Re-enforce digital security

Develop the integrated security to reduce risks

KPMG Smart Government
Catalyse digital progress

Insight Briefing

People and data are no longer confined to physical, specific places. We're working in more agile ways using remote systems to store personally identifiable information. In this modern world without perimeters, cybersecurity becomes a more complex issue.

Lack of perimeter leaves cyber vulnerabilities

The recent ransomware attack on one of the UK Government's widely used outsourcer by Black Basta has shown the devastation that can be caused without the right security measures in place. This attack is currently estimated to cost the outsourcer £15-£20M and that figure will continue to rise[1]. It's not just the attack on the outsourcer though, it's the impact this will cause on people's personal lives with the data that will be exposed and made public.

In 2020, there were more than 29,000 cybersecurity incidents across the globe, with at least 3,236 of those in the public sector.[2] 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]

People and data are no longer within the walls of specific places leaving traditional data security methods ineffective. In environments with no perimeters, cybersecurity has to be more flexible and agile to protect data, networks, workloads, and user identities as users interact in cloud, mobile, on premise, and remote environments. This article introduces zero-trust as a powerful architecture to improve governments' cybersecurity. We present the zero-trust framework in ways that can be useful to technical leaders as well as program and financial managers.

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] ComputerWeekly.com, Black Bast ransomware attack to cost Capita over £15m, 10th May 2023
[2] "Global number of cyber security incidents in 2020, sorted by victim industry and organizat ion size," Statista, 2021.
[3] "IOTW: Almost 50,000 UK government ministers vulnerable to cyber attacks", Olivia Powell, Cyber security hub, 2023.

It is not a product. Zero-trust is a framework or model to trust nothing and verify everything.

Rethink cybersecurity for digital, no-boundary environments

Governments accelerated their digital transformation efforts in 2020, which amplified the need to rethink cybersecurity. However, only 48 percent of government leaders surveyed were using cybersecurity technologies and services to enable their organisation's digital transformation.[4] For the period between Jan 2021 - 2023 overall IT and digital spend by the UK Government was £13.6bn with cyber related contracts being 13% of that spend. There are then varying amounts of investment per department with some investing up to £7m during that period whilst others only invested £5,000 so there needs to be more consistency to ensure the protection is there[5]. As government organisations move more data and applications to the cloud and environments become more dynamic, they must rethink cybersecurity. Zero-trust is an approach to cybersecurity and risk management that government organisations can build to safeguard the environment no matter where data and people are located. It is not a product. Zero-trust is a framework or model to trust nothing and verify everything.

A **zero-trust framework shifts cybersecurity defence focus from network-based, static perimeters to protect users, assets, and resources**. It requires stringent security validation with no implicit trust based on users or locations. For example, if an employee loses their mobile device, zero-trust would provide the capability to know the person who picked up the device does not hold or type on it the way the owner does. When this happens, technology broadcasts the information to the security operations center where humans, with help from technology, assess the situation in real-time and terminate the session.

Adopting a zero-trust framework can achieve a number of valuable benefits that apply no matter where government workers, data, citizens, and other constituents are or what devices or networks they use. Benefits may include improving threat detection, minimising data loss, and lowering risk. Zero-trust also helps organisations enforce security policies and prepare for what might happen next. Most importantly, **zero-trust helps governments maintain public trust.**

Since cyber threats can originate anywhere, we cannot trust the user's **identity,** the **device,** the network, or the **data**. Under a zero-trust architecture, technology spots atypical activity and prevents communication with unauthorised apps, servers, locations, accounts, or human behaviors. These four main components make up a zero-trust framework:

Strong **identity management** employs authentication and user rights to help ensure access only to authorised people. Zero-trust capabilities many government organisations already use are role-based access control, multi-factor authentication, and access where each user or device is granted the minimum system resources to perform its function.

Zero-trust also depends on a mobile **device/workload** management strategy that includes application programming, interface security, and frequent security updates as well as an accurate, detailed workforce device inventory. There is a concentrated risk of single outsourcers to multiple government departments that can be mitigated through a zero-trust framework. There is also an additional risk with the extension of the risk into third parties that sub contract (4th parties). The entire supply chain needs to be secured, including companies, products, and services.

Zero-trust **protects networks** while devices are connected with a software-defined perimeter service. Microvirtualisation provides application-level isolation from the operating system and microsegmentation divides the network and reduces the number of users per network segment. It also maintains cyber visibility into containers and encrypted traffic.

Data security encompasses properly implementing a wide range of technologies and software, including data loss prevention tools and processes, file integrity monitoring, and encryption. Cloud access security broker software resides between users and cloud applications. It monitors activity and enforces security policies to protect data stored in the cloud.

The UK incorporated Zero Trust as a part of their guidance and advice to UK organisations. The government is increasing the cyber resilience of companies in all industries by promoting and enforcing the urgent implementation of this strategy[6]. Looking at government organisations' cybersecurity from a zero-trust perspective may be the approach they need.

[4] "Impacts of COVID-19 on digital transformation strategies and the future of work," KPMG and Forrester, 2020.
[5] Tussell Database, contracts related to ‚IT and Digital' and ‚Cyber')
[6] "Will Rishi Sunak reassess UK cybersecurity policies?" Open Access Government, November 21, 2022.

Zero-trust is a multi-step process you may have already started

Achieving zero-trust across the digital experience is an art and a science. Citizens need easy access to services. They are not technologists, so it is up to government organisations to assure data and each interaction across the digital experience is secure, which is the science. The art is in providing an experience that is easy and seamless.

Installing an app does not achieve zero-trust, no matter what some software vendors might claim. Designing a zero-trust framework is a multi-step, ongoing process that uses a number of components and, similar to puzzle pieces, each component must fit to create a cohesive cybersecurity environment. The good news is many organisations already have pieces of zero-trust already in place. Multi-factor authentication is a good example. The difference is each piece exists because the organisation needs the function, but they are discrete. Now you want a **cohesive framework or architecture designed to trust nothing and verify everything. This is zero-trust.**

Planning for an incremental and in-sequence, step-by-step rollout heightens success and can help secure the needed funding. There are tools available for organisation to be able to give a comprehensive view of the potential financial losses in the event of a cyber attack as well as the best investments to help mitigate those attacks. These tools allow you to make defensible and data-driven decisions and can help you prioritise your remediation efforts. Organisations must **take all of the following actions to adopt zero-trust:**[7]

01 **Establish strong data governance.** Leading organisations understand cybersecurity risks, seek resources to address vulnerabilities, and make risk-based decisions regarding resource allocation. They adopt an enterprise approach that incorporates technology offices such as the chief information officer and also program and functional offices, including personnel and procurement. They prioritise information requiring highest protection levels such as citizens' personally identifiable information (PII) or sensitive government mission data.

02 **Protect the most critical data.** Assign each data breach category a rating of high, medium, or low importance, with the overall data set receiving the highest rating in any category. The department's cybersecurity team should use this classification to select the necessary cybersecurity controls. Collaboration is important to establish enterprise wide cybersecurity priorities that balance risks, impacts, costs, and benefits. Leading organisations focus on mission-critical systems and information.[8]

Each data category requires certain controls, augmented by targeted and compensating controls tailored to specific cybersecurity risks. For example, misuse of accounts with elevated access rights is one of today's biggest cybersecurity threats. While a common control is to limit access to sensitive PII data to certain personnel, categorising data appropriately so it resides in specific systems within the organisation strengthens control. A cost-effective approach is the principle of least privilege.[9]

03 **Deploy a multi-cloud strategy.** In a multi-cloud strategy, organisations use more than one cloud service provider to flexibly align services and capabilities to meet needs. As they move more data to the cloud and increase remote usage, relying on a single cloud service provider may not be enough to meet demands and

[7] Tony Hubbard, Joseph F. KI imavicz, Steve Wong, Jeffrey C. Steinhoff, "Zero-trust in a Virtual Cybersecurity World," Journal of Government Financial Management, Summer 2021.
[8] "Crown Jewels Analysis," MITRE Systems Engineering Guide, p. 167, 2014.
[9] "Cloud Threat Report 2020: Addressing Security Considerations Amidst a State of Constant Change," Oracle and KPMG LLP, research conducted in partnership with ESG, 2020.

provide adequate cybersecurity coverage.[10] In a 2020 survey of 300 public sector organisations across UK, 85.5 percent of respondents said they would "prefer a multi-cloud vendor".

Distributing workloads among different cloud service providers broadens an organisation's security scope by increasing cloud availability to mission-critical applications. A multi-cloud strategy can reduce service disruptions and failures with readily available backup solutions. In addition, organisations can choose the optimal solution in a given situation and assess the cost/benefit among possible solutions and returns on investment based on pricing models.

Organisations can increase agility and reduce costs by reusing existing infrastructure, especially with a cloud-native application. Cloud-native technologies provide the capability to build and run scalable applications in modern, dynamic environments, such as public, private, and hybrid clouds. Combined with advanced technology such as machine learning, they allow developers to create high and impact changes frequently and predictably with minimal effort, saving time and money.

04 **Assign cloud gatekeepers.** Organisations can use cloud access security brokers as cloud gatekeepers to oversee information and threat protection from malicious attackers, even beyond the government customer's network perimeter.[12] These cloud-based security solutions can help enforce cybersecurity policies and regulations and mitigate or eliminate risks of attackers targeting cloud blind spots. Departments also increase assurance of data safety and better control activities throughout their network.

05 **Establish accountability.** Understanding data assets is critical to personal and organisational accountability. It is important to not only implement effective, efficient network controls, but also monitor their use and maintain their effectiveness. Leading organisations continually probe and test cybersecurity capabilities through simulations that attack the data, applications, and services constituting their priority data. They also overlay advanced analytics to automate and discover deeper process insights.

Accountability includes the wise use of resources. Implementing a zero-trust architecture need not be costly. Repurposing existing cyber tools and capabilities to their fullest potential unlocks significant cost savings and enhances cybersecurity. Identifying effective cyber technologies and leading private and public sector practices foster new and improved cybersecurity approaches. Greater effectiveness and efficiency increase performance and save resources by reducing vulnerability to and the impact of cybersecurity attacks.

06 **Foster a cybersecurity mindset.** All organisations and all employees should participate in strengthening cybersecurity. Leading organisations cascade responsibility so all personnel understand the importance of data protection and their specific roles.[13] Routine "cybersecurity hygiene" is invaluable, along with a top-down, bottom-up collective cybersecurity effort by the entire workforce. Top management must be cybersecurity champions, prioritising it in resource allocation and decision-making.[15] In November 2022, the UK's National Cyber Security Centre introduced a new program that continuously checks every internet-connected device hosted in the UK for vulnerabilities to aid the government in defending against zero-day threats.

07 **Cyber Incident Response.** Organisations need to consider integrating a formal response to threats from cyber attacks by integrating this into their business continuity and disaster recovery plans. This has been highlighted as a strategic importance within the government's rerecent Resilience Strategy.

Cybersecurity regulations, malicious actors, acts of nature, and accidents will not slow down while governments ponder their next cybersecurity steps. Start planning or continue your zero-trust architecture implementation now so your organisation is more prepared for what might happen next.

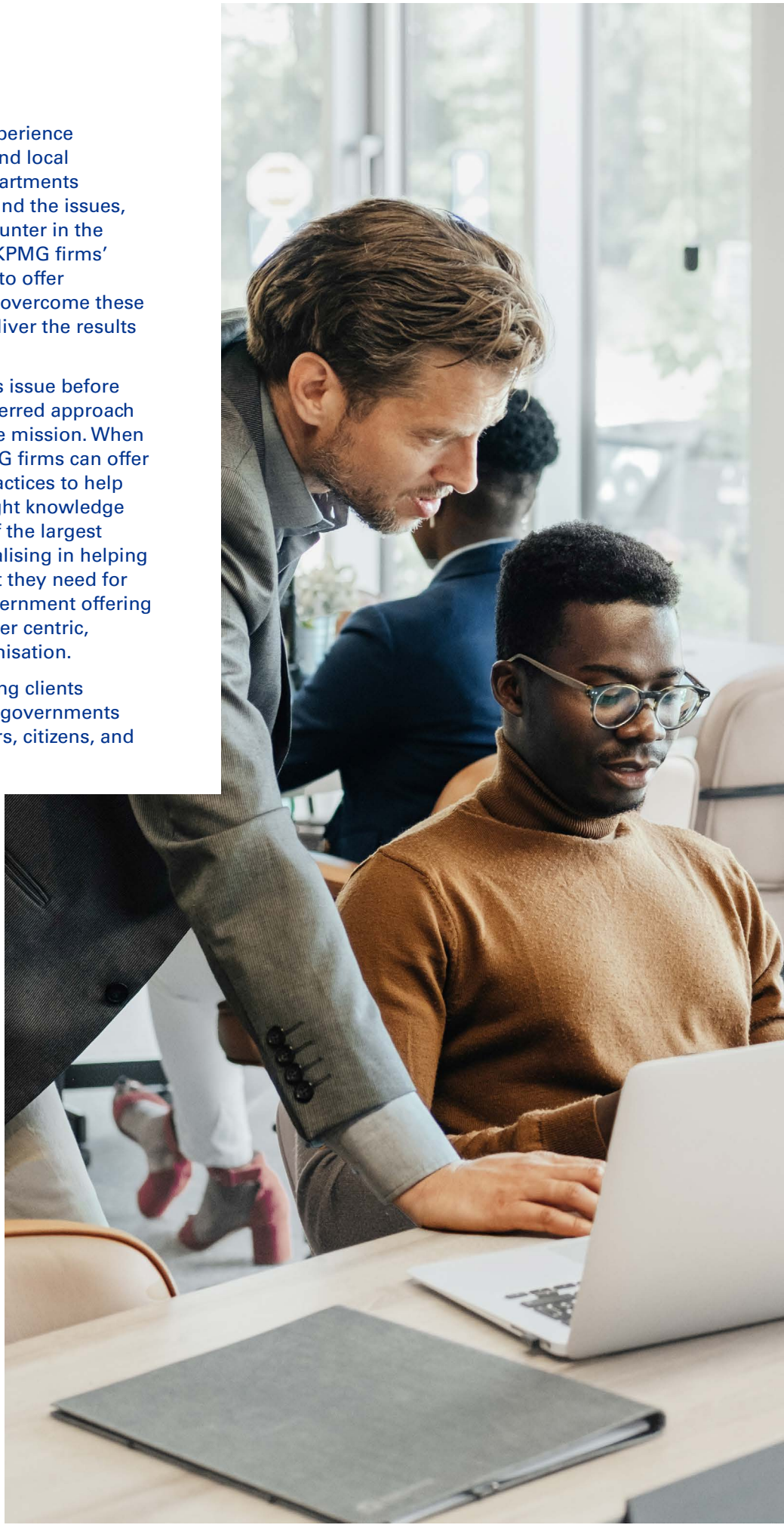
[10] "Agile cybersecurity — by design — for threat-resistant government agencies — The road to new reality for US public sector," KPMG LLP, Fall 2020.
[11] Priya Emmanuel and Paul Glunt, "The sky's the limit for cloud value, but you need a future-ready plan — Have your cloud migration and modernisation efforts stalled? New approaches can help maximize value,"KPMG LLP, US. December 2020.
[12] Microsoft Corporation, "Top 20 Use Cases for CASBs." Microsoft Cloud App Security, 2019.
[13] Tony Hubbard, Geoffrey Weber, and Jeffrey Steinhoff, "Protecting Data Assets in a Perilous Cyber World" Journal of Government Financial Management, Fall 2017.
[15] Tony Hubbard, Jennifer Fabius, and Jeffrey Steinhoff, "Harnessing and Protecting Data Assets," Journal of Government Financial Management, Winter 2018–2019.
[16] "UK government is scanning British internet space for zero-day threats," Tech Crunch, November 7, 2022.
[17] Resilience Strategy - Call for Evidence.pdf (publishing.service.gov.uk) 2021 organisations

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

CREATE | CRT145789B | May 2023

Document Classification: KPMG Public