BAE SYSTEMS

Cybersecurity: A Help or Hinderance to Public Sector Digital Transformation?

Introduction

The UK Government continues to be a global leader in digital transformation. With the launch of the Government Digital Service (GDS) a decade ago, it was one of the first to realise that effective IT modernisation is the key to streamlining processes, reducing costs and delivering better public services. In October 2020 it was ranked second globally by the OECD.[1]

The pandemic has seen the UK Government further flex its digital muscles. Some results have been impressive: UK Government departments delivered 69 new digital services by the end of May 2020, with many more in the pipeline—all while many civil servants were working from home.[2] The Coronavirus Job Retention Scheme (CJRS) was designed, built and launched in less than five weeks and achieved customer satisfaction scores of over 90%.[3]

The Institute for Government claims that these results were borne out of large and talented teams of digital staff, pre-existing tools which could be rapidly repurposed and agile development methodologies.

Yet despite this headline progress in digital transformation, government IT remains heterogeneous. And where there are expanses of legacy technology systems, this can create major cyber risk. To find out more, BAE Systems Applied Intelligence recently commissioned Sapio Research to poll 250 managers with IT responsibility in UK Government departments.

We found that, while the cyber security function itself can often be a major barrier to IT modernisation projects, security concerns are also a major driver for such upgrades.

The drive to modernise government IT

We found that an estimated 60% of UK Government departments have an IT modernisation strategy in place. This could include anything from upgrading desktop estates to migrating key back-end systems to the cloud. Further, most (84%) respondents said their IT modernisation plans had accelerated due to COVID-19.

Why are they doing this? The majority of respondents (63%) pointed to legacy IT limiting business productivity and their ability to manage their IT estates. It's true that visibility and control are easier with connected, intelligent digital systems. On the other hand, legacy apps are often bespoke, limited in functionality and require specialist knowledge locked away in a small subset of workers.

Despite recent advances, government IT still lacks the agility and operational efficiencies that many private sector organisations can boast. Around a third of respondents (32%) also claimed that this is limiting the quality of public services they're able to offer and their ability to collaborate and innovate internally. It may also impact government's ability to attract and retain the brightest and best talent.

Whilst the above are perhaps not unsurprising reasons for modernisation, cyber security concerns are also a major driver for change. Vulnerabilities were cited by 75% as the reason for legacy upgrades, second only to performance improvements (76%). Just over half (53%) also pointed to poor integration between legacy IT and modern security solutions as their top data protection risk.

60%

of UK Government departments have an IT modernisation strategy in place

63%

of respondents pointed to legacy IT limiting business productivity and their ability to manage their IT estates

32%

of respondents claimed that this is limiting the quality of public services they're able to offer and their ability to collaborate and innovate internally

75%

cited vulnerabilities as the reason for legacy upgrades

Why cyber matters

Incidents such as the large-scale SolarWinds campaign against multiple US Government departments have highlighted the growing and increasingly sophisticated threat from hostile nations.[4] More recent still, the exploitation of multiple zero-day vulnerabilities in on-premises Microsoft Exchange Server customers perfectly illustrates the challenge of running legacy technology. Although this started with a few targeted and likely state-sponsored intrusions, just days later multiple APT actors were also exploiting the same flaws to remotely hijack hundreds of thousands of endpoints around the world.[5]

It's already having a negative real-world impact on the public sector: nearly two-thirds (63%) of respondents said they experienced a security incident in the past six months and over half of these (52%) came as a result of missing patches. The bad news is that, the majority of vulnerabilities recorded by the US authorities in 2020 were "low complexity" (63%), meaning an attacker with low technical skills could exploit them, and required no user interaction to exploit (68%).[6]

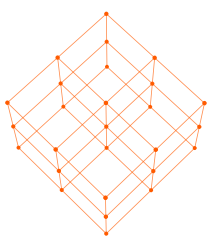
Cybersecurity in the UK is not only viewed as a top driver for IT modernisation but also one of the biggest barriers to infrastructure upgrades (68%), second only to integration issues (69%). If anything, the rapid response to the pandemic has proven that red tape can be circumvented and fast-track processes invoked if the need is urgent enough. Senior decision makers are both more aware of the threat, and impact, of cyber security attacks, and of the need to balance the variety of risks including security and business operations. This can only be enabled through greater awareness at all levels of the organisation, and a more coherent and collaborative perspective from IT and cyber security teams.

63%

of respondents said they experienced a security incident in the past six months

68%

of attackers with low technical skills could exploit low complex vulnerabilities



68%

view cyber security as a top driver for IT modernisation but also one of the biggest barriers to infrastructure upgrades

The future of government IT

So what happens next? We found that respondents say that technology (44%) will be the main focus for cybersecurity improvements, rather than matters of investment, strategy or training. Public sector IT leaders want to start by simplifying their security architecture (45%) — by investing in new technologies and/or vendor consolidation. This would certainly help to cut through the complexity which can hinder effective cybersecurity. A 2020 report claimed that global organisations run an average of 43 discrete security and operations tools to manage their IT environments.[7]

The transition to modern digital technologies, if they are engineered appropriately, affords opportunities to raise the level of security and make use of innate tooling to make security architecture more manageable and integrated in IT development.

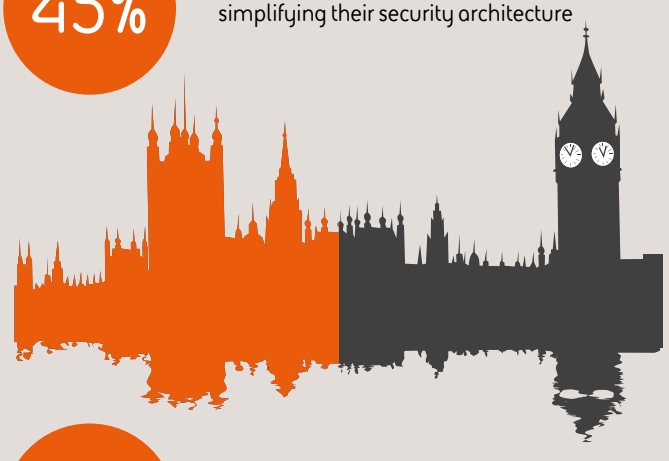
Similar numbers (45%) want to review current cyber risk management strategies to ensure they have the right balance between security and productivity. This returns us to the challenge of security as a blocker on innovation. Certainly, a balance must be struck to ensure public sector employees have the tools they need to collaborate and innovate, without creating unnecessary cyber risk in both the short- and medium-term.

44%

of respondents say that technology will be the main focus for cybersecurity improvements

45%

of public sector IT leaders want to start by simplifying their security architecture



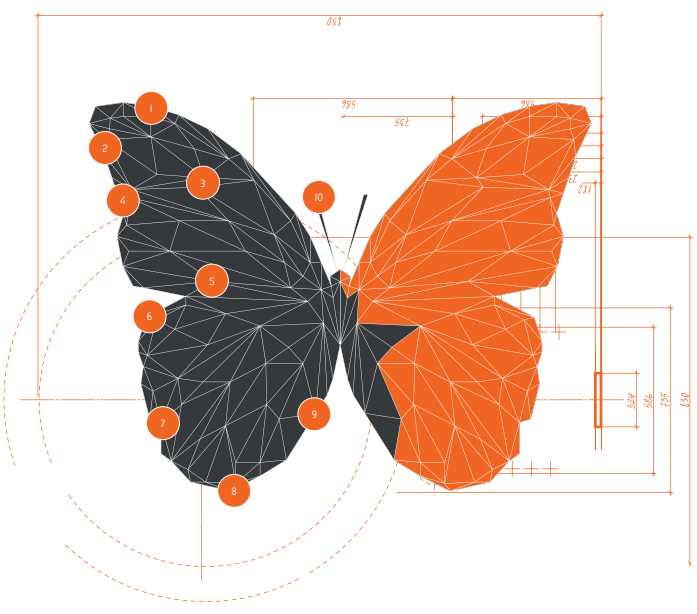
45%

want to review current cyber risk management strategies to ensure they have the right balance between security and productivity

Conclusion

The UK Government is a digital leader relative to its global peers, but there's still much work to do. IT leaders in central government are keen to push on with IT modernisation projects to enhance productivity, IT efficiency and the quality of public services. One of the drivers here is improving cybersecurity, especially addressing vulnerabilities — which are being exploited to increasingly serious effect by threat actors. Yet while security is a driver for digital transformation, it can remain a major barrier to upgrades if internal teams are obstructive.

The way forward lies with breaking down those traditional siloes between security and IT teams, for instance by promoting DevSecOps as a way to integrate security early on in new projects and promoting collaboration throughout a system's lifecycle. Cyber risks relating to cloud-based systems will also require much attention. Applying the right engineering approaches, appropriate to the level of threat and balanced with business operations imperatives, has been shown to enable significant transition away from Legacy IT in a secure manner. Continuing to improve awareness throughout an organisation of the risks involved, and the shared responsibility model of cloud services, will allow greater access to new technologies and the means to operate securely.



[1] UK claims number 2 spot in OECD digital government rankings Jessica McEvoy, GDS (16 October 2020)
[2] Digital government during the coronavirus crisis Institute for Government (accessed 11 March 2021)
[3] Coronavirus Job Retention Scheme: awareness, understanding and customer experience surveys HMRC (October 2020)
[4] SolarWinds hack explained: Everything you need to know Saheed Oladimeji, TechTarget (9 February 2021)
[5] Exchange servers under siege from at least 10 APT groups Matthieu Faou, Mathieu Tartar, Thomas Dupuy, ESET (10 March 2021)
[6] NIST security vulnerability trends in 2020: an analysis Redscan (accessed 11 March 2021)
[7] IT Visibility Gap Study Tanium (accessed 11 March 2021)

BAE SYSTEMS

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/governmentinsights