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.

40th Universal Periodic Review of human rights: UK statement on Iceland

World news story

The UK delivered this statement during Iceland's Universal Periodic Review (UPR) at the Human Rights Council.

The Universal Periodic Review takes place in Geneva.

The United Kingdom acknowledges Iceland's strong human rights record, welcoming the high priority Iceland has given to the work of the Human Rights Council.

We commend Iceland on topping the 2021 global gender gap index rankings and voting in two novel legal acts on Gender Autonomy.

The UK welcomes Iceland's commitment to media freedom and commends its ratification of OPCAT in 2019. We are pleased to see the seriousness which Iceland attaches to combatting human slavery including by introducing a new Human Slavery act in 2021.

We recommend Iceland:

1. Build upon the 2021 Human Slavery act by increasing training for police, prosecutors and judges on investigating and prosecuting perpetrators of modern slavery offences;

2. Ensure an open, merit-based process when selecting national candidates for UN Treaty Body elections;

3. Introduce a criminal law provision that expressly considers racist motivation of an offence as an aggravating circumstance.

Thank you.

Published 25 January 2022

40th Universal Periodic Review of human rights: UK statement on Togo

World news story

The UK delivered this statement during Togo's Universal Periodic Review (UPR) at the Human Rights Council.

The Universal Periodic Review takes place in Geneva.

The United Kingdom recognises Togo’s democratic progress, including the 2019 constitutional reforms re-introducing presidential term limits. The appointment of Togo’s first female Prime Minister is a step forward for gender equality.

The UK acknowledges efforts to implement the International Covenant on Civil and Political Rights. However, we remain concerned about widespread allegations of human rights violations and abuses, including on freedoms of expression and assembly.

We recommend Togo:

1. Implement a comprehensive strategy to tackle child abuse and criminalise contemporary forms of slavery including human trafficking, forced labour and forced marriage, in line with international standards;

2. Ensure that all allegations of arbitrary arrest, detention and torture are promptly impartially and thoroughly investigated and perpetrators brought to justice;

3. Decriminalise same sex consensual relations to protect the human rights of all, regardless of sexual orientation or gender identity.

Thank you.

Published 25 January 2022

TV hosts Suzi and Ortis star in new road safety campaign

The TV presenters are working with National Highways to produce helpful and practical videos and clips featuring advice and information about using the roads.

Footage shows the pair driving on sections of smart motorway, discussing the differences from conventional motorways and explaining how technology is used to keep traffic moving and motorists as safe as possible.

Suzi and Ortis describe how signs and signals give motorists information about the road ahead, including possible obstructions in the road. They also talk about technology being rolled out across the country to detect vehicles that have stopped in live traffic lanes.

They explain what to do in an emergency and also describe Red X signs, emergency areas, how all lane running sections of motorway operate and the use of variable speed limits to reduce congestion.

Suzi, who fronts BT Sport's coverage of MotoGP, said:

> Every driver gets better with more experience and more knowledge about the roads they use. These videos are a quick and easy guide to how smart motorways operate.

Ortis, a star of Channel 5's The Gadget Show, said:

> Smart motorways aim to reduce congestion for millions of motorists. Learning how to use them safely is a great way to contribute to road safety.
>
> I'd advise anyone who uses the roads to watch the videos to ensure they know the best course of action in the rare event they break down on their journey.

The videos are available on the National Highways Driving on Motorways web page.

National Highways Customer Service Director Mel Clarke said:

> Everyone can learn to be a better and safer driver.
>
> We're investing hundreds of millions of pounds to make England's motorways and major A-roads even safer and we can all play our part by making sure we and our loved ones know how to use the network

safely.

Videos and clips of Suzi and Ortis are being posted on National Highways Facebook, Twitter and LinkedIn channels, providing information on how a smart motorway works as an overall system and how to drive safely on a smart motorway.

Updated Highway Code rules which came into effect in September 2021 include clearer advice on where to stop in an emergency. For more information visit Driving on Motorways.

Advice on what to do in the event of a breakdown.

Members of the public should contact the National Highways customer contact centre on 0300 123 5000.

Journalists should contact the National Highways press office on 0844 693 1448 and use the menu to speak to the most appropriate press officer.

Global data experts fire up government's plans to promote free flow of data

- Representatives from Google, Mastercard and Microsoft among the 20 experts meeting today to launch International Data Transfer Expert Council

- Comes as part of government ambition to unlock benefits of free and secure data flow after leaving the EU

A group of experts combining the world's leading academics and digital industry figures, including Google, Mastercard and Microsoft, will meet for the first time today to help Britain seize the opportunities of better global data sharing.

The International Data Transfer Expert Council is launching to provide independent advice to the government to help it achieve its mission of unlocking the benefits of free and secure cross-border data flows now the country has left the EU.

International data transfers underpin our everyday life and are the foundations for our most-used tech, from GPS navigation and smart devices to

online banking. They are also instrumental to digital healthcare – having driven the development of treatment and vaccines during the pandemic.

Removing barriers to data flows will mean these services can be provided more reliably, cheaply and securely. Billions of pounds worth of trade goes unrealised around the world due to barriers associated with data transfers.

Household tech and industry names are represented on the council alongside international universities and organisations at the forefront of this rapidly moving policy area, such as the World Economic Forum and the Future of Privacy Forum.

Data Minister Julia Lopez said:

> Realising the benefits of international data flows has never been more important.
>
> We want the UK to drive forward cutting-edge policies at home and overseas to ensure people, businesses and economies benefit from safe and secure data flows.
>
> Today we're launching a new panel of global experts to help us achieve these aims and I will lead the first meeting so together we can deliver a world-leading and truly global data policy for the future.

There are a range of mechanisms under current UK data protection law which organisations can use to transfer personal data to other countries, including standard contractual clauses and binding corporate rules. The Council will give advice on the development of new international data transfer tools and mechanisms and securing new data adequacy partnerships with other countries.

Now that the UK has left the EU, the government intends to strike deals on personal data transfers with some of its key trading partners around the world. Personal data relates to an identified or identifiable individual and includes secure transfer of information on things such as ethnic origin and IP address.

The government has outlined the first countries with which it will prioritise striking data adequacy partnerships to ensure the data protection standards in the country data is being transferred to mirror the UK's. The UK's current priority countries include the United States, Australia, the Republic of Korea, Singapore, the Dubai International Finance Centre and Colombia. Securing new data transfer agreements will build significantly on the annual £83 billion of data-enabled UK service exports.

Experts on the council have been selected from civil society, academia and industry around the world. Their experiences cover a range of areas including patient healthcare, scientific research, artificial intelligence and finance.

The launch of the council is part of the government's ambitious National Data

Strategy to harness the power of data to boost economic growth, create jobs and deliver new innovations for people and public services.

During its first meeting today, the council will discuss the global opportunities and challenges for international transfers and how the UK can be a global leader in removing barriers to cross-border data flows. This will enable smoother and more straightforward transfers without the need for costly and often complicated contracts.

It will continue to meet quarterly covering issues such as future data adequacy partnerships, the development of new data transfer tools, and how governments can work together to promote greater trust in sharing personal data for law enforcement and national security purposes.

ENDS

Notes to Editors

Members of the International Data Transfer Expert Council are:

- Anne Josephine Flanagan – Data Policy and Governance Lead, World Economic Forum
- Bojana Bellamy – President, Centre for Information Policy Leadership
- Caitlin Fennessy – Vice President and Chief Knowledge Officer, International Association of Privacy Professionals
- Caroline Louveaux – Chief Privacy Officer, Mastercard
- Christopher Calabrese – Senior Director, Privacy and Data Policy, Microsoft
- Dr Clarisse Girot – Asia Pacific Director, Future of Privacy Forum
- Eduardo Ustaran – Partner and Global co-head, Privacy and Cybersecurity Practice, Hogan Lovells
- Professor Elizabeth Coombs – Associate Professor, University of Malta, and Chair, International Committee, Australian Privacy Foundation
- Fergus Allan Cloughley – CEO and Director, Obashi Technology Limited
- Dr Isaac Rutenberg – Senior Lecturer and Director, Centre for Intellectual Property and IT Law, Strathmore University, Kenya
- João Barreiro – Chief Privacy Officer, BeiGene
- Kate Charlet – Director for Data Governance, Google
- Professor Neena Modi – Professor of Neonatal Medicine (Imperial College London), and Consultant in Neonatal Medicine (NHS)
- Nigel Cory – Associate Director, Trade Policy, Information Technology and Innovation Foundation
- Richard Ward – Government Relations Director, IBM
- Ruth Boardman – Partner and co-head, International Privacy and Data Protection Group, Bird & Bird
- Théodore Christakis – Professor of International and European Law (Université Grenoble Alpes), and Senior Fellow (Cross-Border Data Forum)
- Thomas Boue – Director General of Policy (EMEA), BSA The Software Alliance
- Vivienne Artz – Chair of the Data Working Group of the International Regulatory Strategy Group (IRSG), and NED and Vice Chair of the Risk Committee for Global Legal Entity Identifier Foundation (GLEIF)

- Dr Wai Kuan Hon – Of Counsel, Dentons

More information on the Government's plans for international data transfers can be found here.