Re-engineer digital experiences

Embed the resilience to evolve innovation

KPMG Smart Government
Catalyse digital progress

Executive Summary

Not if, but when

For governments, securing the digital experience is nothing new. But as many organisations race to provide the ultimate seamless digital experience, security is often an afterthought.

The ways in which locations, credit cards, and other personally identifying information are leveraged for experience mean security is a very serious issue — it must be built into the initial vision of the citizen digital experience.

Threats have changed

Government workers must view security efforts as one of the most critical pieces of the citizen experience. As technology continues to advance, new threat vectors are creating advanced threats to the security of the citizen. In addition, new ways of working require new security approaches, and government departments must in turn proactively evolve their security systems.

Around 21 million malicious emails to NHS trusts are blocked every month by NHS England's Cyber Security Operations Centre (CSOC). It also provides real-time protection of any suspicious activity to approximately 1.7 million devices across the NHS network.

Modern vulnerabilities include:

- Perimeters to protect no longer have boundaries — work from home and other factors have created environments that are borderless
- Data quickly moving to cloud environments
- Dramatic increases in quantity and scope of cyber threats including phishing, ransomware, and via third-party software and tools
- Pervasive use of mobile apps and self-service technologies
- Generative AI - with the rise of tools such as ChatGPT the possibility of misuse and risks are high

Securing digital experiences

Only 40 percent of UK citizens trust in the government to use data safely, effectively, transparently and with accountability. Governments are responsible for ensuring security both in the cloud and across the entire digital experience.

Cloud-based solutions have seen rapid adoption in recent years, meaning a secure cloud strategy is no longer a nice-to-have.

We recommend:

- Regularly stress test possible incidents to prove the response plan works for cloud-based applications
- Automate early stages of incident response procedures
- Collaborate with departments outside the security team to learn how threat actors think and ways to spot attacks early

"Public attitudes to data and AI: Tracker survey" Gov.UK, November 2, 2022.
"Government sets out strategy to protect NHS from cyber attacks:, Gov.UK, March 22, 2023

Shared responsibility security model

It is the shared responsibility of the government and the service provider to create a secure cloud footprint.

Best practice:

- Practice a modern third-party risk strategy
- Provide citizens an easy-to-use digital storefront secured with multi-factor authentication
- Upskill or hire employees with digital capabilities
- Provide employees with secure networks and devices
- Do not ask for unnecessary personal or private information

Employees are daily digital experience stewards

Government employees must be continually upskilled and trained in modern day-to-day security measures. From identifying phishing emails to using multi-factor authentication, colleagues must be trained to be aware at all times.

Security needs will continue to evolve

As experiences evolve and citizen demands for a seamless experience grow, government departments must keep their finger on the pulse of emerging ways to secure their systems and implement modern systems as they arise.

- Customer Responsibility
- Cloud Service Provider Responsibility

On-premises	**IaaS** (Infrastructure-as-a-Service)	**PaaS** (Platform-as-a-Service)	**SaaS** (Software-as-a-Service)
User Access/ Identity	User Access/ Identity	User Access/ Identity	User Access/ Identity
Data	Data	Data	Data
Application	Application	Application	Application
Guest OS	Guest OS	Guest OS	Guest OS
Visualisation	Visualisation	Visualisation	Visualisation
Network	Network	Network	Network
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

KPMG and Oracle, research conducted in partnership with ESG, 2020.

Breaking down the numbers in the UK

Only **40%** of UK citizens trust in the government to use data safely, effectively, transparently and with accountability.

£2.6 billion

will be spent to build a resilient digital environment by the UK government from 2021 to 2024

"Public attitudes to data and AI: Tracker survey" Gov.UK, November 2, 2022.

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