A PARLIAMENT STREET REPORT

DIGITAL GOVERNMENT: A SECURE FUTURE

PARLIAMENT STREET
partnership in policy

Gigamon®

FOREWORD

The digital landscape has changed more drastically in the last 24 months than ever before, and organisations have had to keep pace with the latest trends, new innovations and digital technology which has revolutionised our approach to modern day problems.

This global wave of digital transformation is not just something which is impacting the private or consumer sectors; public facing organisations and governments have also had to adapt their own operations, as well as external policy and legislation so that it is equipped to deal with the digital demands of society today.

In one such example of how the UK government is modernising its approach to traditional processes, HM Revenues & Customs recently outlined plans to digitalise UK tax. The initiative, known as Making Tax Digital for VAT, allowing business owners to keep digital records and filing returns using compatible software. As of December 2021, nearly 1.6 million taxpayers had joined the scheme, and 69% had reported experiencing at least one benefit since moving to Making Tax Digital.

Technology is also helping to make improvements in other areas of the UK too, such as in the NHS, where better data sharing processes has revolutionised key health services such as finding applicable donors with urgency. Open banking models has also been adopted to allow those in financial need to share their income to enable HMRC to fast-track their applications for new welfare entitlements.

This report will explore the challenges facing public sector organisations such as ransonware and other threats and explore solutions to protectecting public data.

Patrick Sullivan, CEO, Parliament Street

DIGITAL CHANGE

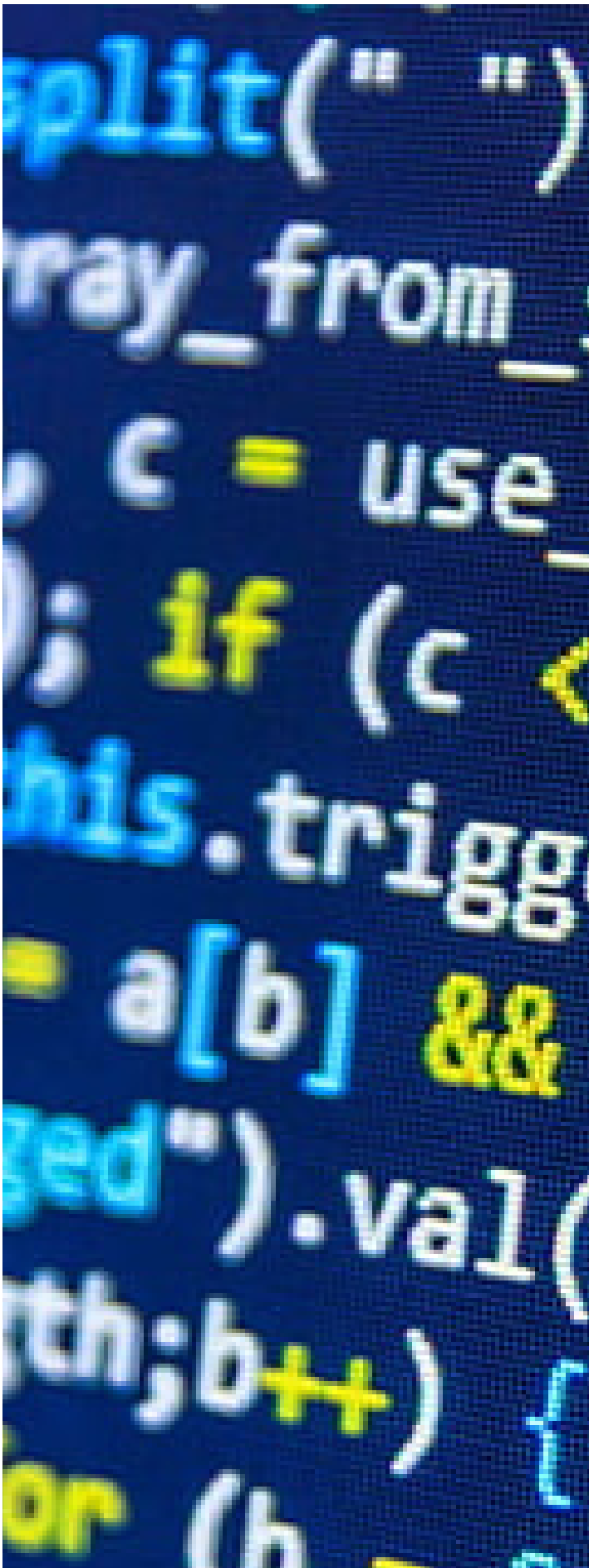
TIn recent years, cyber security has grown exponentially as a threat targeting the public and businesses alike.

Therefore, the UK government recently published a National Cyber Strategy to proactively lead the UK into a future where it is better equipped to deal with the problematic cyber threat scape. As part of this cyber strategy, the UK government has made a £22 billion commitment to the research and development of cyber prevention strategies and national security, and at the heart of it will be technology.

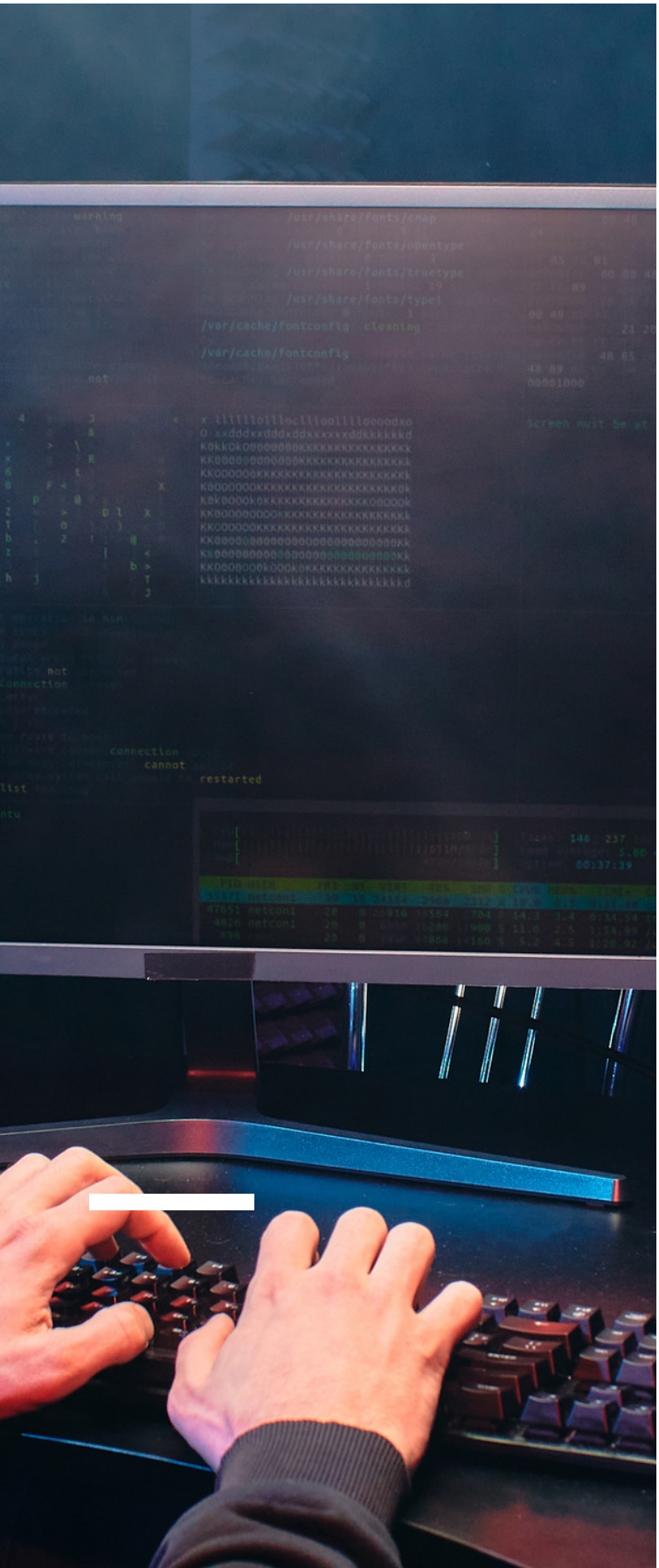
As part of this strategy, the government will lean on artificial intelligence, data and emerging technologies such as 5G and blockchain, to ensure that the UK takes a step-up in terms of its cyber defence mechanisms and its offensive cyber capabilities. This not only includes helping to protect private businesses and consumers, but also to make the public sector more resilient, by helping councils and governmental departments to protect their systems and citizens' personal data from ransomware and other cyber attacks, for example.

However, the UK government is far from the 'finished article' when it comes to technological innovation. A report from the Commission for Smart Government in 2020 even concluded that the UK government has fallen behind. It was suggested that this was due to a confluence of factors, including low levels of digital skills at all levels of public administration, lack of clarity from leadership about responsibilities for digitally enabled services, and outdated procurement systems which have indirectly discouraged innovation in recent years.

In the time since this critical report was published, the government has made key commitments to improving digital capabilities once again, and it's clear that the UK is back on track to cementing its position as a world leader in digital government once again.



RANSOMWARE ON THE RISE



The threat of ransomware against public sector organisations such as local councils cannot be underestimated. To investigate this threat, the Parliament Street think tank conducted a detail survey using Freedom of Information legislation to discover incidents where public sector organisations faced huge risk due to successful attacks.

Merton Council, based in London, disclosed that it has been compromised by a successful ransomware attack three times in the last five years. The Council said that only one of the attacks led to ‘downtime’ where the systems were offline.

A spokesperson explained, “This was due to the Kaseya attack on our hosted environment and resulted in 3 days of some services being disrupted whilst we restored and verified the integrity of data.” It is understood that no ransom fees were paid to hackers.

Meanwhile Brent Council also faced successful ransomware attacks the council disclosed two successful attacks to our researchers. In the first incident that was successful in 2016, some council files were successfully encrypted.

A similar incident happened again in 2018 when files were encrypted. The council paid no ransom and disruption was described as minimal, with the affected files restored via backup systems.

EXPERT VIEW:
BEN JOHNSON, DIRECTOR, GIGAMON

"During the chaos of the Covid-19 pandemic, we all saw how critical public services such as the NHS, local councils and departments such as the treasury were able to adapt and deliver in a time of crisis. Underpinning this performance was a mixture of digital skills, powerful IT capabilities and of course, data.

From the vaccination programme, track and trace through to furlough and grant schemes, the ability for the country to continue to operate despite the disruption came down largely to strategic technology deployments which really provided their worth. However, as the public sector moves forward, the use of personal and private data to deliver targeted services is set to increase dramatically, and unfortunately cybercriminals are all too aware of this trend.

Ransomware has recently been identified as one of the greatest threats to the UK public and private sector and has evolved substantially in recent years. Such attacks creep into an organisation, paralysing the IT systems and forcing decision-makers to pay a hefty sum to regain control of their data. Imagine, for example, if such an attack took place in a hospital, where vital information about medication, treatment and operations were hijacked, the consequences could cost lives.

The reality is that ransomware relies on blind spots in your network, you need to have full visibility of your infrastructure be it physical, virtual or hybrid cloud and to do this cost effectively optimising the security and networking tools you already have. In an increasingly complex world, where digitisation is key, public sector departments need to gain full visibility into workloads across all environments, whether that be hybrid, physical or virtual and across all tools, whether that be the network or security systems.

At Gigamon, we have an impressive track record delivering full visibility to many major government departments, creating tangible cost savings and a reduction of unnecessary data. With cyber crime on the rise and government departments being seen as top target for sophisticated cyber criminals, ensuring complete visibility into network traffic to understand what's happening and when, should be the new normal for any organisation tasked with overseeing crucial data."