# NCSC CEO's speech to mark the launch of the NCSC Annual Review 2021

**Lindy Cameron spoke at an event in the NCSC's London office to launch the organisation's Annual Review.**

Good morning, everybody. It's fantastic to be able to welcome you all to our London headquarters for the launch of the National Cyber Security Centre's fifth Annual Review.

These days we can often find ourselves talking at events over virtual links – and while technology has been a great help during the pandemic, it is absolutely wonderful to see so many faces in person.

One person who sadly is unable to join us today is the Director of GCHQ, Jeremy Fleming. He had intended to be here but has been called away to another meeting, and passes on his apologies.

You may have heard me on some broadcast media interviews this morning talking about the review, which is testament to the mainstream cut-through that our work has.

On the BBC Radio 4 Today programme, Amol Rajan introduced me in a rather unique way – by saying that cyber security is "no longer just for geeks and weirdos"!

Firstly, I'd like to pay tribute to all of the "geeks and weirdos" who have worked so hard to help us in our mission! But at the core of his message, Amol is right – cyber security is something that affects every organisation and individual in the UK. It has stopped being a niche concept and is now firmly established as a mainstream issue – and never more so than over the last year.

I became the NCSC's Chief Executive only a few days before the launch of the previous Annual Review, and it's with great pride that I invite you to read about what my amazing team has achieved over the last 12 months. It's been quite a year in cyber security.

I hope you agree that it is a good read, and testament to the hard work not just of my team but our colleagues in government, law enforcement and the wider private sector. Thanks to this collaborative effort, we have made great progress in our objective to make the UK the safest place to live and work online.

And it is only through these strong and trusted relationships that we are able to have the impact this year's annual review describes.

A particular highlight has been the work we did to support the UK's pandemic response – and in particular, the COVID-19 vaccine roll out.

Of the 777 incidents we dealt with, 20% were linked to the health sector and vaccines. And the brunt of those numbers stem from pro-active flagging of potential vulnerabilities that our team did to keep critical functions to the pandemic response as safe as possible.

To give you just one example, teams from the NCSC worked round the clock to help the University of Oxford's coronavirus vaccine researchers protect themselves from an attempted ransomware attack.
Without this intervention, there was a significant potential that the UK's COVID response could be delayed.

Ransomware was the most worrying trends we have seen over the last year. In my view it is now the most immediate cyber security threat to UK businesses and one that I think should be higher on the boardroom agenda.

That's one of the reasons why our staff have engaged with around 5,000 organisations from a range of sectors from farming and sport to education and Critical National Infrastructure. We have issued guidance and threat assessments to nearly 100 companies and universities.

The NCSC has been actively engaged in dealing with the ransomware threat for a number of years, from the WannaCry attack through to more recent examples such as the attack on Hackney Borough Council.

We have published guidance for organisations for a number of years and publicly reveal the trends we see – helping organisations to build their resilience.

As the threat has grown, we have significantly ramped up our outreach to specific sectors. This has included the creation of our Early Warning Service this year, which alerts organisations to threats as part of our Active Cyber Defence programme to protect organisations at scale.

Ransomware is of course a global threat and we have seen a growth in international incidents in the last year.

Our collaboration with international partners is a vital part of the response and we particularly welcome the vigour with which our colleagues in the United States are joining us in our pursuit of tackling this issue and mitigating its threat.

Governments cannot do this alone, however, and we strongly urge organisations play their part by visiting *ncsc.gov.uk* and following our guidance

Because cyber security is a team sport, and everyone has their role to play – it can't just be a problem for anyone to ignore and assume somebody else is solving. And the continued success of the Suspicious Email Reporting System is a source of pride for showing that this message is getting through. The British public are helping us to keep them – and others – safe.

Launched in partnership with the City of London Police, it has received 5.4 million reports from the public of potentially malicious material – leading to the removal of more than 50,000 scams and more than 90,000 malicious URLs.

And we also launched Cyber Aware – the intelligence service's first TV advertising campaign – directly engaging the British public with advice on how they can increase their cyber security as part of our work to defend democracy.

We want to take as much of the threat out of using technology as possible. That's why we've rolled out new Active Cyber Defence measures like the Early Warning Service, which alerts organisations to emerging threats.

Of course, attacks will still get through – and we have helped to mitigate some significant incidents this year, and where appropriate we have called out who was behind them and elsewhere.

A good example of this was following December's compromise of the SolarWinds IT system management platform. We used data from our ACD services to estimate the extent of damage, inform decision makers in government and support affected organisations.

Five months later, our assessment found that it was highly likely that Russia's Foreign Intelligence Service was behind the attack and subsequent targeting – and this was publicly attributed by the UK Government and our partners in the US.

One other area I would like to touch on is our commitment to giving Parliament and political parties the best support possible on cyber security.

This ranges from supporting on significant incidents against parties themselves, to briefing politicians if there is a significant cyber threat against them personally and to help them safeguard their personal communications and those of their private offices.

The NCSC takes this responsibility very seriously and will continue to do all we can to support parties, individuals and institutions across the political system.

There is still a long road ahead and we will continue to do our best to understand, reduce and respond to cyber attacks.

But I hope you agree that this review demonstrates the great cyber security work that has been delivered – by our team, but also by other organisations – within government, the private sector and law enforcement - and also the public.

I would like to say a huge thank you to everybody has helped to make the UK as safe from cyber threats as possible over the last year.

It is truly a team effort that helps to ensure all of the UK can make the most of the digital age and the opportunities it offers.

And I am delighted to continue today's event by welcoming to the stage one of the people who will be instrumental in helping us meet that ambition – the Chancellor of the Duchy of Lancaster, the Rt Honourable Steve Barclay MP.

Read the Annual Review 2021

**PUBLISHED**

17 November 2021

**WRITTEN FOR**

Public sector

**DATE OF SPEECH**

17 November 2021

**LOCATION**

Nova South, London