Cyber chief: UK facing AI-powered attacks on critical infrastructure within two years

The NCSC warns that 'tech on the cheap' has left UK organisations exposed to AI uncovering and exploiting longstanding cyber security weaknesses and calls for urgent investment in resilience.

- AI-powered malware highly likely to be used in ransomware attack on Britain's critical national infrastructure by 2028, new report warns.
- Head of GCHQ's National Cyber Security Centre to warn, as a society, the era of "tech on the cheap" at expense of security is over.
- New *State of the Cyber Nation* report calls on organisations to make "significant changes" to avert future where AI is used against UK economy and society.

The UK's critical national infrastructure should be braced for a ransomware attack involving AI-powered malware by 2028, a new report published today [Tuesday 3 November] by the National Cyber Security Centre (NCSC) – a part of the UK's signals intelligence agency GCHQ says.

The NCSC's *State of the Cyber Nation* warns that within the next two years, AI adoption by hostile actors is "highly likely" to increase the scale and efficiency of their operations, including ransomware attacks, social engineering, and vulnerability exploitation.

In a speech to launch the report, the CEO of the NCSC, Dr Richard Horne, is set to say that the AI revolution must force UK organisations to reckon with the current state of their cyber security, as new technologies will expose vulnerabilities, failings and underinvestment at an unprecedented speed and scale in the years ahead. The head of the UK's cyber agency will also set out how artificial intelligence represents the critical opportunity to improve the UK's collective cyber resilience, but that organisations must take urgent action to address foundational investments and weaknesses or risk adversaries exploiting them instead.

The warning comes as the government is investing in the UK's defence and resilience capabilities, including greater investment in cyber defence, while taking action through the introduction of the Cyber Security and Resilience Bill and the forthcoming National Cyber Action Plan to strengthen the UK's defences, deter hostile state aggression, keep essential services running and keep the British people safe.

Alongside calls for organisations to strengthen their resilience, last week the Chancellor also announced greater investment in capabilities to help the UK harness AI for cyber defence, including £60 million into developing the first phase of a national Cyber Shield, £70 million for a new National Exposure and Real-Time Vulnerability (NERV) Centre to identify vulnerabilities across critical infrastructure and the economy, and a new AI Cyber Security Centre of Excellence, ran by the National Cyber Security Centre, in Manchester to develop world leading AI security expertise within government.

This year's report suggests that the UK is at a point of "enormous consequence" for cyber security and that organisations across the UK must make use of the tools, standards and frameworks that already exist and are evidenced to protect them from conventional and AI-powered cyber attacks.

The NCSC is imploring organisations across the UK to face what Dr Horne is calling "a moment of choice". In a speech to launch the report, NCSC CEO is expected to say:

> *In the coming months, we face a real prospect of an unprecedented rise in the number of cyber incidents. But we must be clear that is not because AI has invented new ways to attack us. But because vulnerabilities that have been tolerated for far too long can now be discovered and exploited at a scale that was once unimaginable.*
>
> *"For decades, we have collectively got away with doing tech on the cheap.*
>
> *"We can be a nation where leaders of all organisations actively choose to invest with urgency... And where all organisations make security and resilience a fundamental requirement, not an afterthought.*

“The collective result would be a source of enduring national strength for us all.

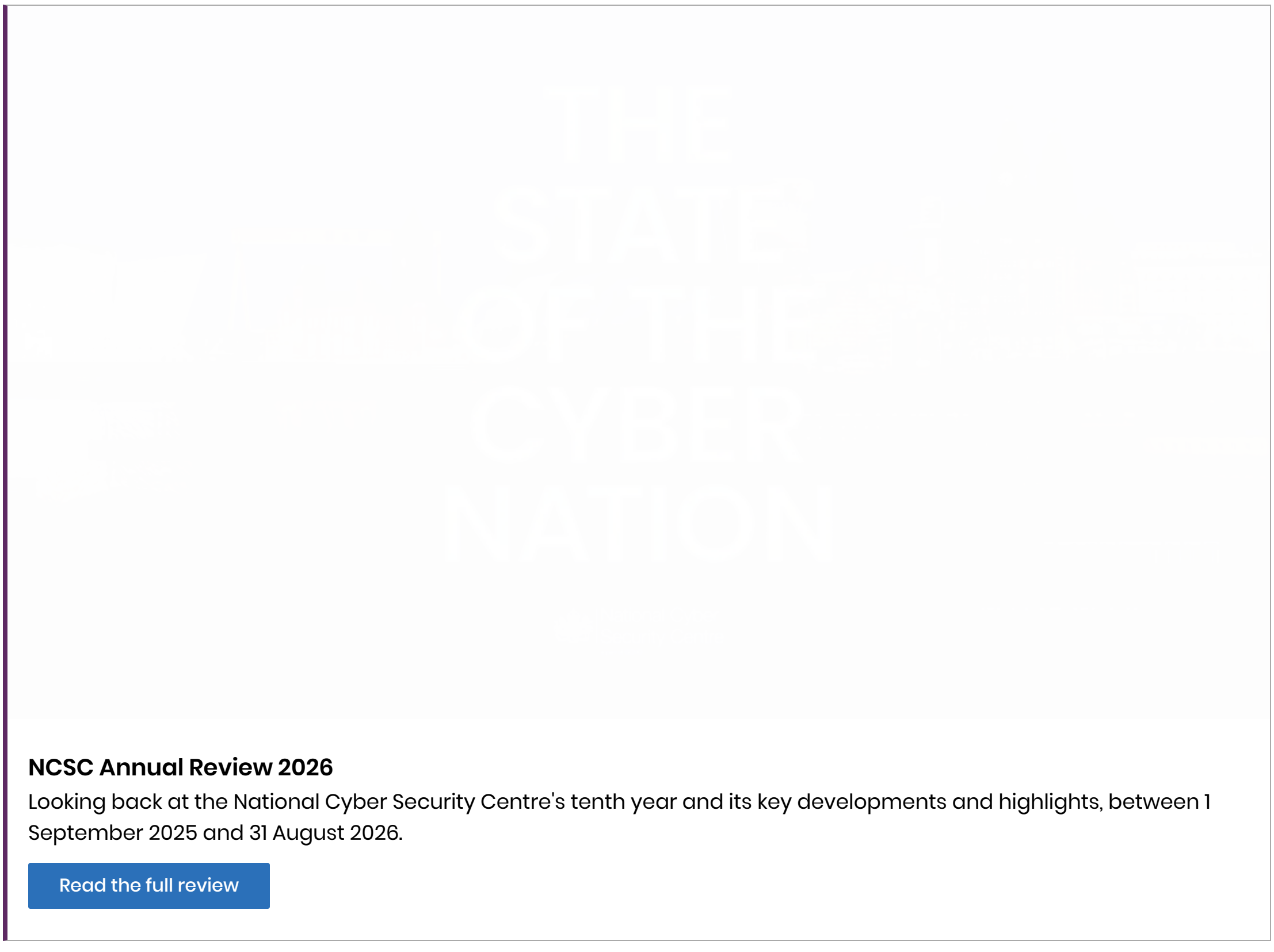
Dr Horne will urge all organisations across the country to “take the responsibility now to make different choices”, including addressing the failure to adequately invest in their technology; not having technology unnecessarily connected to the internet; and making Cyber Essentials the starting point for cyber security, not the end goal, with organisations building greater resilience according to their size, complexity and risk.

He will say that failing to make these choices will result in leaders “having to look their investors, shareholders, employees, customers, suppliers, in the eye and explain…when food isn’t on shelves, lights aren’t on, businesses have gone under.”

In their tenth year, the National Cyber Security Centre plays a more important role than ever before, defending our security on the cyber frontline.

“The NCSC's latest annual report shows cyber threats are growing more sophisticated. We're using the power of AI to help stay ahead of those who seek to do us harm, with a new national Cyber Shield and an AI Cyber Security Centre of Excellence.

Security Minister Dan Jarvis



NCSC Annual Review 2026

Looking back at the National Cyber Security Centre's tenth year and its key developments and highlights, between 1 September 2025 and 31 August 2026.

Read the full review

PUBLISHED

3 November 2026

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

Small & medium sized organisations

NEWS TYPE

General news