GOV.UK

1. Home (https://www.gov.uk/)

Speech

Keeping Britain safe from cyber attacks: Matt Hancock speech

The Minister for Cabinet Office gave a speech on the UK's cyber security strategy and keeping Britain safe from cyber attacks.

Published 25 May 2016

From:

Cabinet Office (https://www.gov.uk/government/organisations/cabinet-office), Government Communications Headquarters (https://www.gov.uk/government/organisations/government-communications-headquarters), and The Rt Hon Matt Hancock MP (https://www.gov.uk/government/people/matthew-hancock)

Delivered on:

25 May 2016 (Transcript of the speech, exactly as it was delivered)

I'm very grateful to the Telegraph for asking me here to this crucial conference on cyber security.

As we're guests of the Telegraph, I want to start with a little story about the telegraph. Not the paper, but the technology.

A century ago, the First World War was raging in Europe, and the Allies were desperate to bring America into the war on our side.

Then, in January 1917, the German ambassador to Mexico received an encrypted telegram from Berlin.

It instructed him to offer the Mexican government money and diplomatic support for an audacious invasion of the United States.

But this message was subject to one of the first and perhaps most influential cyber security breaches in history.

It didn't matter that the idea was half-baked, that the Mexicans had no interest in invading Arizona. When the contents were revealed, American opinion was outraged.

Shortly after, Congress voted to join the war.

So why did the German high command entrust such a sensitive message to Western Union, then, as now, a wire transfer company?

Because they had failed to appreciate an obvious network vulnerability.

The subsea cable they were using did not travel directly from Europe.

Instead it went through Britain, stopping off at Land's End, where the signal was boosted before being transmitted to America.

This meant it very easy for British Naval Intelligence to listen in on the traffic.

Once war broke out, any diplomatic telegrams passing through were copied down and dispatched to Room 40, the forerunner of GCHQ.

I mention this story as a warning against complacency.

Telegraphy was the email of its day: trusted and widely used, familiar rather than cutting edge.

People thought it was secure, but it wasn't.

A hundred years on, our trusted communications are wireless, instantaneous and virtually cost-free. Data is stored in the Cloud, not in filing cabinets.

And this has changed the world beyond all recognition, in my view emphatically for the better.

Vulnerability in cyber security

From the little to the life-changing, remote robotic surgery to online box-sets. We are freer, more prosperous, more knowledgeable about the world than ever before.

Yet this brings with it renewed vulnerability.

Barriers to entry have come crashing down for companies and cyber-criminals alike.

Unlike in 1917 you don't need to be a state to inflict a massive data breach.

When peoples' cyber security isn't up to scratch, you just need a laptop and an Internet connection.

The tech may have got smarter, but the biggest weakness in any system is still the human being.

In the last year, 2 thirds of large businesses in the UK experienced an cyber attack.

Almost a quarter suffered a breach at least once a month.

This matters because we are one of the world's leading digital nations.

Twelve and a half per cent of our economy is now online. No other country does more e-commerce.

In government too we've begun to upload the state, using technology to build more responsive, user-centric public services.

I call it the smartphone state.

And we're still only in the foothills.

Smart energy, networked cities, quantum computing: these all have the potential to transform our lives and refashion our economy.

But to deliver on that promise we have to be able to defend our digital society from those who wish it and us harm.

A strong cyber defence requires three things.

First, we – industry and government – together must recognise that this is a shared responsibility, a duty that we owe our fellow citizens.

Second, that we deliver on that commitment by equipping them with the right skills.

And third, that we can and must turn our vulnerabilities into a source of economic strength.

Let me take each in turn.

Shared responsibility

First, it's vital to recognise this is an issue for CEOs as well as spooks.

The vast majority of the UK's Critical National Infrastructure is operated by the private sector. Power, water and telecoms are all critical targets.

Even outside that our digital lives are in your hands, everything from our life savings to our holiday snaps.

I'm encouraged to see that two thirds of businesses say cyber security is now a priority for senior managers.

Yet there remains a gap between awareness and action.

Only half of the businesses we surveyed this year have taken steps to identify cyber risks.

Make no mistake, the next data breach will happen. It's your duty to make it's not your company splashed across the papers when it does.

But we don't expect you to do it alone.

We've created the UK's first systematic National Cyber Security Programme, and we're almost doubling the funding with £1.9 billion over the next five years.

We're setting up a National Cyber Security Centre (https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus) under GCHQ.

The centre will provide a single point of contact for businesses in need of advice and support.

I want it to become a hub of world-class, user-friendly expertise: a global leader under the steady hand of Ciaran Martin, bridging the gap between the worlds of government and industry.

And today I'm publishing the centre's prospectus (https://www.gov.uk/government/publications/national-cyber-security-centre-prospectus) , setting out how it'll work ahead of its full launch later this year.

And we want to hear from you what you think and how it can help your business.

I strongly recommend that you feed back to us, so we can design the National Cyber Security Centre around your needs.

The right skills

We already know that your number one need is for skills, and this is the second part of facing down the cyber threat.

It's not just that we need more skills. Computer security needs to become a basic life skill, like learning to drive.

And while we want everyone to pass the test, we also need our elite Formula 1 drivers.

So we're growing the talent pool at every stage of the education system.

Learning coding in schools, competitions to get more girls into cyber, residential courses for students in Years 12 and 13 - sponsorship for the most promising undergrads – all under the Government-backed Cyber First banner.

We've opened new routes into cyber security, like the new Trailblazer apprenticeship.

And I'm proud to give my support to the new Extended Project Qualification, which the Cyber Security Challenge just created.

This level 3 qualification, equivalent to an AS Level, teaches the basics of cyber security in three months, and can be studied in schools, colleges or through the Challenge itself.

But industry has to play its part too.

We need more businesses to offer training, sponsorship apprenticeships: more breaks for the best minds.

Because if we commit now, together, the struggle in cyberspace is Britain's opportunity.

That's the third part of securing our cyber defences: not just protecting the digital economy but growing it.

Turning risk into reward

We're already one of the top 5 exporters in the world, and the global market is growing by 20% a year.

A strong cyber security industry means a safer Britain.

So we're funding test labs where cyber start-ups can refine their prototypes:

- a cyber security fund to scale the established players
- a cyber security innovation centre in Cheltenham.

And today I can announce a new cyber security trade champion for the Gulf, to help UK companies win business in the region, while supporting the work of the UK Cyber Ambassador.

This comes alongside our dedicated cyber specialist in Washington, who's been supporting our engagement with cyber businesses in the US.

Our goal is to create a commercial ecosystem where cutting-edge research is backed, start-ups get scaled, and British companies win business around the world.

Conclusion

So shared responsibility, the right skills, and boosting the cyber economy: get these 3 right and we can get across this challenge.

Everyone has their part to play to close the chinks in our armour and the gaps in our capability.

There is no doubt that cyber attacks are a serious and growing problem.

But the history of technological advance - and with it of human progress - is the history of solving problems.

After the First World War the Germans, determined that their codes would never again be cracked, built mechanical encryption machines.

In turn we built the world's first digital computers to break them.

We can't know what we'll evolve in response to the current threat.

But if we are honest about the threat, if we work together we can drive progress, power innovation, build better tech and a safer, more prosperous Britain.

That is our task and I look forward to working with you to achieve it.

Published 25 May 2016

Related content

Policy

- Cyber security (https://www.gov.uk/government/policies/cyber-security)