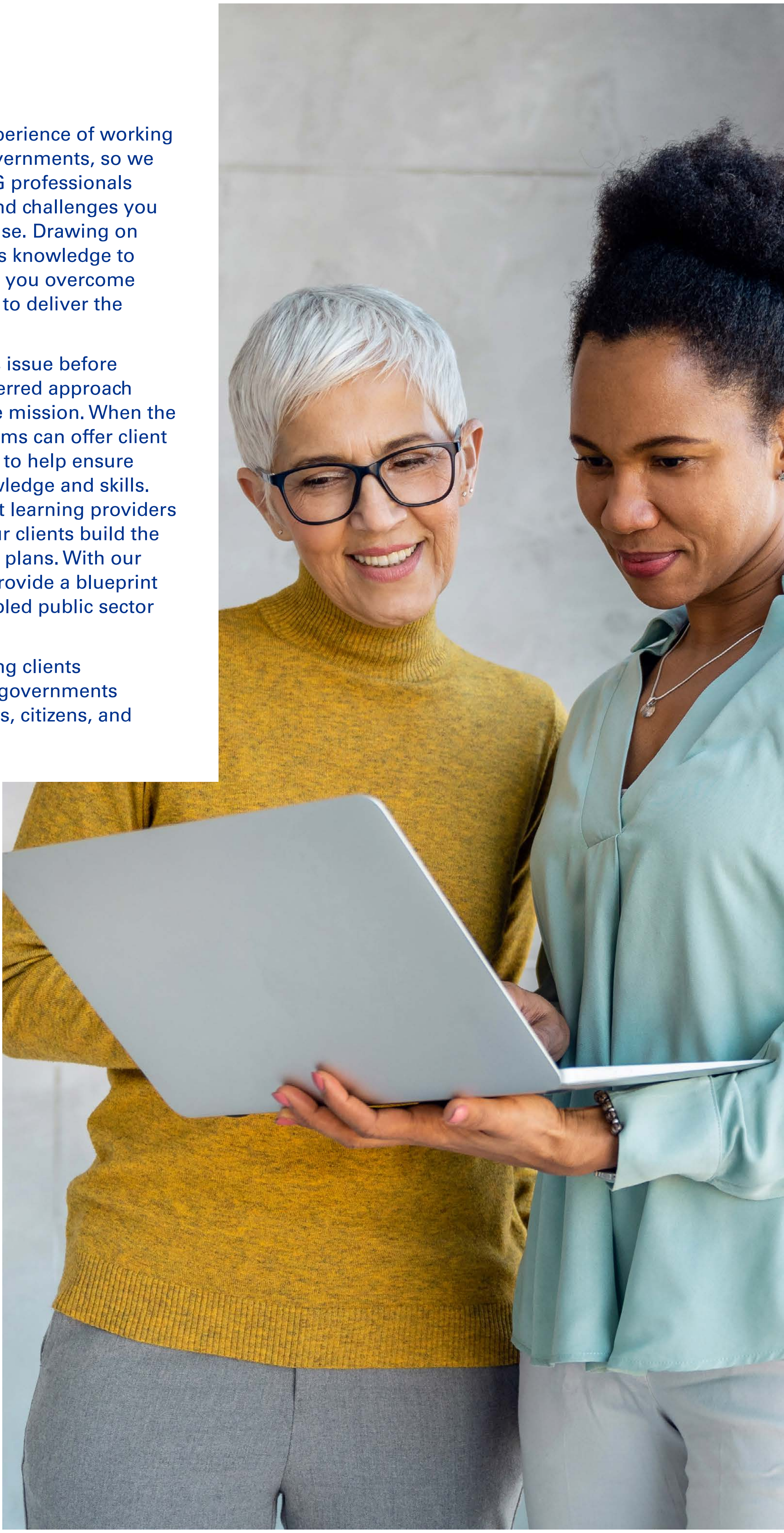
[12] Evie Coffey, "Devon school hit by cyber attack as highly confidential documents leaked," Devon live, January 6, 2023.

About KPMG

KPMG firms have many years of experience of working with national, regional and local governments, so we know how departments work. KPMG professionals understand the issues, pressures, and challenges you encounter in the journey to modernise. Drawing on KPMG firms' government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you to deliver the results that matter.

KPMG teams start with the business issue before we help clients determine their preferred approach because we understand the ultimate mission. When the way people work changes, KPMG firms can offer client insight on leading training practices to help ensure your employees have the right knowledge and skills. KPMG in the UK is one of the largest learning providers in Europe, specialising in helping our clients build the skills and talent they need for future plans. With our Powered Government offering we provide a blueprint for a customer centric, digitally enabled public sector organisation.

KPMG firms are committed to helping clients create value, inspire trust, and help governments deliver better experiences to workers, citizens, and communities.



Contact

Nicholas Fox

Partner, Head of Government (Justice)

KPMG in the UK

Laura Webb

Partner, Public Services Technology Transformation

KPMG in the UK

Richard Krishnan

Partner, Technology and Cyber Risk

KPMG in the UK

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 | June 2023

Document Classification: KPMG Public