First ever Government Cyber Security Strategy to step up Britain's defence and resilience

- First ever Government Cyber Security Strategy launched today, to further protect public services people rely on.
- The public will be able to contribute to this effort by reporting cyber incidents or weaknesses with digital services.
- New Cyber Coordination Centre to be established, which will transform how data and cyber intelligence is shared, as Steve Barclay warns of ever growing cyber threat following a string of attacks.

Britain's public services will be strengthened to further protect them from the risk of being shut down by hostile cyber threats, Chancellor of the Duchy of Lancaster Steve Barclay will say today.

The minister will outline the cyber threat that government and wider public sector systems face in a speech today, as he launches the first ever Government Cyber Security Strategy.

In the speech in central London, Mr Barclay will say that Britain is now the third most targeted country in the world in cyberspace from hostile states.

The new strategy will be backed by £37.8 million invested to help local authorities boost their cyber resilience – protecting the essential services and data on which citizens rely on including housing benefit, voter registration, electoral management, school grants and the provision of social care.

Chancellor of the Duchy of Lancaster Steve Barclay said:

> Our public services are precious and without them individuals can't access the support that they rely on.
>
> If we want people to continue to access their pensions online, social care support from local government or health services, we need to step up our cyber defences.
>
> The cyber threat is clear and growing. But government is acting – investing over £2billion in cyber, retiring legacy IT systems and stepping up our skills and coordination.

The new strategy outlines how central government and the public sector will continue to ensure that public services can function in the face of growing cyber threats. It will step up the country's cyber resilience by better sharing data, expertise and capabilities to allow government to 'Defend As One', meaning that government cyber defence is far greater than the sum of

its parts.

Of the 777 incidents managed by the National Cyber Security Centre between September 2020 and August 2021, around 40% were aimed at the public sector. In 2020, both Redcar & Cleveland and Hackney Councils were hit by ransomware attacks impacting council tax, benefits and housing waiting lists. Gloucester City Council was then the subject of a further cyber attack in 2021.

Members of the public will also be able to contribute to the effort, with a new vulnerability reporting service allowing individuals to report weaknesses in digital services.

The strategy will make core government functions, such as the delivery of essential public services, more resilient than ever before to cyber attack from malicious actors.

It follows the recent publication of the National Cyber Security Strategy, which called on all parts of society to play their part in reinforcing the UK's economic strengths in cyberspace, through more diversity in the workforce, levelling up the cyber sector across all UK regions, expanding offensive and defensive cyber capabilities and prioritising cyber security in the workplace, boardrooms and digital supply chains.

Key announcements in the strategy include:

- Establishing a new Government Cyber Coordination Centre (GCCC), to better coordinate cyber security efforts across the public sector. Building on successful private sector models, such as the Financial Sector Cyber Collaboration Centre, the GCCC will rapidly identify, investigate and coordinate the government's response to attacks on public sector systems. The centre will be based in the Cabinet Office and will ensure that data is rapidly shared, allowing us to 'Defend As One'.
- A new cross-government vulnerability reporting service, which will allow security researchers and members of the public to easily report issues they identify with public sector digital services. This will enable organisations to more quickly fix any issues identified.
- A new, more detailed assurance regime for the whole of government, which will include robust assessment of departmental plans and vulnerabilities. This will give central government a more detailed picture of government's cyber health for the first time.
- £37.8 million invested into local authorities for cyber resilience – protecting the essential services and data on which citizens rely on including housing benefit, voter registration, electoral management, school grants and the provision of social care.
- An innovative project to reduce government risk through culture change, in partnership with small businesses and academia.
- Stepped up work to understand the growing risk from the supply chains of commercially provided products in government systems, ensuring security is a key part of procurement and working with industry on cyber vulnerabilities.

Government Chief Security Officer, Vincent Devine said:

> We need this bold and ambitious strategy to ensure that government’s critical functions are significantly hardened to cyber attacks.
>
> The strategy is centred around two core pillars, the first focussing on building a strong foundation of organisational cyber security resilience; and the second aimed at allowing government to ‘defend as one’, harnessing the value of sharing data, expertise and capabilities.