Richard Horne's speech at the NCSC Annual Review 2026 launch

NCSC CEO Richard Horne launches the Annual Review 2026: The State of the Cyber Nation.



Introduction

A woman sprints down the tube staircase.

In that moment, her future could go one of two ways.

In one, she hops through the doors that are sliding shut.

She arrives home early to discover her partner having an affair, ends her relationship and changes the course of her life.

In the other, she misses the doors and takes a later train.

In this version of the future, the woman stays with her unfaithful partner and struggles to support his choices.

Now, to many of you, that will be familiar as the plot of the film “Sliding Doors”.

Which might seem an odd way to introduce our “State of the Cyber Nation” report.

But the theme of that film, that seemingly inconsequential moments and decisions can alter the trajectory of our futures.

Couldn’t be more relevant for cyber security today.

Ten years on from the NCSC’s formation, it is clear that our nation is living through a moment that, in hindsight, we will see as one of enormous consequence.

A *Sliding Doors* moment.

A moment of choice.

There is much speculation and debate about what our future might look like in a world of ever more capable artificial intelligence and what that means for our collective cyber security.

There is no avoiding it.

Whether you and your organisation choose to harness AI or not, its impact will be felt by us all but there is an uncomfortable truth that the immediate cyber security risk we face from AI is not new.

Technology foundations

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.

It is because vulnerabilities that have been tolerated for far too long can now be discovered and exploited, at a scale and pace that was once unimaginable.

And because far too many of our organisations and supply chains rest on weak technology and operational foundations.

The very same foundations that AI is now being built upon.

The Leaning Tower of Pisa gives a useful metaphor.

It's renowned, not for its beauty, or the brilliance of its circular design but because it was built on flawed foundations.

That, it transpired, could not bear the weight placed upon them.

Now the difference is, we already know that the technology foundations our society depends on need reinforcing and reinvestment.

That's why in the NCSC we continue to stress the importance of cyber security fundamentals, which are really technology and operational fundamentals.

I am proud of the work we do in the NCSC 24 hours a day, every day of the year, to intervene and disrupt cyber attacks against our nation at scale.

Working with incredible partners in industry, for example, issuing a total of over 110,000 proactive notifications and Early Warning alerts to UK organisations in response to the PHP vulnerability.

But as Ken McCallum said in his speech last month.

Everyone has a stake in our security.

Every person, every organisation, our technology providers, frontier AI labs have a responsibility to play their part to build organisations and a society in the UK that can withstand the volume of cyber attacks we may face.

If leaders of organisations of every size and type do not take the responsibility now to make different choices then they will one day have to look their investors, shareholders, employees, customers, suppliers, families and friends in the eye and explain why, despite knowing the consequences, they failed to make the choices required.

When food isn't on the shelves, when lights aren't on, businesses have gone under. We may have to explain that we saw the warning signs, understood the risks and still didn't make the right choices.

Why we remained wilfully blind.

Tech on the cheap

For decades we have collectively got away with tech on the cheap.

End-of-life systems kept running for just one more year well-needed upgrades pushed back, as a 'cost efficiency' and technology providers failing to invest in security by design and default.

We have installed technology then failed to invest in it throughout its lifecycle.

Granted access where it was convenient rather than where it was necessary.

Procured services based solely on their price without asking whether the technology and operations underpinning them was resilient or secure.

And failed to put in place the monitoring needed to detect when things go wrong.

All of which are not desirable features.

They're fundamental requirements.

The very foundations of cyber security that we recognise through Cyber Essentials have championed for so many years and are the foundations of a resilient business for most organisations in an AI-enabled world.

Now importantly, that also carries through to the technology that underpins the automation of physical processes that are vital to modern life.

Electricity switching, sluice gates in water facilities, dam operations, manufacturing lines, heating, refrigeration controls.

Whilst they're not seen as traditional IT, they too are not built on the strong foundations they require.

Their resilience and security is even more overlooked in investment decisions.

Our resulting exposure as a society is huge and increasingly exploited in cyber attacks as we are seeing in the disruption of refrigeration units across Europe.

Threat landscape

As Ken warned a few weeks ago the period of post-Cold War stability has ended.

Every day, our military networks are subjected to sustained and persistent, widespread attempts to penetrate our systems.

Including notable campaigns by Russia that intentionally fall below the threshold of armed conflict as they escalate their attempts at hybrid warfare.

Despite the pressures of the Middle East conflict, Iran is still carrying out malicious cyber operations globally including against the UK and individuals that are seen as a threat to the regime putting them at risk of physical harm.

And all the while, recent “smash and grab" type ransomware attacks by criminals have seen threats to publish stolen data, in attempts to extort victim organisations, with people across the country facing uncertain personal implications.

And we know that China highly likely has the intent and is best positioned to use AI for operations against our critical national infrastructure and other strategic targets with their activity representing the most sophisticated and sustained cyber challenge the UK faces.

And artificial intelligence it is a set of machine processes and may never mean us harm, but in the hands of those who do it can become a force multiplier increasing the speed and scale of our adversaries' operations.

AI is our greatest opportunity

Yet the same technology that can strengthen the hand of our adversaries can also strengthen our own.

As I’ve said before, AI has the potential to be one of the greatest opportunities in cyber defence.

It's enabling vulnerabilities to be found and fixed faster than ever.

Major technology providers are now fixing hundreds of vulnerabilities in a single update. The Linux Kernel Project alone patched more than a thousand vulnerabilities last month.

And we are harnessing it.

Last week, the Chancellor reinforced that commitment by backing the national Cyber Shield as you just heard from Minister Lloyd.

And a new National Exposure and Real-Time Vulnerability Centre will use AI to identify vulnerabilities across our critical infrastructure and economy.

Working with partners across government from the AI Security Institute on the secure development and deployment of AI, through to the AI Threat Assessment Centre, the National Protective Security Authority, The Government Cyber Unit and many others we are ensuring that the future of AI is one that serves our security, our prosperity and the public good.

And resilience isn't built by technology alone.

It too rests upon foundations, governance, accountability and legislation.

And that's why, the Cyber Security and Resilience Bill is such a vital step forward it will establish a minimum level of resilience across our critical national infrastructure.

And the National Cyber Action Plan to be announced soon will ensure the actions needed to strengthen our nation's defences are taken.

The future we can build

So back to our *Sliding Doors* moment.

There is a future that is in our gift a future made possible because we all took the actions required to reinforce our technology foundations.

We can be a nation where leaders of all organisations actively choose to invest with urgency and not delay in replacing end-of-life technology.

Where critical physical systems are inaccessible to attackers.

Where passkeys are adopted as the norm.

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.

We can have an economy that is able to withstand disruptive cyber attacks.

Not because the threats we face have vanished.

Because they will not.

And not because technology stops evolving.

Because it will not.

But because we realised we had to choose before crises forced our hand.

Just like the generations before us built the roads, railways and energy networks that transformed Britain and powered its prosperity for decades to come.

It is now our turn and our responsibility to shore up the foundations of the technology upon which we, and future generations, rely so that we do not build the digital Leaning Tower of Pisa.

As our AI Minister Kanishka Narayan said a few weeks ago, the consequences of this moment we find ourselves in could be felt for generations.

Conclusion

There may come a day when the choices available to us now have passed...

The doors have closed, train has left the station, and we've been left behind.

A day when boardroom conversations or living room discussions are no longer about what should be done, but about what should have been done.

Let us be the generation that got on the train.

So that when we are asked, 'where were you when AI changed everything?'

Our answer will be found in the actions we took.

Thank you.



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

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Public sector

DATE OF SPEECH

3 November 2026

LOCATION

Nova South, London