Risk facing UK "widely underestimated", cyber chief to warn in first major speech

Richard Horne will describe the cyber risks facing the nation as “widely underestimated” and call for collective action against an increasingly complex array of threats.

- Head of GCHQ’s National Cyber Security Centre (NCSC) will use first major speech to emphasise the need for sustained vigilance in an increasingly aggressive online world.
- Richard Horne urges organisations to collectively boost resilience by following NCSC advice amid signs of widening gap between risks the UK faces and its ability to handle them
- Comments made in speech to launch the NCSC's eighth Annual Review, which will highlight growing threat including from state actors

The nation's new cyber security chief will use his first major speech today to issue a rallying call for collective action against an increasingly complex array of threats.

Speaking at the National Cyber Security Centre’s (NCSC) London headquarters for the launch of its Annual Review, Richard Horne will describe the cyber risks facing the nation as “widely underestimated”, warning that Britain and its allies are competing in a high-stakes contest for cyberspace. He will say:

> “What has struck me more forcefully than anything else since taking the helm at the NCSC is the clearly widening gap between the exposure and threat we face, and 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 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.”

Turning to the changing threat landscape, Richard Horne will highlight a combination of the UK’s growing dependency on technology and adversaries who are conspiring to use it against us. He will say:

> “Hostile activity in UK cyberspace has increased in frequency, sophistication and intensity. We see this in the intelligence we can access through being part of GCHQ.
>
> “Actors are increasingly using our technology dependence against us, seeking to cause maximum disruption and destruction.
>
> “Last week, the Chancellor of the Duchy of Lancaster warned about the aggression and recklessness of cyber activity we see coming from Russia. And with our partners, including at the NPSA, we can see how cyber attacks are increasingly important to Russian actors, along with sabotage threats to physical security, which the director general of MI5 spoke about recently.
>
> “All the while, China remains a highly sophisticated cyber actor, with increasing ambition to project its influence beyond its borders.
>
> “And yet, despite all this, we believe the severity of the risk facing the UK is being widely underestimated.”

Richard Horne will also highlight the real-world impact of cyber attacks, drawing on recent examples that have disrupted lives, jeopardised safety, and eroded trust in our online world. He will say:

> “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.
>
> “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.”

On the launch of the NCSC’s Annual Review, **Chancellor of the Duchy of Lancaster Pat McFadden said**:

> “As a nation, we must harness technology to drive growth and opportunity, without leaving ourselves vulnerable to the ever-growing threat from malicious cyber actors.
>
> “The NCSC is at the centre of the Government's efforts to strengthen the cyber resilience of organisations and individuals.
>
> “We must work alongside industry to meet the increasingly sophisticated challenges we face and make the UK the safest place to live and work online.”

NCSC Annual Review

In the Review, published today (3 December), the NCSC highlights the increasingly challenging online environment that the UK and its allies are navigating to ensure a safe and prosperous digital world for its citizens.

State threat

Characterising the 2024 cyber threat landscape as “diffuse and dangerous”, the Annual Review notes a rising frequency of cyber incidents and a growing severity in their impact.

Over the past 12 months, the NCSC has observed how conflicts are fuelling a volatile threat landscape, including Russia’s deployment of destructive malware

against Ukrainian targets, and routine attempts to interfere with the systems of NATO countries in support of its war effort.

China is described as a highly sophisticated and capable actor targeting a wide range of sectors. In February 2024, the NCSC co-signed an advisory on observed compromises of U.S. Critical National Infrastructure (CNI) by Volt Typhoon, and in March 2024 the UK government called out China state-affiliated actors for targeting democratic institutions.

Iran-based threat actors remain aggressive in cyberspace, and the Democratic People's Republic of Korea (DPRK) continues to prioritise raising revenue to circumvent sanctions and collect intelligence in its cyber activity.

Criminal threat

Ransomware is highlighted as the most pervasive cyber threat to UK organisations, highlighting the financially motivated ransomware attack on Synnovis, a supplier to the NHS, which had a significant impact on citizens.

Elsewhere, cyber criminals' use artificial intelligence (AI) to increase the volume and heighten the impact of cyber attacks. In January 2024, the NCSC published an assessment of the near-term impact of AI on the cyber threat, highlighting how it can be used for reconnaissance, social engineering and analysis of exfiltrated data.

The Annual Review also notes an observation from the NCSC that the application of AI to cyber defence will exceed the uplift in any adversary capability or application.

Incidents

This year, the NCSC's Incident Management team handled **430 incidents**, compared to 371 the previous year. Of these, 347 involved some level of data exfiltration and 20 incidents involved ransomware.

The top sectors reporting ransomware activity into the NCSC this year were academia, manufacturing, IT, legal, charities and construction.

Elsewhere, the Incident Management team issued **542 bespoke notifications** informing organisations to a cyber incident impacting them and provided advice and guidance on how to mitigate it. This was more than double the 258 bespoke notifications issued last year.

Almost half of the bespoke notifications sent this year related to pre-ransomware activity, enabling organisations to detect and remove precursor malware before ransomware was deployed.

NCSC Annual Review 2024

Take a look at the NCSC's Annual Review 2024, showcasing key developments and highlights between 1 September 2023 - 31 August 2024.

PUBLISHED

3 December 2024

WRITTEN FOR

Large organisations

Public sector

Cyber security professionals

Small & medium sized organisations

NEWS TYPE

/

General news