Building a cyber-resilient public sector

Introduction

It is very fitting that I should be talking to many of you virtually today. For the Covid 19 pandemic has tested all of us in every possible way and yet technology has enabled us to carry on.

To work from home, to see a doctor, to keep in touch with our families and friends and to educate our children.

It has also enabled government to carry on providing the precious public services that we as citizens rely on.

But while we have been making the very most of technology – so too have cyber criminals.

Seizing our sudden shift online as an unprecedented opportunity to disrupt our day-to-day lives and do our organisations harm, all of which can have a devastating impact with lasting examples.

Let me give you just three examples from the last eighteen months, from local government, where digital services are increasingly being targeted by our adversaries due to the personal and financial data they hold.

In Redcar and Cleveland, residents couldn't access key services or seek social care advice. They couldn't make online appointments or look at planning documents for many weeks after the council's computer systems and website came under attack in early 2020.

Likewise in Hackney, essential council tax, benefits and housing services for residents were left devastated after a ransomware incident almost fifteen months ago – while the most recent target, Gloucester City Council, is still working to recover full use of its IT systems after a cyber attack just before Christmas.

We cannot dismiss these events as one-offs.

This is a growing trend – one whose pace shows no sign of slowing.

I am proud to say that when UK public services have suffered attacks, the government has acted fast to support getting key services back up and running, and also to manage any risks to stolen data – with the National Cyber Security Centre – the NCSC – providing expert technical advice.

However, the public rightly expects us to do everything we can to prevent these attacks in the first place and to get services quickly back to normal when they do indeed happen.

It isn’t just local authorities that are affected.

We have repeatedly warned the public about the rapid rise in consumer-focused scams by professional predators.

Businesses and retailers, too, are on our adversaries hit-lists. Just in December, three hundred Spar grocery stores in the north of England were affected by a computer and IT outage.

And as if to prove the hackers’ total lack of scruple, an attack last year on the Irish health system meant people had to wait for cancer treatment and X-rays.

Indeed globally, we have seen the impact on our allies, including the US government, following the compromise of Solarwinds’ network management software in 2020.

And we have witnessed, too, the destabilising effects on public confidence in Ukraine following recent cyber attacks on its government infrastructure.

So my priority now – having taken over this critically important brief as lead government minister for cyber – is to ensure that the UK government, at all levels, is much more resilient to cyber attacks.

Delivering change through the Government Cyber Security Strategy

That is why the first ever Government Cyber Security Strategy – which I am delighted to be launching today – is so important.

If we are to continue to prevent our public services coming under pressure and to protect them from the harmful consequences of cyber attacks, we need to act.

The Strategy has a very clear vision.

Our core government functions, from the delivery of public services, to the operation of National Security apparatus, must be more resilient than ever before to cyber attacks.

And we are setting out the clear aim for government’s critical functions to be significantly hardened to cyber attack by 2025.

This aim accounts for all public service organisations – including across local government, and the health and education sectors – which in many cases are starting from a very low level of maturity.

Achieving our aim is essential. Not only to protect government functions and public services but also to realise the ambitions set out in the Integrated Review and the National Cyber Strategy

It will also help cement the UK as a democratic and responsible ‘Cyber Power’.

Only by ensuring that cyber attacks neither disrupt our core functions, nor erode vital trust and public confidence can we use the full potential of cyber as a lever to protect and promote our interests in a world that is being fundamentally and rapidly reshaped by technology.

The Government Cyber Security Strategy will deliver this in two fundamental ways.

First, by building organisational cyber resilience in a way that allows government organisations to understand the risks and threats they face, and indeed then to manage them.

To do this we will adopt the NCSC's Cyber Assessment Framework for the whole of government, as the foundation of a new, detailed and comprehensive assurance regime, backed up by independent assessment.

And from this we will emerge not with a generic sketch of government cyber defences but a properly objective picture of our collective strengths and weaknesses –

And far from being an additional layer of bureaucracy and compliance, the new assurance regime will be an early warning system for all government organisations.

By the very nature of their activities, some of these organisations regularly face more sustained, determined, and well-resourced attacks on them.

And we all have a vested interest in getting their protection right.

So – as the second fundamental element of the Government Cyber Security Strategy – we are going to 'Defend as One'.

Ensuring that government presents a defensive force more powerful than the sum of its parts.

At the moment, considerable talent and capability is spread over a range of government organisations – and is not always harnessed to best effect.

Our new Government Cyber Coordination Centre, or GCCC, will transform how we use cyber security data – by facilitating threat and vulnerability management at scale, and fostering partnerships across the public sector and the Union – to rapidly identify, investigate and coordinate responses to incidents.

This joint venture between the Government Security Group, the Central Digital and Data Office and the NCSC, – is intended to underpin our long-term ambitions for cyber security, and ensure that our efforts are better coordinated.

Investment in cyber resilience

The significance of the cyber security challenges we face is reflected in the funding we as a government are making available to tackle them.

The government is investing £2.6 billion in cyber over the next three years – significantly more than the £1.9bn that was committed in the last National Cyber Strategy, with a particular emphasis on improving the government's own cyber security.

This includes over £85m to tackle the challenges facing councils, helping them build their cyber resilience and protect vital services and data.

And we will continue to invest in government's cyber resilience, prioritising by risk to ensure that our most critical functions and services are protected.

Developing leadership and skills

I'd like to give particular focus to the importance of people and culture in making this a reality.

Strong leadership is crucial to success.

And I welcome the strong emphasis public sector leaders are placing on cyber security as a catalyst and enabler for UK digital transformation.

Indeed for my own part, one of my top priorities will be promoting government cyber resilience and driving forward the implementation of this strategy across government.

I look forward to working with the Prime Minister and my Ministerial colleagues, who I know are very supportive of this agenda.

Technical experts are also, of course, crucial to building 'secure by design' government infrastructure. But we also need sufficient skills and knowledge beyond the specialised technical roles, alongside the 'softer skills' they will need for management roles later in their careers.

From 2022, we will have 130 cyber apprentices across 21 government departments, and we are going to carry on building on this great foundation.

And the new Cyber Fast Stream will begin to produce leaders as part of the Autumn 2022 cohort – a generation with the technical expertise to bring the Cyber Strategy off the printed page and into practice.

Even so, there is much more to do.

Because government cannot address the skills challenge alone.

As I set out in the National Cyber Strategy, we will need a whole-of-society approach to equip Britain with the skills it needs to prosper in a digital age.

This afternoon I'm off to Ada, the National College for Digital Skills, to see the fantastic work they are doing to equip young people – I'm having a go myself – with Computer Science and STEM skills and expertise.

The kind of expertise running throughout society that will turn this vision into reality not just for the government but Britain – making us a Cyber Power at the forefront of the digital age.

Conclusion

Everyone who is involved in the cyber security sector can be proud of the progress made so far.

But to meet the threats we face in the coming decade we must build on our success and intensify our approach to cyber security.

The Government Cyber Security Strategy is the foundation of that effort.

A stronger, better-defended government sits at the very heart of the UK as a cyber power – leading the work to deter and disrupt the activities of those who wish to do us harm.

Today marks another important step in our journey to creating a cyber resilient public sector.

There is now a huge task ahead of us.

But having laid the framework for success through the strategy. I look forward to taking this challenge forward with all of you.