NCSC CEO's speech to mark the launch of the NCSC Annual Review 2024

NCSC CEO Dr Richard Horne announces the launch of the eighth Annual Review

Good morning and welcome to the launch of the NCSC's eighth Annual Review.

I am thrilled to see you here this morning.

This is the first Annual Review that I have the pleasure of launching and I would like to start by thanking Felicity, who led the organisation as interim CEO through a large part of what's been a really busy year before I stepped into my role.

Our mission remains the same today as it was when the NCSC was stood up all those years ago: to make the UK the safest place to live and work online.

What is different is the scale of the challenge in fulfilling that mission.

The contest

I believe I have joined the NCSC at an inflection point which calls for sober reflection.

Because we find ourselves now in a contest for cyberspace.

It's a contest between those of us who are using technology to conduct and improve our lives and prosperity and those people who seek to use our digital dependency against us.

The UK has one of the world's most advanced digital economies.

It is underpinned by online infrastructure which we all rely on to keep the lights on and the water running, to improve our public services, to keep businesses running, and to drive our growth and prosperity.

But those critical systems and services make attractive targets for hostile states and malicious actors in cyberspace.

They are increasingly using our technology dependence against us, seeking to cause maximum disruption and destruction.

In the past year, we have seen crippling attacks against institutions that have brought home the true price tag of cyber incidents.

The attack against Synnovis showed us how dependent we are on technology for accessing our health services. And the attack against the British Library reminded us that we're reliant on technology for our access to knowledge.

What these and other incidents show is how entwined technology is with our lives and that cyber attacks have *human* costs.

Threat landscape

In conjunction with this increased dependence comes a threat landscape that is diversifying at speed.

Hostile activity in UK cyberspace has increased in frequency, sophistication and intensity. We can see this in the intelligence we can access through being part of GCHQ.

State and criminal actors are using cyber capability against organisations across our society seeking to undermine us.

Last week, you will have heard the Chancellor of the Duchy of Lancaster warn about the aggression and recklessness of cyber activity we see coming from Russia.

And with our partners – including at the National Protective Security Authority, otherwise known as the NPSA – we can see how cyber attacks are increasingly important to Russian actors, along with sabotage threats to physical security which both the Director General of MI5 and the Chief of SIS have spoken about recently.

All the while, China remains a highly sophisticated cyber actor with increasing ambition to project its influence beyond its borders.

Earlier in the autumn, authorities in the United States reported that China state-affiliated actors compromised US telecoms networks.

Now, given the global interconnectivity in telecommunications, we at the NCSC judge that there is almost certainly a threat to UK data from opportunistic collection as a result.

And we assess that all sectors of UK society are under threat of data theft from this activity – not just traditional intelligence targets – given the low threshold for information being of value.

These examples illustrate some of the challenges we face and yet, despite all this, we believe the severity of the risk facing the UK is being widely underestimated.

There is no room for complacency about the severity of state-led threats or the volume of the threat posed by cyber criminals.

The defence and resilience of critical infrastructure, supply chains, the public sector, and our wider economy must improve.

What has struck me more forcefully than anything else since taking the helm at the NCSC is the clearly widening gap between, on the one hand, the threat and our exposure to it and, on the other, the defences that are in place to protect us.

And what is equally clear to me is that we all need to increase the pace we are working at to keep ahead of our adversaries.

The problem

The NCSC, as the National Technical Authority, has been publishing advice, guidance and frameworks since our inception in a bid to drive up the cyber security of the UK.

The reality is that advice, that guidance, those frameworks need to be put into practice much more across the board.

We need all organisations – public and private – to see cyber security as both an essential foundation for their operations and a driver for growth, to view cyber

security not just as a ‘necessary evil’ or compliance function but as a business investment, a catalyst for innovation and an integral part of achieving their purpose.

The benefits that security can bring should be no surprise.

Research from insurers shows organisations are 92% less likely to make a claim on their cyber insurance if they have implemented security controls outlined by Cyber Essentials, a government programme which has evolved since its launch ten years ago but which remains just as relevant today.

The way forward

Together, we’re going to have to change how we do things. As our community innovates, it must also build the defences and through those defences our resilience.

We have to make sure that technology is working for us as consumers, as users, as people; that the market for technology incentivises a ‘secure-by-design’ approach; that no-one treats security as a postscript.

Cyber security legislation and regulation, such as the new Cyber Security and Resilience Bill, are crucial steps towards hardening the UK’s cyber defences.

This will be an opportunity to broaden the scope of current regulations to protect more services and supply chains to put regulators on a stronger footing and to strengthen reporting requirements to build a better picture across government of cyber risk to the UK.

Conclusion

It’s not enough any more to talk about being resilient.

We must all take the crucial steps that bolster our defences, that improve and grow our capability to contest.

And that includes the ability to continue and recover on the occasions that attacks do get through, and this is often overlooked.

The NCSC has always believed that cyber security is a team sport – that is true now more than ever.

We need to work together to protect each other and build a deep understanding of just how dependent we are on our teammates.

The rules haven't changed but the field of play is evolving fast.

Together, we must act to safeguard all our interests and our prosperity.

Thank you for joining us today.

Read the Annual Review

PUBLISHED

3 December 2024

WRITTEN FOR

Public sector

Cyber security professionals

Large organisations

Small & medium sized organisations

DATE OF SPEECH

3 December 2024