Speech: Chancellor of the Duchy of Lancaster speech at the National Cyber Security Centre: 16 October 2018

I am delighted to be here for the National Cyber Security Centre's second annual review.

The digital revolution has transformed our lives in profound ways.

We can see how much it has changed the world:

Every time we shop…

… every time we need directions…

…and even every time we try to talk to our children!

As our digitally connected world has expanded at an extraordinary rate, so too has the scale of vulnerabilities and the frequency of attacks that we face.

Thousands of public and private sector organisations worldwide are falling victim to ransomware attacks.

Our supply chains are being compromised.

Our critical national infrastructure continues to be a target for attack from nation states and cyber criminals.

… and we are seeing threats to our democracies from attempted outside interference.

It is right that in the face of these shared threats the UK stands strong with its international partners and allies, and that we work alongside them to confront, expose, and disrupt hostile or malicious activity.

You will have seen recently our attribution of a range of malicious cyber attacks to the work of the Russian Military Intelligence. This builds upon a host of cyber attacks we attributed with our international partners – including the WannaCry incident, one of the most substantial to hit the UK in terms of scale and disruption, to North Korean actors.

We will continue to reaffirm our shared vision for an open, peaceful and secure digital world based on the rule of law and norms of behaviour.

Protecting the British people, the systems that we rely upon, and our very democracy itself, is essential.

It is for this reason that cyber security remains a top priority for the

government – because it impacts our national security, and our economic prosperity too.

The story so far

This is why we recognised the need for a comprehensive response to cyber security, spearheaded by Government through our National Cyber Security Strategy launched in 2016.

We set out ambitious proposals to take a more active role to defend our people, to deter our adversaries and develop our capabilities to ensure the UK remains the safest place to live and do business online.

One of the most visible elements of the strategy was the formation of the National Cyber Security Centre…

… to bring together our very best intelligence and technical expertise into a single world leading authority. The NCSC has undertaken some pioneering work in its first two years.

You will hear shortly from Jeremy and Ciaran, who will be highlighting the NCSC's significant achievements shortly…

And as a Government, we have done much more to strengthen the UK's defences and make this country a harder place for adversaries to operate in – setting clear direction, pushing innovation, and building capabilities and partnerships.

We have invested in our cyber capabilities within law enforcement, such as the National Crime Agency's Cyber Crime Unit and the Regional Organised Crime Units, so we can pursue those who persist in attacking us, wherever they are.

We have developed early intervention programmes to divert those at risk of going down the wrong path.

And we are inspiring more potential cyber security experts and entrepreneurs…

… through our programmes in schools and universities, and through our work with industry to retrain.

We are also working with our world-class universities and stimulating ground breaking research, to establish a pipeline of cutting-edge cyber security companies.

We have launched a range of initiatives to incubate and scale-up, including our new cyber accelerator in London, so we can turn many more great ideas into global businesses,.

And in April, we published a new Cyber Security Export Strategy, setting out how we'll help the UK's world leading cyber companies sell their innovative capabilities overseas.

Underlining the fruits of those efforts, the UK cyber security industry is

now generating over £5 billion for the economy.

Rising to the challenge

At this half way point in the delivery of our National Cyber Security Strategy, we have put in place many of the building blocks to transform the UK's cyber security and resilience. These are demonstrating clear results.

But we can never become complacent. Just as the threat from cyber criminals and hostile nation states continues to evolve, so too much we continue to innovate, and to re-focus our efforts to bring about a step-change in our response.

In government we are stepping up our protection of crucial public sector systems. I can today announce that we are launching a scheme to test and improve our own ability to identify and act against sophisticated and persistent cyber-attacks.

The new scheme – called GBEST – is based on the successful CBEST model developed by the financial sector.

It uses cutting-edge intelligence to determine the objectives of our cyber attackers, their priorities for attack, and the techniques and vulnerabilities they may attempt to exploit.

By taking the best from the private sector and adapting it to meet our own needs, we improve our resilience against attacks in the future. Each year we will be running exercises to test and improve our protection and response.

Our ability to succeed in the face of these challenges also relies on the strength of the partnerships we create.

And our ability to demystify what cyber security actually is.

While it's difficult to avoid headlines about attacks and breaches, doing something about it is still often seen as too technical.

Or too difficult.

Or someone else's problem.

Cyber security is everyone's responsibility. We consider it vital that all organisations must embrace and embed cyber security, starting from the boardroom down.

This is why we have targeted our efforts at driving long-term change, by helping boards to better understand the risks that they face and to invest appropriately.

This year's survey of cyber breaches revealed only 30% of businesses have a board member with responsibility for cyber security. This is not good enough.

We need to ensure that boardrooms provide active leadership to ensure cyber

security is ingrained into organisational cultures and models. Indeed we need to affect the mind-sets of those leading our companies.

The same survey highlighted that only 10% of businesses require their suppliers to adhere to any cyber standards.

With the implementation of new Data Protection laws earlier this year, it is more important than ever for organisations to understand the data they have, to know who it is shared with and how it is protected.

Yes, cyber security can be complex…

… but it should not be beyond the capability of any board member to understand the basics and ensure an organisation has a strong risk management regime in place.

So the government will be stepping up its efforts to encourage – and challenge – companies to put proper cyber security arrangements in place.

I will be writing to all FTSE 350 Chairman to highlight the a new Board Toolkit that NCSC is developing, to help them understand cyber risk, and will be meeting a number of them in the coming months to understand their plans.

And this isn't just about minimising operational, financial and reputational risk. Building resilience amongst employees and customers can also be a catalyst for far greater change.

Our Cyber Essentials scheme extends our influence to those organisations that provide products and services to government.

We are specifying standards that will improve their cyber security…

And also ensure they use these contractual arrangements to ensure they help those in their supply chains – often smaller companies – be more secure.

I am encouraged that firms like Barclays, Astra Zeneca and Airbus and are already encouraging their suppliers in turn to adopt Cyber Essentials.

But, we can do more…

… Which is why the government is also partnering with more than 500 private sector organisations through our national Cyber Aware campaign.

..to encourage citizens and businesses to take the really simple protective steps that can prevent the majority of high volume, low sophistication attacks.

Together, these measures will equip UK organisations with the right mentalities and skill sets to harden their defences, delivering long-term, cultural change.

Looking ahead

We've made good progress since we launched the strategy…

… but there's much still to do to keep pace with our adversaries.

We need to … forge closer partnerships with industry and academia…

… and develop the cyber security profession to create clear career pathways and a more diverse and inclusive workforce.

We are supporting Cyber Security Challenge UK as they launchCyber Re:coded – Europe's biggest cyber careers show in London yesterday and today. To help attract new starters into the industry.

And, in December this year, we will publish our comprehensive cyber skills strategy that will set out proposals to take us to 2021 and beyond.

Our cyber security science and technology strategy – due to be launched in the new year – will look into the future, to identify a clear direction for how we make the most of the opportunities that new and emerging technology brings us…

…from AI to quantum computing and smart cities, whilst at the same time seeking to minimising its risks.

As Government, we also want to underline our ambition in going after one of the biggest prizes – to make all products and services secure by design.

As the internet of things continues to expand, it can't be right that consumers are simply left to secure their own products.

The challenge is to encourage manufacturers to help consumers by building protections into their design.

While this will take global cooperation to fix, I am pleased to say that this last weekend I announced that new Code of Practice for consumer internet connected devices, such as smart home assistants and toys, is being established.

Our commitment is to help manufacturers understand how this code of practice will sit within the broader standards landscape…

… and make it straightforward for them to introduce changes to improve the cyber security of their products…

…so it's easy for consumers to ensure that their devices are as secure as the homes they are in.

Alongside other measures including consumer guidance on smart devices in the home, this world leading approach is trying to shift the burden of security away from consumers.

And help us meet our commitment to make the UK the safest place in the world to be online.

Conclusion

Thank you for listening – I am delighted the strategy is developing and I look forward to working with Jeremy and Ciaran in the years to come.