Press release: ‘Designing out’ cyber threats to businesses and personal data

- UK to become a world leader in ‘designing out’ many forms of cyber threats to online services and digitally enabled products by investing in development of hardware solutions to complement software solutions
- 40% of UK businesses have experienced a cyber security breach or attack in the last 12 months
- New investment through the modern Industrial Strategy to build on UK strengths in cyber security and increase share of a global market predicted to grow to £39 billion in a decade

The UK is set to become a world leader in the race to eradicate some of the most damaging cyber security threats facing businesses and better protect consumers, Business Secretary Greg Clark announced today.

Businesses and consumers will benefit from increased security and protections built into digital devices and online services we use every day. This is with the help of up to £70 million in government investment through the Industrial Strategy Challenge Fund and backed by further investment from industry.

This investment will support research into the design and development of hardware so that they will be more secure and resilient from the outset. This aims to ‘design out’ many forms of cyber threats by ‘designing in’ security and protection technology/solutions into hardware and chip designs, ultimately helping to eradicate a significant proportion of the current cyber risks for businesses and services in future connected smart products.

With cyber threats constantly evolving, the best defence in the future is seen as developing innovative solutions that can work independently and protect against threats even during attacks. The government wants to ensure that every UK organisation is as cyber secure and resilient as possible.

A further £30 million of government investment will aim to ensure smart systems are safe and secure. Smart internet connected devices can include anything from operating a central heating thermostat via a smart phone, to pressing a button to unlock the front door. There are expected to be more than 420 million such devices in use across the UK within the next 3 years.

Business Secretary Greg Clark said:

> This could be a real step-change in computer and online security, better protecting businesses, services and consumers from cyber-attacks resulting in benefits for consumers and the economy. With businesses having to invest more and more in tackling ever more complex cyber attacks, ‘designing in’ security measures into the

> hardware's fabric will not only protect our businesses and consumers but ultimately cut the growing cybersecurity costs to businesses.
>
> This is our modern Industrial Strategy in action. Building on the UK's heritage and strengths in computing and cyber security alongside the government and industry investing together to ensure the UK capitalises on its position to become a leader in the growing markets and technologies of tomorrow.

Nearly all UK businesses are reliant on digital technology and online services, yet more than 40% have experienced a cyber-security breach or attack in the last 12 months. Hackable home Wi-Fi routers can be used by attackers in botnets to attack major services and businesses. Moreover, consumers are often the worst affected by mass information leaks than the organisation that held their data. Businesses are having to spend increasing amounts on cyber security, up to 20-40% of their IT spend in some cases. And as more and more systems are connected, whether in the home or businesses, there is a need for security that is secure by design.

Digital Minister Margot James said:

> We want the UK to be a safer place to live and work online. We're moving the burden away from consumers to manufacturers, so strong cyber security is built into the design of products. This funding will help us work with industry to do just that, improving the strength and resilience of hardware to better protect consumers from cyber-attacks.

Dr Ian Levy, National Cyber Security Centre's Technical Director, said:

> The National Cyber Security Centre is committed to improving security from the ground up, and we have been working closely with government to promote adoption of technology and practices to protect the UK.
>
> We hope this additional investment will drive fundamental changes to products we use every day. This is vital work, because improving hardware can eradicate a wide range of vulnerabilities that cause significant harm.

The government aims for R&D investment to reach 2.4% of GDP by 2027– the biggest increase in public investment in R&D in UK history.

The modern Industrial Strategy sets out Grand Challenges to put the UK at the forefront of the industries of the future – AI and Data is one them. Through this Grand Challenge, the UK will be at the forefront of the AI and data revolution, helping sectors boost their productivity through new

technologies, helping people develop the skills they need and leading the world in the safe, ethical use of data.

1. The up to £70 million Digital Security by Design challenge will be delivered by UK Research and Innovation through the Industrial Strategy Challenge Fund, subject to business case approval and match funding from industry.

2.The £30.6 million Ensuring the Security of Digital Technology at the Periphery programme will be delivered by UK Research and Innovation through the Strategic Priorities Fund. The programme aims to ensure that Internet of Things systems are safe and secure, particularly as more critical applications emerge meaning there is increased vulnerability to broader, more sophisticated cyber-threats. Effective solutions need to combine cyber and physical safety and security with human behaviour, influence new regulatory response and validate and demonstrate novel approaches. This will build on current investments including the PETRAS Internet of Things Research Hub and other activities supported through IoT UK.

3. The Department for Digital, Culture, Media and Sport (DCMS), in conjunction with the National Cyber Security Centre (NCSC), has been carrying out a review in the security of internet-connected consumer products. DCMS published the Code of Practice for Consumer IoT Security in October 2018 to support industry with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in the digital world. DCMS also published guidance for consumers on securing smart devices in the home: Secure by design.

4. Cyber Aware is HMG's public awareness and behaviour change campaign on cyber security. It encourages the public and micro businesses to adopt 2 simple behaviours to help protect themselves against the cyber threat – install the latest software and app updates, and use a strong and separate email password. At the end of 2017/18, an estimated 10.6 million adults and 1.2 million SMEs claimed they were more likely to maintain or take up key cyber security behaviours as a result of Cyber Aware.

5. The UK government is fully committed to defending against cyber threats and address the cyber skills gap to develop and grow talent. A five-year National Cyber Security Strategy (NCSS) was announced in November 2016, supported by £1.9 billion of transformational investment.

6. The NCSC provides a single, central body for cyber security at a national level. Since it became fully operational in 2016, the NCSC has helped to support with 1,167 cyber incidents – including 557 in the last 12 months.

7. Software based solutions allow for fast reaction to a changing threat landscape but can often be limited to individual vendors or vulnerabilities. Hardware, using the lessons learnt from software-based defences, can remove whole classes of attacks where the benefit can be far-reaching.