National Cyber Security Centre
a part of GCHQ

It's time to act

Open your eyes to the imminent risk to your economic security.

Annual Review 2025

National Cyber Security Centre
a part of GCHQ

Cyber risk is no longer just an IT issue — it's a boardroom priority.

Cyber incidents can disrupt operations, damage reputation, and lead to serious financial and legal consequences. For today's leaders, cyber resilience is about having the strategic foresight to prepare for, respond to and recover from cyber attacks.

Co-created with industry leaders for industry leaders, Cyber Governance Training ensures boards are equipped to meet their cyber security responsibilities with clarity and confidence.

It's time to act. Start your **Cyber Governance Training** today.

ncsc.gov.uk/cyber-governance-for-boards

Contents

‘For too long, cyber security has been regarded as an issue predominantly for technical staff. This must change. All business leaders need to take responsibility for their organisation’s cyber resilience.’

Foreword

Nobody wants to believe that their business operations could grind to a halt following a cyber attack. But any leader who fails to prepare for that scenario is jeopardising their business's future.

Over the last year, cyber attacks on household brands have brought the NCSC's work to the forefront of public consciousness. Empty shelves and stalled production lines are a stark reminder that cyber attacks no longer just affect computers and data, but real business, real products, and real lives.

We've also seen how organisations that suffer a cyber attack can experience financial losses, lengthy service disruption with customers' personal data often caught in the crossfire.

The recent cyber attacks must act as a wake-up call. The new normal is that cyber criminals will target organisations of all sizes, operating in any sector. From local coffee shops to providers of critical national infrastructure, every organisation must understand their exposure, build their defences, and have a plan for how they would continue to operate without their IT, (and rebuild that IT at pace) were an attack to get through.

In today's volatile and technology-dependent world, online attacks can also be the outcome of geopolitics. As this year's review illustrates, nearly half of all incidents handled by the NCSC over the last 12 months were of national significance.

And 4% of these were categorised as 'highly significant' – attacks which we define as 'having a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy.' That marks a 50% increase in highly significant incidents, an increase for the third consecutive year.

These numbers clearly illustrate that the challenge we face is growing at an order of magnitude.

We do see some organisations – ones with well-thought-through plans for continuity and recovery already in place – respond well to disruptive cyber attacks. This is what all organisations should aspire to, because almost every business depends on technology to function. But for too long, cyber security has been regarded as an issue predominantly for technical staff. This must change. All business leaders need to take responsibility for their organisation's cyber resilience.

Cyber security is now critical to business longevity and success.

It is time to act.

Richard Horne — CEO, NCSC

Open letter

An open letter from Shirine Khoury-Haq, CEO of The Co-op Group, reflecting on the high-profile cyber attack.

Dear business leaders & decision makers,

I am writing this letter as a CEO whose business has just experienced a cyber attack, in the hope that by sharing some of our experiences and learnings, you can all feel better equipped in dealing with what is a mounting issue for us all.

On April 25th, our Co-op was the victim of a multi-stage cyber attack, as confirmed by the National Cyber Security Centre and National Crime Agency, which were both close to our investigation.

While you can plan meticulously, invest in the right tools and run countless exercises, nothing truly prepares you for the moment a real cyber event unfolds. The intensity, urgency and unpredictability of a live attack is unlike anything you can rehearse. That said, those drills are invaluable - they build muscle memory, sharpen instincts, and expose vulnerabilities in your systems.

At Co-op, our routine investment in security, the deliberate segregation of systems and frequent testing laid a strong foundation for our response to this cyber attack. It was, however, the extraordinary talent of our in-house teams and partners that made the difference.

Together, we responded quickly and decisively, mitigating the impact of the primary attack, blocking further attempts and maintaining our ability to still serve our members and customers in our frontline business areas, despite the significant business interruption and impact that this incident created.

Despite our swift and effective action to defend our Co-op from the hackers, some of our members' data was accessed, such as names, contact details and dates of birth. As a member-owned business, this affected us all deeply and our apology was transparent and swift.

The attack has had a significant impact on me, my colleagues and on our members. I will never forget the strain it put on those people making it right, or the concern it has given our members, to whom I answer.

While the security of your systems will no doubt remain on your radar, please continue to account for the fact that the timing and nature of a cyber attack like this is unpredictable. New challenges will always emerge and threats to corporate infrastructures will never stop.

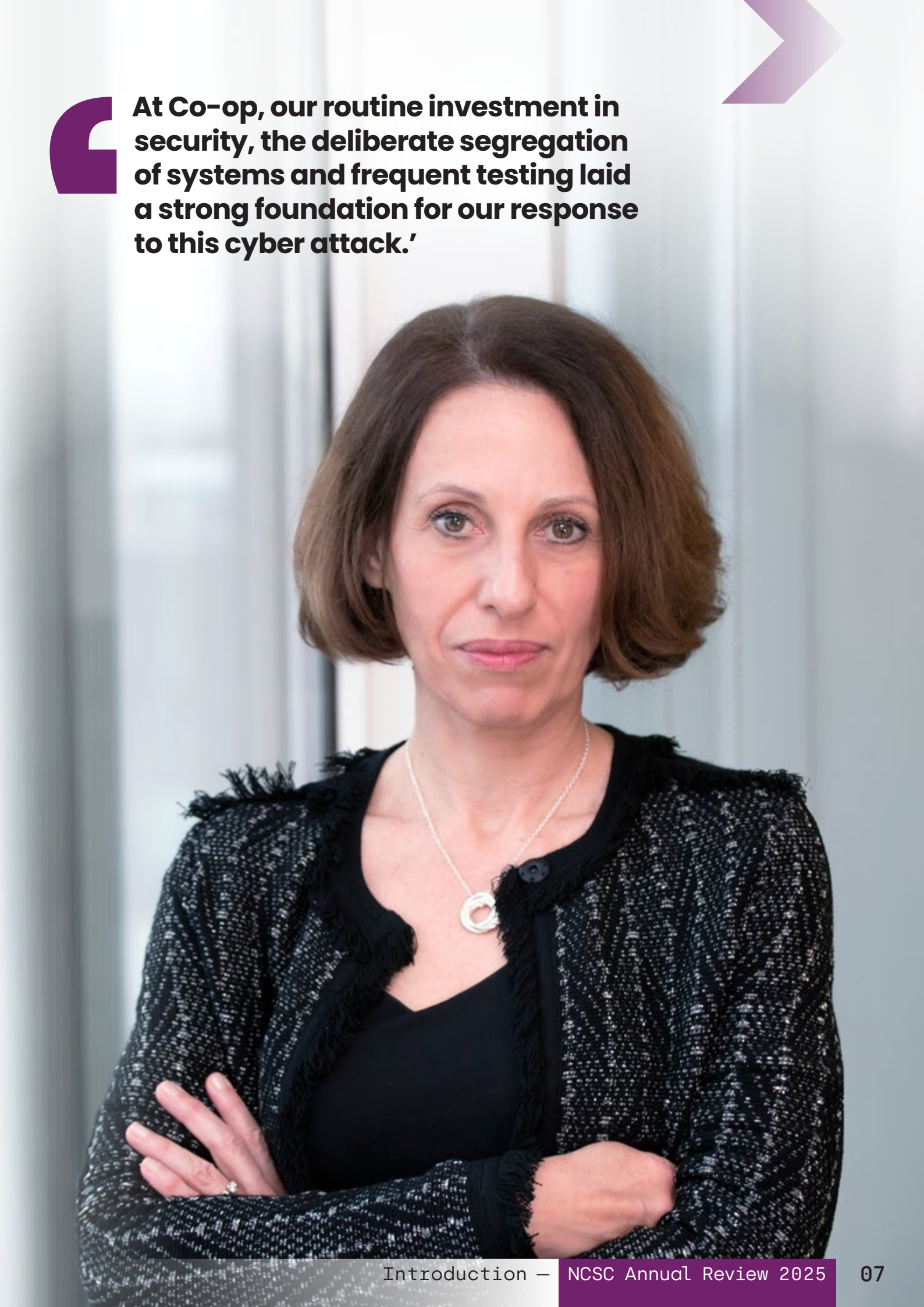
And where I am grateful for my teams and experts, I am even closer now to how we defend against cyber threats, and I am routinely engaging with NCSC guidance.

The buck stops with us as senior leaders. Please continue to consider the best route to protecting your business, but also the best means to defend against an attack, including supporting customers and colleagues, at every possible stage.

Yours sincerely,

Shirine Khoury-Haq
— CEO, The Co-op Group

At Co-op, our routine investment in security, the deliberate segregation of systems and frequent testing laid a strong foundation for our response to this cyber attack.'



Ministerial foreword

The United Kingdom is one of the most digitally connected countries in the world.

That is something to be celebrated. With so many aspects of people's lives having an online dimension, it is absolutely right that we should seek to maximise the benefits of rapid technological progress.

Yet despite the myriad of opportunities to harness these advancements for the good of our society and our economy, the potential for bad actors to exploit them and cause harm also continues to grow. The more we expand and innovate, the greater our exposure to risks.

Recent high-profile cases have underscored the scale and intensity of the threat and the devastating impact cyber attacks can inflict. These incidents – along with the many others that do not attract national and international attention – are a sharp reminder of the need for constant vigilance.

All of this means that cyber security has never been more pivotal to our national security and our economic health. Within this context, the ongoing effort to keep people and organisations safe online, spearheaded by the National Cyber Security Centre (NCSC), is critical.

As this review demonstrates, the NCSC has made strong progress in a number of areas. Over 13,000 organisations are part of the free Early Warning service, giving them exclusive access to information on potential cyber attacks. The Takedown Service has seen over 1.2 million phishing campaigns removed from the internet, with half taken down within an hour of being detected.

These are welcome developments, but we must go further. I will continue working closely with our world-leading intelligence and law enforcement community, including the outstanding specialists at the NCSC, to detect, disrupt, deter and defeat those who threaten our security and economic wellbeing.

This is not a task one department or service can take on alone. As with other national security threats, it needs a whole-system response, which is what my role as a joint Home Office and Cabinet Office Minister will deliver. It is also important to emphasise that this goes beyond government and our partner agencies – everyone has a role to play.

The United Kingdom is one of the most technologically advanced countries on earth. Our quest for further progress depends on strong security, which is why we will pursue both with equal determination and care.

Dan Jarvis MBE MP
— Minister of State (Minister for Security)

‘Cyber security has never been more pivotal to our national security and our economic health.’

> **Don't be an easy target; prioritise cyber risk management, embed it into your governance, and lead from the top.'**

Message from Director GCHQ

This year, the realities of cyber attacks have hit the headlines and impacted the bottom lines of many companies. Incidents like the high-profile attacks on Marks & Spencer, the Co-op Group and Jaguar Land Rover serve as a stark reminder that the cyber threat is not just an abstract concept but a real one with real-world costs.

The importance of vigilance, resilience and the collective responsibility to defend against an increasingly complex threat is clear. Cyber security is a matter of business survival that demands action.

I am immensely proud of the entire NCSC team for their exceptional efforts in safeguarding the UK's digital landscape. Their expertise and dedication are an asset to the country. Their work continues to raise awareness, build expertise and reinforce the security of our national infrastructure. But cyber security is a shared responsibility – an obligation for individuals, businesses, and government alike to ensure a more secure digital future for everyone.

It's time to act. We must all play our part and take decisive steps. Don't be an easy target; prioritise cyber risk management, embed it into your governance, and lead from the top.

Anne Keast-Butler — Director GCHQ

The NCSC at a glance

The National Cyber Security Centre, a part of GCHQ, helps businesses, the public sector and individuals protect the online services and devices that we all depend on.

Our mission is to make the UK the safest place to live and work online so that everyone – whether at work or at home – can navigate the cyber landscape safely and with confidence.

Since 2016, the National Cyber Security Centre (NCSC) has safeguarded the UK's critical systems and online services, delivering world-leading guidance, tools and frameworks for business and citizens alike. When cyber attacks occur **–** or services are disrupted **–** we provide incident response to minimise harm, restore operations, and help organisations get back on their feet.

The NCSC was formed by combining separate parts of government, MI5 and GCHQ to create the National Technical Authority for cyber security. We lead the UK's defence against the most advanced cyber threats, including those from nation states, hackers, and cyber criminals.

The NCSC works closely with international allies, law enforcement and the UK's intelligence and security agencies to ensure we understand the cyber threat, and how we can defend against it.

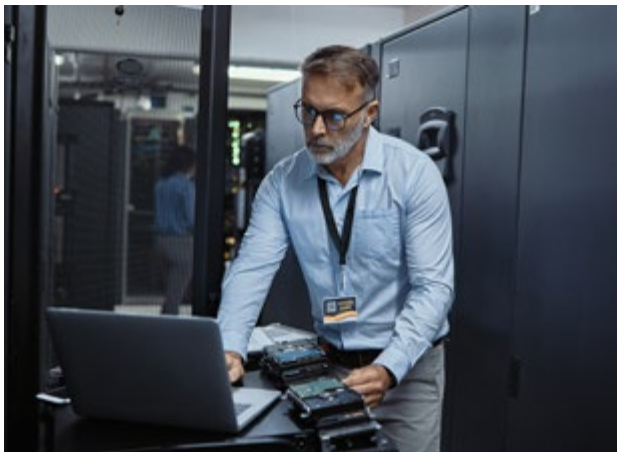
We also harness talent across schools, universities, and the tech community, driving research into emerging technologies to explore new ways to reduce harm at scale. At the same time, we are investing in the UK's national security by nurturing the next generation of expertise that the expanding cyber security sector needs to thrive.

A shared responsibility

Whether you're working for critical infrastructure making sure the lights stay on, or simply setting up your child's phone, the UK's cyber security is a shared responsibility where everyone needs to play a part. Only then can we stay ahead of the cyber criminals and hostile states that seek to do us harm.

What is cyber security?

Cyber security helps individuals and organisations reduce the risk and impact of cyber attacks. Its core function is to defend the digital services and devices we rely on from online threats, which includes safeguarding the vast amounts of data and personal information stored locally or in the cloud. Cyber security also ensures that innovative and emerging technologies (such as AI) can be deployed in a secure way, so the opportunities they present can be fully realised.



Why is cyber security important?

Cyber security matters because most organisations in the UK rely on digital technology to function. It ensures the UK's critical national infrastructure continues to operate in our increasingly connected world, and that governments can provide essential services.

> **'Cyber security should therefore be a key part of every organisation's operational resilience.'**

Organisations that suffer a cyber attack or data breach can expect financial losses, lengthy service disruption, regulatory response and reputational damage. Cyber security should therefore be a key part of every organisation's operational resilience. When it's done well, cyber security can be a catalyst for innovation and an enabler of growth, not just a 'necessary evil' or compliance function.

On an individual level, phones, smart devices, online services and the wider internet are now a fundamental part of modern life. Cyber security can prevent criminals from accessing our accounts and services, and helps us to navigate our online lives, safely and with confidence.

National Cyber Security Centre
a part of GCHQ

Free cyber security toolkit from the cyber experts at the NCSC

The **Cyber Action Toolkit** is a free, personalised cyber security solution for sole traders, micro businesses and small organisations that turns cyber protection into simple, achievable steps for your business.

With built-in features that recognise your progress, you can work at your own pace, helping you protect your business's money and reputation from cyber criminals.

It's time to act. Try it now.

cybertoolkit.service.ncsc.gov.uk

2024–25 Timeline

September 2024

Attribution **5** — UK and allies uncover Russian military unit carrying out cyber attacks and digital sabotage for the first time.

Advice **18** — The NCSC and allies issue advice to counter China-linked campaign targeting thousands of devices.

Speech **19** — The NCSC CEO discusses how the global threat picture remains unpredictable at Aspen Cyber Summit with fellow Five Eyes cyber security leaders.

Alert **27** — UK and US issue alert over cyber actors working on behalf of Iranian state.

October 2024

News **7** — Dr Richard Horne starts his role as the new CEO of the NCSC.

Guidance **7** — The NCSC publishes new guidance that helps CISOs communicate with Boards to improve oversight of their cyber risk.

News **15** — All UK schools now eligible for free PDNS cyber resilience service following successful rollout.

Speech **16** — The NCSC CEO calls for greater global resilience against online security threats at Singapore International Cyber Week.

News **23** — Cyber Essentials marks a decade of boosting businesses' cyber defences with an event in the House of Lords.

Campaign **26** — Five Eyes launch Secure Innovation guidance for tech startups.

November 2024

Campaign **18** — UK's cyber security and law enforcement bodies launch Black Friday campaign urging citizens to turn on 2-step verification.

December 2024

Speech **3** — The NCSC CEO describes the cyber risk facing the nation as "widely underestimated" at the launch of the NCSC annual review.

January 2025

Consultation 14 Counter ransomware consultation launched by the Home Office with support from the NCSC.

Blog Post 15 The NCSC highlights the merits of choosing passkeys over passwords to help keep online accounts more secure.

February 2025

Guidance 4 The NCSC and international cyber agencies unveil new guidelines to secure edge devices from increasing threat.

Guidance 5 The NCSC and the NPSA develop guidance and resources for the UK's research and innovation sector to combat the increasing threat.

Event 13 The NCSC CEO attends Munich Security Conference and speaks on a panel about "Emerging Cyber Threat" along with counterparts from Germany and Ukraine.

March 2025

Campaign 1 The NCSC joins the government's Stop! Think Fraud campaign and highlights cyber security advice to help citizens stay safe online.

News 8 Winning teams from 2024/25 CyberFirst Girls competition attended a prize-giving ceremony at Jodrell Bank.

Guidance 20 New guidance from the NCSC outlines a three-phase timeline for organisations to transition to quantum-resistant encryption methods by 2035.

Blog Post 28 The NCSC welcomes DSIT's Cyber Security and Resilience Policy Statement which sets out a series of legislative proposals that will help tackle the increasingly prolific and diverse cyber threats to the UK.

April 2025

Event 1 The NCSC CEO co-hosts an industry roundtable in Manchester with NCC Group.

Training 8 DSIT and the NCSC launch the Cyber Governance Code of Practice and Training to enable Boards to govern cyber risks with confidence.

Advisory 9 The NCSC and international partners publish new information and mitigation measures for those at high risk from two spyware variants - BADBAZAAR and MOONSHINE.

May 2025

News 1 — The NCSC leads HMG's response in supporting the retail sector after a number of incidents affect major high street names such as Marks & Spencer and Co-op Group.

Event 6 — The NCSC hosts CYBERUK, the UK government's flagship cyber security event, which convened over 2,000 delegates in Manchester.

Assurance 8 — The Cyber Resilience Test Facilities and Cyber Adversary Simulation schemes mark a significant step forward in NCSC's mission to enhance the UK's cyber resilience.

Advisory 21 — UK and allies expose Russian intelligence campaign targeting western logistics and technology organisations.

Technical 22 — The NCSC and DSIT launch new ETSI standard for AI to set a benchmark for securing AI systems and protecting them from evolving cyber threats.

June 2025

Guidance 4 — New principles developed with industry and government partners to help organisations achieve the conditions to underpin a cyber secure culture.

July 2025

Scheme 10 — The NCSC, NPSA, DSIT and DBT launch the Secure Innovation Security Reviews Scheme to support the UK's emerging technology sector.

Attribution 18 — In support of UK sanctions against GRU actors, the NCSC leads international attribution for Russian military intelligence group APT28.

News 21 — For the first time, BBC cameras are permitted to film behind the scenes at the NCSC as part of its dedicated programme on ransomware.

August 2025

News 6 — Cyber Assessment Framework v4.0 launched to support essential service providers in strengthening cyber risk management amid growing threats.

Attribution 27 — UK and allies expose China-based technology companies for enabling global cyber campaign against critical networks.


ACCESS
CARD

Chapter 1

Countering the cyber threat

The cyber threat to the UK

Understanding the escalating threat across complex environments.

State actors continue to present a significant threat to UK and global cyber security, aided by an evolving cyber intrusion sector. As threats intensified, our incident management team faced a record number of nationally significant incidents.

The NCSC works across government, and in partnership with international allies, industry and academic colleagues, to deter, degrade and detect the cyber threat posed by hostile nation states and cyber criminals. Through timely advisories and public attributions, we help organisations understand the nature of these threats, assess their exposure, and take informed action to strengthen their defences.

China

China continues to be a highly sophisticated and capable threat actor, targeting a wide range of sectors and institutions across the globe, including the UK. In September 2024, the NCSC and international allies **exposed a covert network operated by a China-linked company called Integrity Technology Group also known as Flax Typhoon.** The actor managed a botnet (that is, a network of internet-connected devices that are infected with malware to conduct co-ordinated cyber attacks) consisting of over 260,000 compromised devices around the world.

Further, in August 2025, the NCSC co-sealed a **cyber security advisory** with international partners linking three China-based companies to a campaign **targeting foreign governments** and critical networks. The activities described in the advisory partially overlap with campaigns previously reported by the cyber security industry most commonly under the name Salt Typhoon.

Russia

Russia continues to act as a capable and irresponsible threat actor in cyberspace. Russia's most disruptive threat activity continues to be focused on Ukraine, in support of their illegal military campaign. The NCSC continues to publicly expose Russian cyber activity (such as the **Authentic Antics malware** which steals victims' login details and tokens to enable long-term access to email accounts) and give mitigation advice. This creates a more challenging environment for Russian actors to operate in.

Russia's invasion of Ukraine and the ongoing Israel-Gaza conflict have also inspired a growing number of Pro-Russia hacktivist groups seeking to target the UK, Europe, US, and other NATO countries in retaliation for what they perceive as the west's support for

Ukraine and Israel. These threat actors are not subject to formal or overt state control, and they choose their targets (including ones in CNI sectors) based on what is vulnerable, which makes their activities less predictable.

Iran

Throughout early 2025, Iran has highly likely concentrated its cyber operations in support of its military and wider geopolitical objectives in relation to the Middle Eastern crisis.

In June 2025, US government agencies issued a fact sheet detailing the need for increased vigilance for potential cyber activity by Iranian state-sponsored or affiliated threat actors against US critical infrastructure and other US entities. The NCSC assesses this threat highly likely extends to UK entities. The implications and impact of the Iran-Israel conflict are still developing, but the NCSC continues to work closely with government, industry and international partners to understand and mitigate the cyber threat from Iran.

Democratic People's Republic of Korea (DPRK)

The DPRK's cyber activity mainly seeks to raise revenue, to collect intelligence and to offset the impact of international sanctions. DPRK threat actors indiscriminately target cryptocurrency companies and users globally, and attempt to steal data from defence industries, governments, and academia to improve their internal security and military capabilities.

UK firms are almost certainly being targeted by IT workers from the DPRK – disguised as freelance third-country IT staff – to generate revenue for the DPRK regime. It is also highly likely that UK-based cryptoasset firms are currently at risk of being targeted by DPRK-linked hackers seeking to steal or obtain funds through illicit means. The DPRK remains a prolific and capable threat actor, and the NCSC continues to work with partners to understand and address the risk to the UK.

Ransomware

Ransomware remains one of the most acute and pervasive cyber threats to UK organisations. This was highlighted by ransomware attacks on Marks & Spencer, the Co-op and others across the retail sector, with the sight of empty shelves a stark reminder of the potential operational and financial impact on victims. However, most cyber criminals are **sector agnostic**, selecting victims based on organisations they believe:

- are most likely to pay a ransom
- are vulnerable to operational downtime
- hold sensitive data that would cause significant harm to UK citizens if leaked

Of course, this makes *any* organisation a potential victim of ransomware attacks, as the NCSC's CEO points out in **this year's foreword**. And despite the

disruption of the **LockBit ransomware operation in 2024** - one of the most deployed ransomware strains globally - the threat from ransomware remains high. The cyber crime ecosystem is resilient, and the ransomware threat is diversifying in response to international efforts to counter its malign impact on society and the economy.

NCSC guide to ransomware

The **NCSC's ransomware resources** include guidance on mitigating malware and ransomware attacks, and advice on how best to recover should the worst happen.

Artificial intelligence (AI)

Threat actors of all types continue to use AI to enhance their *existing* tactics, techniques and procedures (TTPs), rather than to create novel attacks. That is, they are using AI to increase the efficiency, effectiveness, and frequency of their cyber intrusions. Actors linked to China, Russia, Iran and the DPRK are using large language models (LLMs) to evade detection, support reconnaissance, process exfiltrated data, access systems through social engineering, and support vulnerability research and exploit development (VRED).

In the last 18 months, security researchers have identified new techniques that exploit AI, including fully automated spear-phishing campaigns, hijacking cloud-based LLMs, automating post-breach attack stages and data exfiltration. The most significant AI-cyber development in the near-term will highly likely come from AI-assisted VRED, enabling access to systems through the discovery and exploitation of flaws in the underlying code or configuration.

Keeping pace with these 'frontier' AI-cyber developments will almost certainly be critical to cyber resilience for the decade to come, as we explained in our recent assessment on the **Impact of AI on cyber threat from now to 2027**. AI will almost certainly pose cyber resilience challenges to 2027 and beyond, across critical systems and economy and society. These will range from responding to an increased volume of attacks, managing an expanded attack surface and keeping pace with unpredictable advancements and proliferation of AI-cyber capability.

Cyber proliferation

The global commercial cyber intrusion sector will almost certainly expand over the next five years with state demand for intrusion products to meet national security requirements being a key driver. States providing a permissive operating environment in less-regulated regimes will almost certainly result in a growing number of cases which violate state legislation and privacy laws of victims.

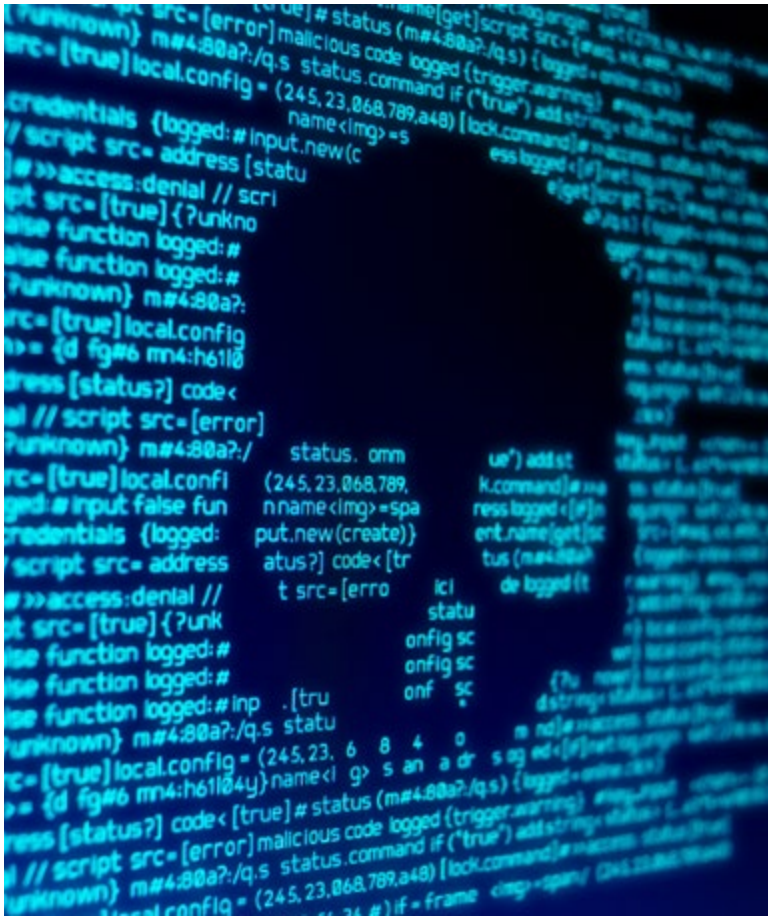
Diversification in the commercial cyber intrusion market means the capability on offer across the market will highly likely enable the exploitation of an increased range

of computer systems, thus moving beyond common personal devices. As the cyber intrusion market evolves, there is likely an increasing number of smaller entities - vulnerability researchers and exploit developers - operating in formal and informal collaborations with other specialist entities, rather than working in large providers. Government and whole-of-society efforts to influence players in the market and counter proliferation will almost certainly continue to be necessary.

The Pall Mall Process

The UK and France-led Pall Mall Process brings together international partners and stakeholders for an ongoing and globally inclusive dialogue to address the proliferation and irresponsible use of commercial cyber intrusion tools and services. It acknowledges the importance of public-private partnership and multi-stakeholder collaboration for a more secure cyberspace.

The Pall Mall Process hosted its second conference in Paris in April 2025 resulting in 26 states signing up to a Code of Practice which sets out a series of detailed recommendations for States as responsible regulators, customers and users of commercial cyber intrusion capabilities. The NCSC plays a leading role in supporting the FCDO, working in partnership with France, to advance the Pall Mall Process.



Threat to critical national infrastructure (CNI)

Cyber threat to the UK remains high. Cyber remains a discreet, low-cost, high-impact vector through which threat actors target the UK's CNI for espionage, ransomware and disruptive purposes. Ransomware conducted by financially motivated criminals continues to be the most immediate, disruptive threat to CNI sectors. The high-profile cyber attacks by the DragonForce ransomware group left customers unable to make payments, and saw the data of all 6.5 million Co-op members stolen. More broadly, we've detected a shift in hacktivist activity to include low-skilled attacks against operational technology (OT) systems.

Incident Management

The NCSC Incident Management Team (NCSC IM) responds to cyber incidents impacting UK organisations. We play a core role in minimising harm, restoring operations and helping victims to get back on their feet. The team is responsible for triaging incidents, supporting affected organisations and - for nationally significant incidents - serves as the central coordination hub for the cross-government response. This ensures there's a rapid, unified effort to protect UK citizens and critical services.

NCSC IM works closely with the National Crime Agency and wider law enforcement partners who play a pivotal role in tackling cyber threats. By bringing together the operational, technical, and strategic capabilities of government, NCSC IM enhances our collective ability to detect, deter, and mitigate cyber threats. This coordinated approach not only reduces harm to the UK but also strengthens our national cyber resilience.

We also work closely with the UK's Cyber Incident Response companies, law enforcement, UK and international intelligence partners and wider industry, to protect UK interests.

Incidents of national significance

This year NCSC IM received **1,727** incident tips from a combination of our own information flows and reports from partners and victims. These were triaged into **429** incidents requiring support from the NCSC IM team. This represents a similar total trend from the previous year.

However, **nationally significant incidents** represent **48% (204)** of all incidents, a significant increase from last year **(89)**. A nationally significant incident covers incidents in the upper three categories in the NCSC and UK law enforcement categorisation model. Amongst this year's incidents, **4% (18)** were categorised as highly significant in nature. This marks a 50% increase in highly significant incidents, an increase for the third consecutive year.

NCSC IM treats all reports in confidence. We encourage all affected organisations to report incidents to regulatory bodies who in turn view engagement with NCSC IM positively. However, for many businesses, reporting a breach is not mandatory. Since many chose not to do this, our data is not a true reflection of the number of cyber incidents that impact the UK.

Categorising UK cyber incidents

The UK government cyber attack categorisation is designed to improve response to incidents. The top 3 categories deal with nationally significant incidents.

Category 1

National cyber emergency

A cyber attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life.

Category 2

Highly significant incident

A cyber attack which has a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy.

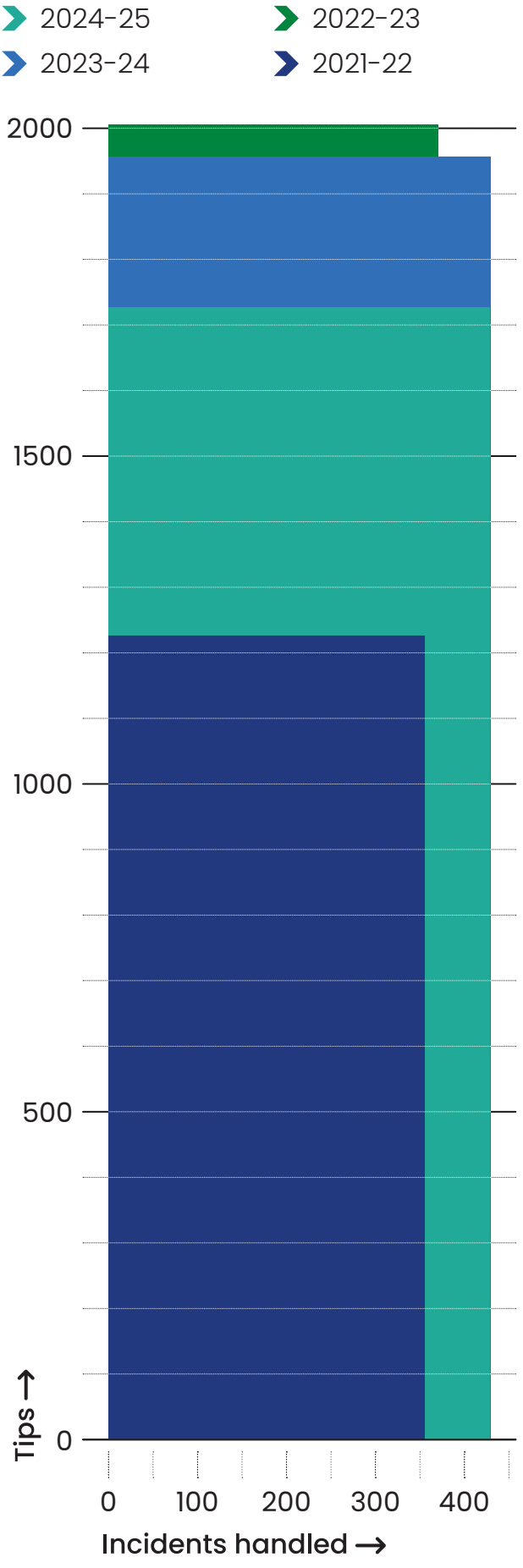
Category 3

Significant incident

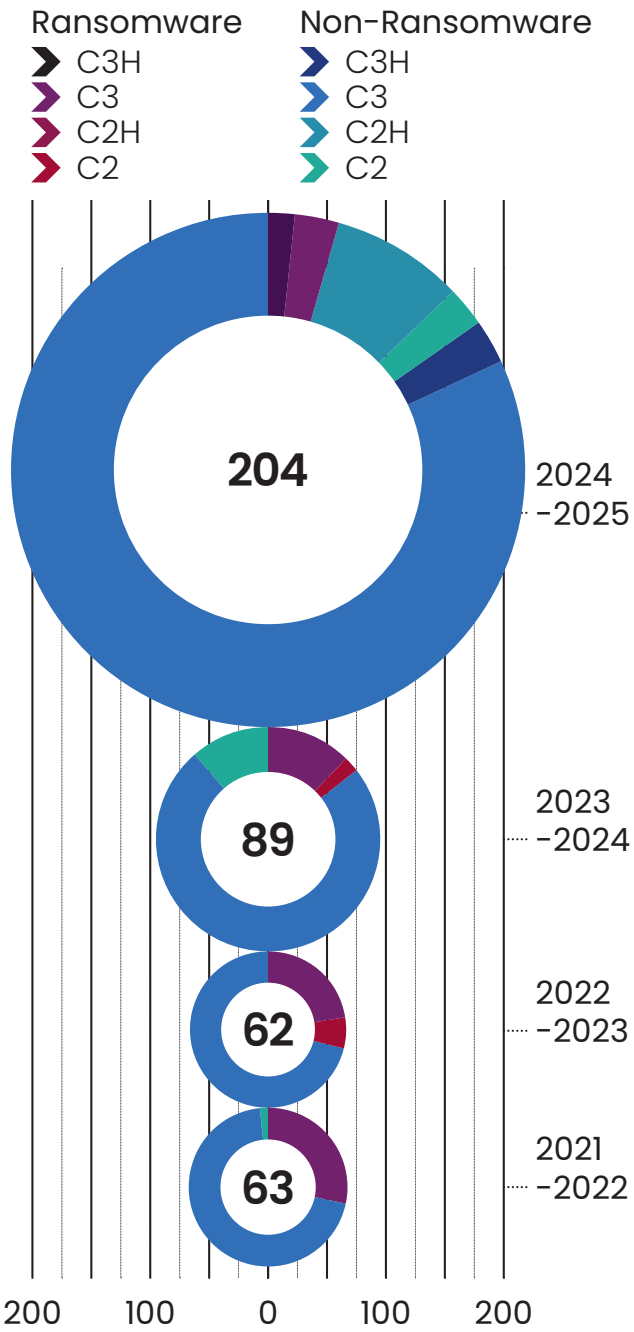
A cyber attack which has a serious impact on a large organisation or on wider/local government, or which poses a considerable risk to central government or UK essential services.

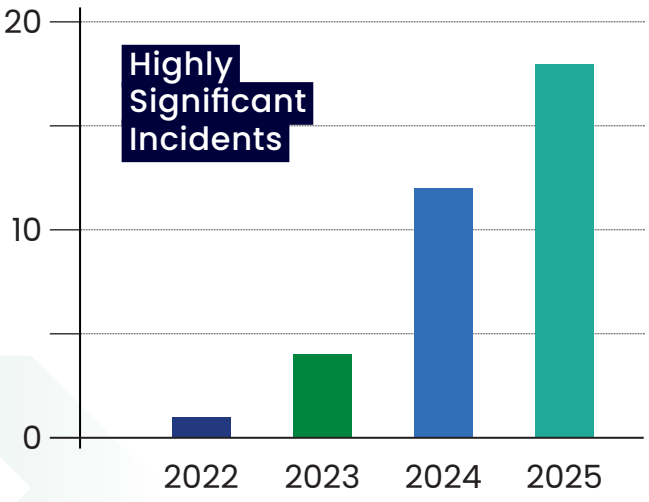
The top sectors reporting ransomware activity to the NCSC this year were academia, finance, engineering, retail, and manufacturing. However, no sector (and no organisation) is exempt from this threat.

Tips vs Incidents handled



Cyber Incidents breakdown





Report a cyber incident

Organisations can find out where to report a cyber incident in the UK using the signposting service at **gov.uk/report-cyber.**

You may need to report your incident to the ICO if there has been a breach of personal data. You can find out more by using the ICO's self assessment tool.

If you're an **individual** and you've lost money, tell your bank straight away and report it to Action Fraud or in Scotland, contact CyberScotland.

Vulnerabilities in legacy systems

A contributing factor to the increase in the volume of severe incidents is the exploitation of vulnerabilities by a small number of cyber actors. For example, NCSC IM published alerts for **CVE-2025-53770** (Microsoft SharePoint Server products), **CVE-2025-0282** (Ivanti Connect Secure, Policy Secure & ZTA Gateways) and **CVE-2024-47575** (Fortinet FortiManager), signposting organisations to the respective vendors' security advisories. These three CVEs alone were associated with 29 incidents managed by the NCSC.

‘Beyond detection’: why collaboration is vital to combatting the evolving threat

Our adversaries have the ability to innovate and evolve. As cyber defenders, we must do the same.

In last year's Annual Review, we spoke about the cyber threat becoming "increasingly diffuse and dangerous". 2025 has seen that trend intensify. We are in a period of sustained international competition, punctuated by multiple acute crises and increasing conflict. Cyber is being used by state and non-state actors to achieve their goals, and the overall cyber threat to the UK is growing from an already high level. The NCSC's incident statistics underline this growing intensity, with nationally significant incidents up by 50%.

Understanding the world we are in, and the role that cyber now plays within crisis and conflict, means we must also shift how we respond. In the face of escalating threat, we must develop the ability to rapidly interpret intent, capability, and geopolitical context across multiple actors in complex environments.

The need for this is increased by the varied ways we see threat actors operate, for the differing purposes of espionage, destruction, influence and leverage. This ranges from core capability and differing intents, from tightly controlled elite units to generating ecosystems of private sector, hacktivism and proxies access.

Of course, not all threat actors are equal. In the application of technologies, for example, there is a huge difference between a state-linked actor using AI for vulnerability research and exploit development (VRED), and a low-skilled cyber criminal using a jailbroken LLM to create more convincing phishing messages.

Regardless of the technical capabilities, the cumulative effect on threat is significant, leading to increased diversification, intensification and frequency of cyber threats across every sector in the UK.

While the threat is intensifying, the activity that the NCSC has repeatedly called out is not radically new, whether that's the targeting of western technology companies by the Russian GRU or the operational activities of hacking group Scattered Spider. It's more 'evolution than revolution', with existing techniques, tactics and procedures (TTPs) exploiting the complexity of the connected systems, networks and data we increasingly rely on.

Taken together, it means that traditional modes of understanding and response based on steady, static threat actor groupings are outdated. We exist in a world now where no one actor can understand everything, where no one government can set rules alone, and where digital sovereignty does not exist. It is a world where the ability to compromise the fundamental infrastructure of our lives comes at relatively low-cost, with near-anonymity and little fear of repercussion.

All this makes cyberspace a unique environment with unique challenges.

What is needed to operate in this environment are strategies to respond, deter and counter that are informed, context-aware and flexible. Understanding threat today is not just about detection; it is about

outcompeting adversaries in insight and agility. We must be able to make sense of a complex, broad technical landscape at pace, and link this to geopolitical context, not least in understanding the intent of actors and our global exposure to them.

Recognising this places huge emphasis on collaboration. Not one of us holds a monopoly on information, though we each have unique data and insight. The ability to share what we can, understand and respond to an increasingly differentiated threat environment is what will give us a competitive and strategic advantage in a world that is increasingly trying to diminish that advantage. And that work should not just be in how we share insight and the data that underpins it, but also how we generate it too. In this world, as cyber security professionals we must be technically and politically literate, and able to collaborate rapidly, flex and respond to a level of threat that is beyond what we have seen before.

The question for all of us now is 'What more can we do to understand threat collaboratively, and at the pace we need to in a conflictual environment?' Our sharing communities need to be deeper, faster and more actionable, sharing data and insight at speed, driving quicker evidence-based decision making.

Together with our colleagues across government, industry and academia, the NCSC is seeking to develop a data-led, collaborative response to threat insight and sharing. Our initiatives range from our established i100 and Cyber League initiatives (which brings together a trusted community of NCSC and industry cyber experts to work on the biggest cyber threats facing the UK), to our Trust Groups, a sector-specific community of CISOs which are so integral to information and threat sharing. More recently, we've launched the LASR (Laboratory for AI Security Research), a UK public-private initiative conducting foundational and applied research on AI security, focused on government national security priorities. It means that industry data and expertise are part of the design, not just as passive contributors, but as strategic partners in shaping defences that are relevant to different threat types.

> **'Understanding threat is not just about detection, it is about outcompeting adversaries in insight and agility.'**

But we must all do more. Our adversaries have the ability to innovate and evolve TTPs against an increasingly volatile and uncertain geopolitical climate. As cyber defenders, we must ensure that we can do the same. As our collaborative work drives resilience and makes life harder for threat actors, we must turn our threat understanding and response into real competitive edge, helping us to get ahead of the threat in an increasingly contested and competitive online world.

Chapter 2

Resilience at scale

National Cyber Security Centre
a part of GCHQ

Protect your organisation with Cyber Essentials

Cyber Essentials is a UK government-backed certification that proves your organisation is protected against the most common cyber threats.

Implementing just five key controls reduces risk, builds protection and gives stakeholders verified assurance that your organisation prioritises cyber security and meets the UK minimum standard for cyber security.

It's time to act. Get Cyber Essentials certified.

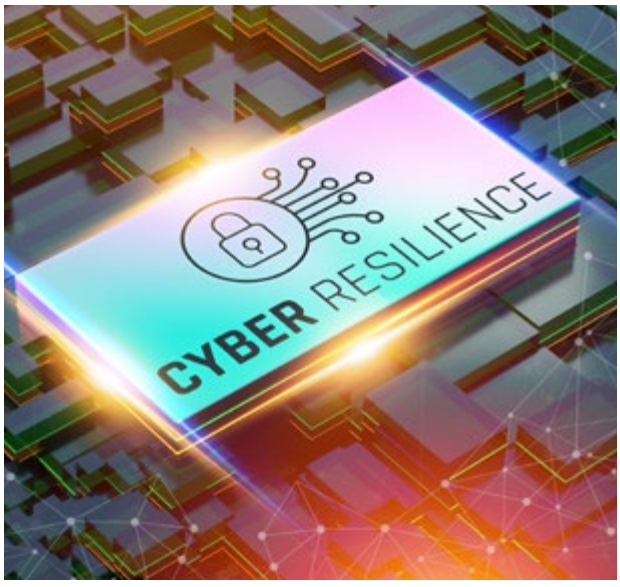
CYBER ESSENTIALS

ncsc.gov.uk/cyberessentials

Building cyber resilience, growing the economy

Helping organisations of all sizes to prepare, protect, detect and respond.

The NCSC's objective to raise national resilience is about enabling the UK to withstand and recover from cyber threats – across society, the economy, and critical infrastructure. With the severity of incidents rising, effective vulnerability management is more important than ever. Our tools, partnerships, and NCSC-recognised industry services are also helping to grow the economy by strengthening the digital foundations that businesses, public services and innovation depend on.



Our future offerings will look to build on the existing catalogue by focusing on the things that the NCSC is uniquely positioned to do, thanks to our deep ties with industry and academia. We are looking at two key areas:

- **Focus on user need, efficacy and evidence** — We are investing in user research and data science expertise to further mature our understanding of the interventions that make a positive difference to the cyber security of organisations across the UK. We are committed to automating that evidence base and making it transparent, to invite and encourage challenge and review.
- **Innovation and experimentation** — The second phase of our Active Cyber Defence (ACD) initiative aims to focus the NCSC's efforts on developing services that cannot currently be met by the commercial market, and/or where we can bring a unique contribution as part of GCHQ.

Don’t wait for the breach: why don’t organisations act earlier?

The role of leadership, culture, and behavioural science in encouraging proactive approaches to cyber security.

Cyber security needs to be a boardroom issue. It affects financial performance, operational continuity, and corporate reputation. Yet, despite the rising frequency and severity of cyber incidents, many organisations still do not act until after a breach has occurred. The consequences – legal, financial, and reputational – can be devastating, as seen in several high-profile attacks this year.

This delay is not simply a matter of oversight. It reflects a complex mix of behavioural, cultural, and financial dynamics that shape how organisations perceive and respond to cyber risk. Drawing on behavioural science theory and recent research into cyber security culture, this article explores why action is often deferred, and what senior leaders can do to change that.

At a basic level, the lack of preventative action can be explained by not having a full understanding of:

- the likelihood of a cyber attack happening to them
- the possible impact this could have on their business
- their ability to prevent (or recover from) a cyber attack

Furthermore, research suggests that individuals are more likely to act when they:

- feel positively about the action
- believe others expect them to do it
- feel confident in their ability to follow through

Therefore, a focus on understanding the true cyber risk facing organisations, the impact breaches could have and the actions that could be taken will help organisations take action before they are victims of a cyber attack.

Understanding and communicating cyber risk

A common barrier to proactive cyber risk management is the belief that their organisation is unlikely to be targeted. Smaller organisations, or leaders in sectors such as healthcare, manufacturing, or education might ask *"Why would cyber criminals attack us?"* This reflects a behavioural theory called optimism bias – the assumption that negative events are unlikely to happen to them. It's reinforced by a lack of visible threats and limited understanding of how cyber attackers operate. Cyber criminal attackers target vulnerabilities, not sectors, so every organisation with digital assets is a potential target.

Since most organisations rely on digital technology to function, cyber is another risk – like financial or legal risk – that the board needs to

manage. The Cyber Governance Code of Practice helps boards and directors manage digital risks so they can protect their organisations from cyber attacks.

A key challenge here is ensuring board members can communicate effectively about cyber risk. Unlike financial or legal risk, *cyber risk* is not always on the board's agenda. Leaders are fluent in the language of revenue, liability, and shareholder value, but cyber security is often framed in technical terms that feel disconnected from business strategy. To address this problem, the NCSC published guidance on 'Engaging with Boards to improve the management of cyber security risk', which helps CISOs to communicate more effectively with board members.

As the guidance explains, cyber risk must be translated into business risk, so that board members can approve necessary mitigations. For example, what happens if the factory comes to a grinding halt or the website goes offline? These impacts could affect share price, customer trust, and regulatory standing. By acknowledging this, it becomes far easier to prioritise and govern cyber security effectively.

The cost of inaction

Like any other business risk, cyber security will be competing for limited resources - both in terms of money and, crucially, space within the board's agenda. Without a visible threat, investment in prevention is frequently deferred. As a result, cyber security remains underfunded—until a breach occurs. Only then do attitudes shift, public scrutiny intensifies, and urgency becomes unavoidable.

IBM's X-Force 2025 Threat Intelligence Index notes that the UK is the most targeted European country for cyber attacks. In the UK, businesses have lost billions of pounds to cyber attacks over five years. Many of these losses could have been prevented through basic cyber hygiene and cultural change. Boards must recognise that investing in cyber resilience today protects long-term value and reduces the likelihood of costly disruption.

Once risk and impact are better understood, organisations can then consider what preventative action they will take. While this article can't cover every element of this, one overarching theme we urge all organisations to consider is their approach to 'cyber security culture', as this can be the springboard for a whole range of good cyber security behaviours and practice.

Building a positive cyber security culture

Research shows that any efforts to improve the cyber security of an organisation will only ever be effective if they are supported by a *culture* that encourages this improvement. An organisation's culture influences how cyber security is approached, for example how decisions are made, how incidents are managed and people's attitudes towards it.

What is cyber security culture?

Cyber security culture is the collective understanding of what is normal and valued in the workplace with respect to cyber security. It sets expectations on behaviour and relationships, influencing people's ability for collaboration, trust, and learning.

Leaders have a vital role to play in setting the tone for their organisation's culture. While some goals can be achieved by the cyber security team, significant and sustained impact needs leadership buy-in and advocacy

This year, the NCSC published its Cyber Security Culture Principles, outlining what good culture looks like and how to shift perceptions and behaviours. Applying the principles will help you tackle the behavioural barriers identified in this article and provide a foundation for change. To support implementation, the NPSA launched the Security Culture Tool, helping organisations assess and shape their entire security culture.

Improving cyber risk culture is not a technical issue – it's a leadership issue. Boards must set the tone from the top and embed cyber resilience into the organisation's DNA.

Don't wait for the breach

Cyber incidents often act as powerful cues to increase cyber security but by then, the damage is done. The cost of inaction is rising, and the window for preparation is narrowing. Organisations must move from reactive to proactive approaches to cyber security. This means challenging assumptions, quantifying risk, investing in prevention, and embedding a culture of cyber resilience at every level. The question is no longer *if* your organisation will face a cyber incident, but *when*. The time to act is now.

Empowering organisations

NCSC tools & services

The NCSC's evolving suite of tools and services have been developed to help organisations stay ahead of the cyber criminals and hostile states that seek to do us harm. From foundational protections like Cyber Essentials to advanced frameworks such as the CAF and innovative initiatives like ACD 2.0, the NCSC continues to deliver targeted, evidence-based solutions that meet the diverse needs of UK organisations.

The services described in this section are designed to help organisations protect themselves, prepare for incidents, detect threats, and respond effectively.

Cyber Governance for Boards

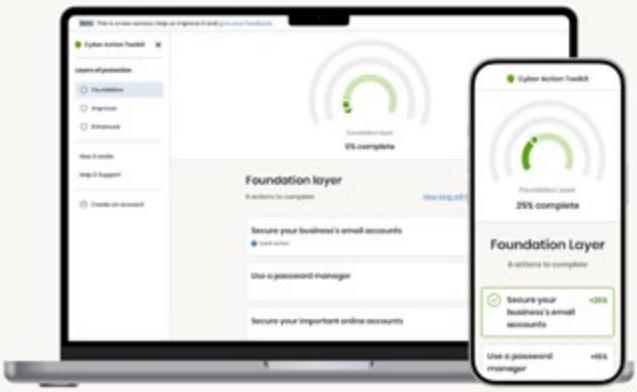
In partnership with the Department of Science, Innovation and Technology (DSIT), the NCSC created a Cyber Governance Training programme designed to empower boards to confidently implement the Cyber Governance Code of Practice. This tailored support package outlines the essential steps boards must take to gain meaningful oversight and assurance that cyber risks are being effectively managed.

Cyber Governance Training

Co-created with industry leaders, this training ensures boards are equipped to meet their cyber security responsibilities with clarity and confidence. The Cyber Governance Training aligns with the five core principles from the Cyber Governance Code of Practice. These are:

- Risk Management
- Strategy
- People
- Incident Planning, Response & Recovery
- Assurance & Oversight

Each module takes around 20 minutes to complete, and includes expected learning outcomes and links to relevant NCSC resources.



Cyber Action Toolkit

Smaller organisations – such as the 5 million sole traders, micro and small businesses active in the UK – can feel overwhelmed by the range of cyber security resources and guidance offered by the NCSC. For this reason, the NCSC has produced the Cyber Action Toolkit, a new way of providing advice in a way that engages small businesses, and more importantly, encourages them to take action.

The Cyber Action Toolkit is designed to be a single destination for sole traders to small organisations who are new to cyber security, and believe that cyber security is too complex, too expensive, and not a priority for their business. It provides a starting point and turns cyber protection into simple, achievable steps for businesses, allowing them to track their progress.

The Cyber Action Toolkit has been positively received by the 2,500 users who've taken part in our research, which showed that interactive approaches like this encourage businesses to take action when compared to simply providing cyber security guidance. The Cyber Action Toolkit has now moved to Public Beta and is being rolled out to all sole traders, micro and small businesses across the UK.

Cyber Essentials

While the cyber threat evolves, one thing remains constant; cyber criminals continue to exploit basic weaknesses in systems. Despite this, many UK organisations still aren't guarding against even the most basic cyber threats.

We need more organisations to take action now, to put in place the foundational cyber security controls that will raise both their resilience and that of the wider UK. Getting Cyber Essentials certified can help do this.

Over a decade ago, GCHQ was challenged by industry to identify the most essential cyber security protections for organisations. Drawing on our insights and understanding of the threat, we identified 5 technical controls that every organisation, regardless of size, should implement. And despite emerging technologies and new ways of working, those 5 controls are as relevant today as they were 10 years ago.

Even sophisticated attackers will exploit basic weaknesses, and implementing these 5 controls has been proven to work; data from the Cyber Essentials Insurance company tells us that organisations with Cyber Essentials are 92% less likely to make a claim on their insurance.

10 Years of Cyber Essentials

Since its launch in 2014, Cyber Essentials has steadily grown year-on-year in both take-up and recognition. In recent years this has accelerated, with certification rates increasing by over 17% in the last year. To coincide with the 10th anniversary, an independent impact evaluation report was published by the government, assessing the efficacy of the scheme.

- Most Cyber Essentials users **(85%)** believe the scheme has directly improved their understanding of cyber security risks, while an even greater proportion **(88%)** believe it has improved their understanding of the steps they can take to reduce those risks.
- **86%** say it has directly strengthened their senior management's understanding of the risks posed by cyber attacks.
- **91%** say that the scheme has directly improved their confidence at being able to consistently implement steps to reduce cyber security risks.
- **71%** agree that the scheme has directly strengthened how seriously their organisation takes cyber security.
- **79%** believe that the scheme has a positive impact on the confidence of their own clients and customers.
- **69%** believe that Cyber Essentials has increased their market competitiveness.

Cyber Essentials 'at-a-glance'

39,790 +17.5%

Cyber Essentials certifications awarded

12,850 +17.3%

Cyber Essentials Plus certifications awarded

402 +12.3%

Cyber Essentials Certification Bodies across the UK

The top three reasons given by organisations for getting Cyber Essentials were:

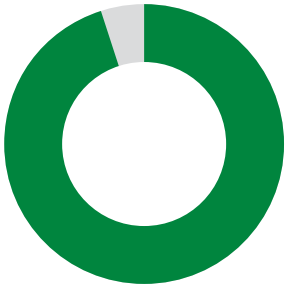
- **to give confidence to our customers (39%)**
- **to generally improve our security (31%)**
- **required for a contract (24%)**

Data from IASME's review of Cyber Essentials 2024-2025

Of organisations that gained certification this year, the top benefits were listed as:

- **it has allowed us to bid for new work**
- **it has given confidence to our customers and partners**
- **it has allowed us to advertise that we care about cyber security**

Data from IASME's review of Cyber Essentials 2024-2025



95%
of customers would certify to Cyber Essentials next year.

78%
would recommend certifying to other organisations like theirs.

1.1%
fail rate, dropping for the fourth straight year.

75%
of CE certifications were renewals, an increase of 3% on the previous year.

Data from IASME's review of Cyber Essentials 2024-2025

Funded Cyber Essentials Programme

In its third and final year, the Funded Cyber Essentials Programme (FCEP) continued to strengthen the cyber resilience of small organisations in high-risk sectors by providing funding and support to help them achieve Cyber Essentials certifications. Year 3 focused on emerging technology sectors (including AI , semiconductors, advanced robotics), and in February 2025, support was extended to barristers.

Since launching in December 2022, FCEP has helped over 850 small organisations.

- Year 1: packages funded for **369 organisations**
- Year 2: packages funded for **251 organisations**
- Year 3: packages funded for **233 organisations**
- **93%** of participants that gave feedback reported that Cyber Essentials changed the importance of cyber security within their organisation
- **100%** expressed confidence in maintaining the controls implemented.

The success of the FCEP is largely due to Assured Cyber Advisors—experts who offer tailored, accessible support to small organisations. They bridge the gap between technical know-how and the challenges small businesses face, such as limited budgets and in-house IT knowledge. Their clear guidance and hands-on support were vital in helping organisations achieve certification. There are now 128 Cyber Advisors working across the UK.

Cyber Essentials for supply chain assurance

Despite an increasing trend in supplier-based breaches, just 14% of UK businesses reviewed the cyber risk of their immediate suppliers in the last 12 months. This is often down to lack of capacity, capability and tools within buying organisations. The government is calling on large organisations to better address supply chain cyber security risk by developing approaches to improve adoption of Cyber Essentials within their supply chain.

- Alongside DSIT, the NCSC teamed up with the UK's leading banks – Barclays, Lloyds Banking Group, Nationwide, NatWest, Santander UK, and TSB – to issue a joint statement encouraging businesses to strengthen their cyber defences and adopt the Cyber Essentials scheme across their supply chains.
- Cyber Essentials Impact Evaluation found 48% of respondents reported saving time on cyber security due diligence where a potential supplier is Cyber Essentials certified.
- Suppliers also report increased efficiency as they can use their Cyber Essentials certificates as evidence across their customer base, reducing the time spent filling out duplicative questionnaires.
- A new tool has been developed by IASME that allows organisations to drop a large list of suppliers into a bespoke search function and find out which suppliers are certified to either Cyber Essentials or Cyber Essentials Plus.

Active Cyber Defence

Automated prevention, at scale

The NCSC's Active Cyber Defence (ACD) initiatives harness automation and data to prevent attacks at scale. The services described in this section effectively operate 'behind the scenes', and block cyber attacks before they reach their targets. Once organisations have registered with a service, they don't need to interact directly with the service to benefit from protections, and are instead protected automatically.

Early Warning

For many organisations, the cost of continuous network monitoring is prohibitive, and the specialist skills needed to do it often aren't available in-house. That's why the NCSC developed Early Warning, a free service designed to inform organisations of potential cyber attacks on their network, as soon as possible, potentially giving invaluable time to detect and stop a cyber incident before it escalates.

The NCSC's Early Warning uses information feeds from the NCSC, trusted public, commercial and closed sources, which includes several privileged feeds which are not available elsewhere.

You can register for Early Warning and see the other free NCSC services on the MyNCSC website.

Early Warning at-a-glance

13,178

Number of organisations signed up to Early Warning by year end.

316,343

Total number of Early Warning alerts sent to IP addresses belonging to customers across the year.

131,000

Amount of reports sent to IPs of 1,350 organisations we suspect had signs of being compromised by malware or hacking.

187,000

Number of IP addresses, belonging to 4,030 organisations, that were sent reports of vulnerabilities.

‘Share and Defend has blocked millions of attempts to access known scam websites, significantly enhancing online safety for millions of UK citizens. ‘

Takedown Service

We are working tirelessly to disrupt cyber attacks (such as malware and phishing sites) before they can cause damage to UK citizens and organisations. The NCSC’s Takedown Service works with hosting providers to remove malicious websites from the internet - at scale and in near real time - and blocks any attack infrastructure to limit the harm that cyber criminals can cause.

The Takedown Service at-a-glance

1.2m

cyber-enabled commodity campaigns removed.

26,000+

phishing campaigns targeting HMG departments disrupted.

79%

of confirmed phishing attacks targeting HMG departments were resolved within 24 hours of detection.

50%

of these attacks were taken down within less than 1 hour (which is a significant improvement on the year prior which was approximately 4 hours).

Share and Defend

Data from the NCSC Takedown service is used by another NCSC service, Share and Defend. This service shares feeds of known malicious domains with internet service providers (ISPs) and others so that they can be blocked or taken down. Since March 2025, Share and Defend, has blocked millions of attempts to access known scam websites, significantly enhancing online safety for millions of UK citizens. This collaborative approach, in partnership with BT and other industry leaders, is disrupting cyber-enabled crime at scale, bolstering national resilience, and supporting the government's Plan for Change.

To complement these services, last year the NCSC published:

- guidance for domain registrars and operators of DNS services to reduce the prevalence of malicious and abusive domain registrations
- guidance for brands to help their advertising partners counter malvertising (malicious advertising) and reduce the risk of cyber-facilitated fraud

Mail Check

Mail Check is the NCSC's platform for assessing email security compliance. It helps domain owners identify, understand and prevent abuse of their email domains.

- **13,193** organisations now using Mail Check (3,744 last year)
- **402,796** domains scanned by Mail Check (80,464 last year)
- **1,014,887** Urgent or Advisory alerts raised

Web Check

Web Check helps users find and fix common security vulnerabilities in their websites. It tells you what you need to worry about, when you need to worry about it and what you need to do about it.

- **4,624** organisations using Web Check
- **133,913** domains and URLs scanned (63,384 last year)
- **569,467** Urgent or Advisory alerts raised

Suspicious Email Reporting Service (SERS)

Since its inception in April 2020, the Suspicious Email Reporting Service (SERS) has been a successful way of enabling the public and businesses to report suspicious emails to the NCSC, leading to the removal of thousands of scams.

- over **10.9m** reports received in the last year
- total number of reports since April 2020 reached over **45m**
- **412,000** malicious URLs removed by the NCSC since 2020

PDNS for Schools

Protective Domain Name Service for Schools ('PDNS for Schools') is a free cyber security service, developed by the NCSC, that's designed to protect schools from a variety of online threats. It helps prevent malware, ransomware, phishing attacks, and other online threats from reaching school networks. Since rolling out the scheme in England and Scotland, over 13,000 schools are already being protected.

By early 2025, all schools across the UK were able to benefit from PDNS for schools. It's part of a wider cyber security offer of guidance and tools the NCSC has provided so schools can focus on what they do best: educating pupils. For more additional information about the service, please visit our PDNS web pages. We intend to extend the service to schools in Wales and Northern Ireland by the end of the year.

'Prior to implementing PDNS for schools, we were reporting 24m allowed queries and 19k blocked queries; and post this event these numbers increased to 66m allowed queries and a staggering 10m blocked queries. Expanding the service to protect our schools highlighted to us how our schools were exposed to significant cyber related attacks.'

Medway Council

PDNS for 'high-risk' individuals

Nearly 600 of the UK's high-risk individuals[1], including Cabinet Ministers, are registered with the NCSC services. PDNS, which prevents access to malicious domains, has been broadened to unmanaged personal devices providing unique data insights. In response to the ongoing cyber threat of spear-phishing against personal accounts, PDNS is now available as an app. Through bespoke agreements with Google and Microsoft, the NCSC has extended free enhanced protection to hundreds of personal accounts belonging to high-risk individuals, closing a critical vulnerability gap and enabling faster threat detection and response.

1 A high-risk individual is someone whose work or public status means they have access to, or influence over, sensitive information that could be of interest to nation state actors.

High-risk individuals include those working in political life (including elected representatives, candidates, activists and staffers), academia, journalism and the legal sector.

Engineering resilience against critical loss

Prevention and detection aren't enough: resilience means building systems which can operate and recover following a disruptive cyber intrusion.

The cost to Marks and Spencer and its insurers following the ransomware attacks earlier this year is estimated to exceed £300m. However, the impacts of cyber attacks are now felt beyond the victim organisation. Destructive cyber intrusions increasingly affect customers, third parties, and wider society.

For example, the ransomware incident suffered by pathology laboratory services provider Synnovis led to significant clinical healthcare disruption across the London region, and incurred costs of £32.7m, far outstripping Synnovis' profits of £4.3m for 2023. It also directly contributed to at least one patient death. This starkly illustrates the scale of exposure across our hyper-connected and technology-dependant society, especially where legacy infrastructure and systems need to be maintained.

These challenges are only magnified when considering the technical legacy often held in organisations. Having a strategy to address technical legacy is a foundational precursor to engineering resilience. Recognising this, the NCSC included an emphasis on understanding threat actor methods and motivations coupled with monitoring and threat hunting in the Cyber Assessment Framework v4.0

Resilience engineering

Established cyber security measures (such as risk management, protective monitoring, business continuity and disaster recovery) remain essential mitigations. However, the NCSC believes that organisations must look beyond contemporary controls and consider how we engineer fundamental resilience, so they recover critical services in the face of the unexpected.

'Resilience Engineering' is a discipline that has heritage in safety engineering and a range of sociotechnical disciplines. It aims to improve an organisation's ability to anticipate, absorb, recover and adapt in the face of unexpected shocks such as cyber compromise which could result in disruptive or destructive events.

How can resilience engineering be applied to the cyber security domain?

In designing systems to be resilient we can draw on several existing and emerging cyber security architectural and operational approaches.

Infrastructure as code allows us to rapidly and reliably replicate and reconstitute systems and infrastructure. This is an essential component of rapid recovery from loss or compromise, but also allows the deployment of trusted, immutable infrastructure making it far more difficult for threat actors to maintain persistence.

> **'To complement engineering resilience, organisations need to ensure prepared operational crisis response capabilities are scaled to their size and complexity.'**

Similarly having evidence of **immutability of backups** and that there are **practised recovery and rehydration** procedures for situations where total environment loss, including the loss of identity and access management, hypervisors, cloud configurations and more, has occurred is essential for timely and effective recovery.

Segmentation through both logical and physical architectural patterns allows for isolation and contained operation either as-needed to minimise impact during an event, or persistently to create trust boundaries such as through cross-domain solutions. The NCSC has emergent anecdotal evidence that those organisations who intervene during a destructive event and self-isolate, recover quicker with less impact. Approaches including **Privileged access Workstations (PAWS)** and **segregation of management planes** enhance resilience against systems administrator compromise by materially complicating total environment compromise and loss through privileged access.

Applying the principle of least privilege universally and across all services further limits the potential damage from breaches. This approach should be complemented by the use of microservices, context-aware and individualised authorisation, and application isolation, all of which reduce the 'blast radius' of a compromised component or service. These principles underpin a Zero Trust Architecture (ZTA), which assumes no implicit trust within the system.

Observability and monitoring are key enablers for Engineering Resilience, to enable observation and rapid response to events. Comprehensive observability and data collection (hosts, infrastructure, edge, cloud, and applications etc.) provides opportunities for anomaly detection, response and post incident learning, which are critical for minimising impact and improving future resilience.

Chaos engineering, the deliberate introduction of failure to validate detection and recovery, is a

complementary approach to evidencing control efficacy in dealing with systems failure and the ability to self-heal. Some contemporary organisations repeatedly test through such approaches that resilience exists against partial and sudden loss along with the ability to detect and respond.

In the most critical situations having **critical business functions running on duplicate but distinct technology stacks** can provide resilience against a range of operational and cyber security related risks.

Resilient Operations

To complement engineering resilience, organisations need to ensure prepared operational crisis response capabilities are scaled to their size and complexity. Such measures include ensuring availability of crisis response runbooks either digitally or physically on isolated platforms or hardcopy, emergency communication procedures and for physically diverse organisations fall back digital identity.

Looking forward, there is value in addressing Nassim Taleb's concept of 'Antifragility'. This means moving beyond simply withstanding shocks, to growing stronger because of them. Each incident becomes an opportunity to refine protections, detection capabilities, and response strategies, ensuring that systems not only survive but evolve.

Defending the UK's critical national infrastructure

Closing the widening gap between the threat to critical systems, and our ability to defend them.

A step change in cyber resilience doesn't happen overnight.

In last year's annual review, we warned that the gap between the threat posed to critical national infrastructure (CNI) and the ability of owners and operators of CNI to defend against it was widening. Narrowing this gap became our top priority for the year, as we focused on raising the resilience of the UK's most critical sectors to the most advanced cyber actors.

This has increased our knowledge of CNI cyber maturity in order to inform targeted interventions, giving them the tools to detect and evict sophisticated actors from their networks. With a better understanding of those organisations carrying the highest risk, we have continued developing the UK's defensive capabilities to improve vulnerability detection and operational response.

We seek to ensure the UK has the capability to defend, hunt and evict threat actors to reduce the vulnerability and impose cost on adversaries operating against the most critical systems. This is being achieved through identifying and developing cyber security communities across the UK, alongside tradecraft and capability experimentation.

Interconnected threat to CNI

The increasingly complex and interconnected nature of our technology and systems across CNI delivers great benefits - but also risks. This means that cyber-initiated attacks could have physical consequences.

Working closely with our partners at NPSA we both recognise the importance of supporting CNI to address physical, personnel and cyber vulnerabilities. A key priority to should be to review the countering sabotage guidance, and to act on it.

'Preparedness For Crisis' project

The National Security Strategy 2025 described the UK as entering a new era "characterised by radical uncertainty". The international order is being reshaped by an intensification

of great power competition, authoritarian aggression and extremist ideologies. This uncertainty brings many challenges, including threats to our cyber resilience.

As we explain in the threat chapter, disruptive cyber attacks are now part of the playbook for aggressors. This means operators of essential services should understand what defensive actions they could take if there was a step change in threat, allowing them to continue to operate their services even in a crisis. They should be prepared to increase their situational awareness (for example with enhanced threat hunting) or harden defences (for example by isolating operational technology or reducing the attack surface).

> **'Operators of essential services should be prepared to increase their situational awareness or harden defences.'**

The NCSC's 'Preparedness for Crisis Project' continues to place emphasis on the importance of organisations testing and gaining assurance in advance, and integrating these processes into their resilience strategies. Over the next year, the NCSC will be focused on helping organisations to prepare for crises, with new advice, guidance and tools.

Threat sharing and threat hunting

We have also continued to arm the most critical systems with threat intelligence through the TiSP (Threat Intelligence Sharing Platform), having this year onboarded over 50 private sector CNI organisations. In spring 2025, the NCSC convened two of the largest threat hunting workshops to date, tailored for both public and private sector cyber defenders. These comprised 60 experienced analysts from 28 government organisations and 80 experienced analysts from 55 private sector CNI organisations. These events are part of a community to improve threat hunting, upskill organisations, and share detailed insights into real incidents experienced by attendees.

Sector-specific interventions

With the majority of the UK's CNI privately owned, the NCSC continues to offer specialist, sector-specific technical advice to industry. Informed by the threat landscape, our offering to CNI sectors has continued to be enhanced to ensure private sector owners and operators are well informed and have prioritised cyber security. We have continued to treat the cyber security of CNI as a shared responsibility, promoting our advice and guidance and empowering organisations to take action using this.

The Cyber Security and Resilience Bill (CSRB) is critical to our objective of improving cyber resilience of the UK's highest priority public and

private sector CNI, including recovery planning against advanced threats. The CSRB will provide the baseline against which both the regulatory framework and regulator capabilities will be uplifted.

In the **transport** sector, alongside government and industry, we have used our role as the National Technical Authority for cyber security to consider cyber security risks related to critical emerging technologies, such as Connected and Autonomous Vehicles (CAVs); gaining insights from innovative projects such as the new self-driving shuttles in Milton Keynes city centre.

In the **finance** sector, a multi-year collaborative project between the NCSC and the Bank of England has concluded, resulting in an initiative to embed cyber security into the renewed banking system used across the country.

Following the designation of **data centres** as CNI, we've helped shape government understanding of the cyber risk to that sector and the critical interdependencies. We have continued to work closely with DSIT to prepare for the implementation of the CSRB. If enacted, more organisations (such as managed service providers) would be brought into scope of the NIS Regulations, the UK's Network and Information Systems Regulations that aim to ensure the security and reliability of digital infrastructure. The government would also have new executive powers to respond to evolving cyber threats.

Our work to assist the **energy sector** in protecting its infrastructure over the last year has been wide-ranging, including providing technical advice and guidance on the cyber security challenges associated with mitigating the risks and collaborating directly with critical suppliers on cyber security projects and extended support to operators of renewable energy assets, helping them to manage cyber security risks as part of the drive to secure the UK's ambitions for a Net Zero future.

Cyber risks to UK defence

In light of the 2025 Strategic Defence Review's recognition of intolerable cyber risks in UK Defence, we've intensified collaboration with the Ministry of Defence (MOD) to boost cyber resilience across its supply chain. Adoption of Active Cyber Defence (ACD) services has grown, extending protective DNS and host-based tools - typically reserved for the public sector - to key suppliers. These tools block threats, gather metadata for NCSC analysis, and provide expert support.

We've revitalised the Defence Technical Information Exchange (DTIE), a joint NCSC-industry forum for sharing threat intelligence and mitigation strategies among key defence suppliers. Additionally, we've supported the development and launch of MOD's Defence Cyber Certification (DCC) scheme, which ensures supplier cyber resilience through

independent certification – providing assurance of organisational cyber resilience in support of future defence procurements.

The NCSC has also maintained its vital role in supporting complex defence programmes, providing expert technical advice to ensure the security and resilience of strategic projects and their supply chains. Notable collaborations include:

- The **Dreadnought** programme, the replacement programme for the Royal Navy's Trident missile Vanguard Class submarines which form the UK's nuclear deterrent.
- The **Future Combat Air System**, the UK's requirement and programme of record to deliver a next generation combat air capability. FCAS forms part of The Global Combat Air Programme, an international partnership between the UK, Japan and Italy which will design, manufacture and deliver the next generation crewed combat aircraft.
- **AUKUS**, the Australia-UK-US defence partnership. This includes supporting the design and development of the ASTUTE replacement nuclear powered submarines known as SSN-AUKUS.
- **Op Highmast** the Carrier Strike Group 25, through support to MOD with cyber security advice as part of the Op Highmast planning process.

The UK health sector

Focusing on cyber security across the health sector is essential to ensure sensitive data is protected, critical services operate smoothly, and public trust is upheld. In August 2024, the NCSC responded to several cyber attacks in the health sector, including the ransomware attack on Synnovis. In the aftermath, the NCSC brought together senior health representatives from across the four nations to identify shared challenges.

Since then, a broad collaboration has been fostered between the NCSC, UK health organisations, and industry partners. Within this partnership new tools and services through the Active Cyber Defence (ACD) 2.0 programme have been piloted, including Attack Surface Management and Deception Technology. Other initiatives include:

- Preparing for future threats by assessing quantum readiness
- Managing vulnerability disclosures
- Sharing threat intelligence and tradecraft
- Supporting supply chain security through initiatives like the NCSC Early Warning service and Cyber Essentials scheme

The NCSC has also worked with the health sector to help develop the joint NCSC/DSIT Software Code of Practice , which promotes secure software development. The NHS is the first large organisation to build use of this product into their software procurement process.

National Cyber Security Centre
a part of GCHQ

CAF 4.0: Manage cyber risk with confidence

Designed for the UK's critical national infrastructure in sectors such as energy, healthcare, transport, digital infrastructure, and government, the **Cyber Assessment Framework (CAF)** provides a comprehensive framework to evaluate how well your organisation meets expected cyber outcomes.

Whether you're responding to regulatory requirements, external oversight, or internal governance needs, the CAF supports alignment with legal obligations, helping you manage cyber risk with confidence.

Cyber threats are evolving, close the widening gap between the threat, and our collective ability to defend against them.

It's time to act. Adopt CAF 4.0 now.

ncsc.gov.uk/cyber-assessment-framework

Strengthening government cyber security

The NCSC is working closely with the Government Digital Service (GDS) to support the development of a more interventionist model for cyber security across government. Together, we are collaborating on a Target Operating Model that will set out how this approach will work in practice, including ensuring clear roles, responsibilities and processes for managing systemic risks.

Our collaboration is already delivering key initiatives such as:

- the GovAssure cyber assurance regime, which provides a consistent and rigorous framework for assessing departmental resilience
- the Government Cyber Coordination Centre (GC3), which strengthens threat intelligence sharing, vulnerability management and incident response across government

We are now expanding this joint working to other areas including how centralised cyber security services are delivered across the public sector. Our collective efforts aim to address long-standing challenges such as legacy IT vulnerabilities, improving collective preparedness, and ensuring that government services remain secure and resilient. By combining the NCSC's technical expertise with GDS's leadership on digital delivery, we are building a stronger, more proactive approach to cyber security across the public sector.

Supporting democracy in a borderless cyber landscape

The 2024 Annual Review highlighted a pivotal year for global democracy, with elections taking place across numerous nations amid rising geopolitical tensions and rapid technological change. Throughout 2025, the NCSC has continued to reflect on lessons learned and monitor an evolving threat landscape, particularly as innovations in technology and election services reshape democratic processes.

Cyber threats know no borders. In response, we have strengthened collaboration with international partners, working closely with FCDO's International Cyber Network, to share insights, build resilience, and promote best practice on election security.

As the threat landscape evolves, the NCSC remains committed to supporting both domestic and international partners. In the UK, we are working closely with the Electoral Commission and the Joint Election Security Preparedness Unit to assess and strengthen cyber risk controls ahead of major democratic events. The next UK general election, is expected to be the first to rely predominantly on cloud-based Electoral Management Systems, marking a significant shift in how elections are administered and secured.

To prepare for this transition, we are supporting the Ministry of Communities Housing and Local Government to ensure that security

standards and resilience measures are future-proofed. This work forms part of a broader strategy to modernise and secure UK elections, as outlined in the government's 2025 Elections and Democracy Bill. The Bill also includes proposals to lower the voting age to 16, expand digital voter ID options, and improve voter registration systems.

> **'Organisations need to look at their security in the round to make the right choices.'**

Updating the Cyber Assessment Framework (CAF)

Since the last version of the NCSC Cyber Assessment Framework (CAF) was published in April 2024, its adoption has continued to spread. It is now used by nearly all UK cyber regulators and is established in the public sector via GovAssure, the cyber security assurance scheme for assessing the critical systems of government organisations.

The most significant amendments in version 4.0 reflect the changing threats that organisations face:

1. A new section on building a deeper understanding of attacker methods and motivations to inform better cyber risk decisions.
2. A new section on ensuring software used in essential services is developed and maintained securely.
3. Updates to the section on security monitoring and threat hunting to improve the detection of cyber threats.
4. There is improved coverage of AI-related cyber risks throughout the CAF.

The NCSC is supporting the community of cyber regulators and oversight bodies that use the CAF so that their sectors can make a quick transition to CAF v4.0. The CAF forms part of a broader suite of tools we provide to regulators and operators to build confidence and resilience, including:

- Cyber Resilience Audit, a scheme that gives consumers confidence in companies that have been assessed as meeting the NCSC standard for delivering independent cyber audits. The Cyber Resilience Audit scheme members will undertake independent cyber audits on behalf of a Cyber Oversight Body.
- Cyber Adversary Simulation, a scheme that assures commercial organisations providing Cyber Adversary Simulation services which meet our CyAS Standard. We have designed the scheme so that buyers can use it independently as part of their own cyber resilience activities, or under the direction of their Cyber Oversight Body.

Secure Innovation

Operating a secure business is not just about cyber security; organisations need to look at their security in the round to make the right choices. The NCSC therefore works in partnership with NPSA, as the National Technical Authority for Physical and Personnel Security, to help organisations address the full range of security threats that they may face. The campaign has had international impact, with its guidance adopted by Five Eyes countries in October 2024, helping protect innovation, reputation, and national security.

Building on the Secure Innovation campaign, the Secure Innovation Security Reviews Scheme is a joint initiative by the NCSC, NPSA, DSIT and Department of Business and Trade (DBT). It provides partial funding for up to 500 organisations in the UK emerging technology sector with direct support and guidance from an approved Security Reviewer to protect their ideas, technologies, reputation, and future success. Businesses must be registered and based in the UK, have under 250 staff and be working in one of the 17 sensitive areas of the economy set out in the National Security and Investment Act, or selected sectors from Invest 2035: the UK's modern industrial strategy.

Launched in July 2025 after a successful pilot, the scheme is delivered via InnovateUK and Business West, with most costs funded by DSIT. Reviews are conducted by vetted professionals and include a site visit, a report with recommendations, and a follow-up call.

Industry assurance

Supporting a thriving cyber security industry

We continue to support the UK's thriving cyber security industry by leveraging the NCSC brand, so consumers know who and what they can trust. It works as follows:

- as the National Technical Authority for cyber security, we set the standard for what constitutes best-practice
- we assess industry providers against this standard
- we license our brand to those who meet the standard, then work in partnership with those assured service providers

We now have a network of around 500 companies offering 'badged' services on our behalf, helping UK organisations to prepare for, protect against, detect and respond to cyber threats. Two new initiatives designed to help boost confidence in cyber resilience were announced at the flagship CYBERUK conference earlier this year.

- A new ecosystem of assured Cyber Resilience Test Facilities will allow technology vendors to demonstrate the cyber resilience of their products.
- A Cyber Adversary Simulation scheme will help organisations test their defences.

Cyber Resilience Test Facilities (CRTFs)

The industry-provided Cyber Resilience Test Facilities (CRTFs) bring the NCSC's evidence-based method of technology assurance to life using the NCSC's published approach of Principles Based Assurance. Following their successful participation in last year's pilot, an initial operating capability of three Test Facilities will offer Cyber Resilience Testing for internet-connected products.

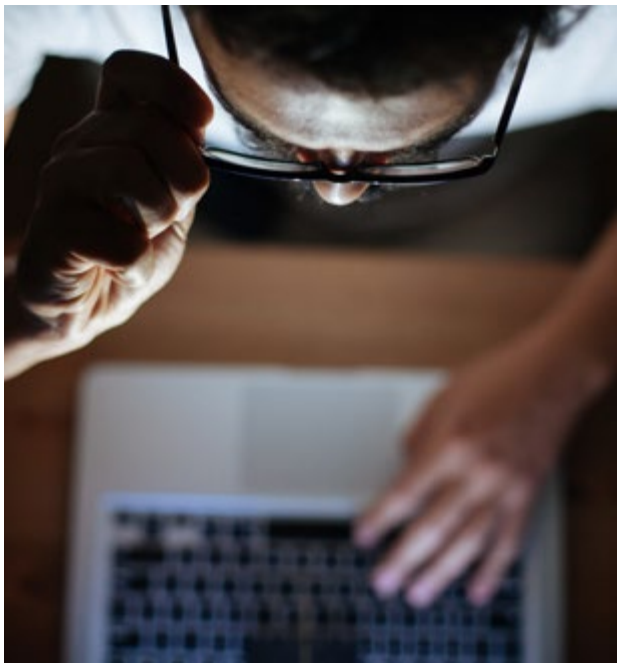
The initial service offering assesses connected products against the Cyber Resilience Testing (CRT) Assurance Principles and Claims (APC) standard, assessing resilience to commodity attacks from public facing connections. This standard has been aligned with DSIT's Software Security Code of Practice.

We continue to work closely with our Test Facilities, including the development of opportunities for training and accreditation for those involved in its delivery. Work is also ongoing to develop the market for this assurance and to support it as it

scales up. This will see the ecosystem grow to include, amongst other things, high assurance cyber resilience testing, with the development of additional APCs.

Cyber Adversary Simulation (CyAS)

Companies assured under the CyAS scheme will deliver services to test an organisation's cyber security, including their ability to prevent, detect and respond to sophisticated simulated cyber attacks (red teaming). We have developed the CyAS scheme in partnership with Cyber Oversight Bodies – cyber regulators and government – who are exploring the use of the scheme in their sectors. It has been designed as a means of providing end-to-end assurance and evidence for any organisation of sufficient maturity and criticality to test their cyber defences. The scheme will launch as a Minimum Viable Product and is expected to evolve as the user community grows.



Cyber Resilience Audit (CRA)

The Cyber Resilience Audit scheme has grown steadily since its launch last year. The NCSC has assured 17 providers to conduct independent CAF-based audits. The scheme has been developed alongside Cyber Oversight Bodies with responsibility for understanding cyber resilience within their sector. This currently includes:

- The Department of Finance, Northern Ireland
- The Department of Health and Social Care and NHS England
- Department for Business and Trade (chemical sector)
- The Office for Nuclear Regulation

GovAssure (the assurance programme that provides assessment of the cyber security of critical systems underpinning government's essential services) announced that it will adopt NCSC's Cyber Resilience Audit scheme for independent assurance reviews from 2026. This move will drive quality CAF-aligned reviews for government organisations under GovAssure.

Assured Cyber Security Consultancy

The NCSC's Assured Cyber Security Consultancy scheme assures companies offering services to organisations with complex or high-risk cyber security requirements. In addition to the long-standing offerings of security architecture, risk management and audit & review, this year we launched a pilot post-quantum cryptography (PQC) offering in order to build market capacity to address this national challenge. There are two offerings under the PQC offering:

- **Discovery & Migration Planning:** all companies within the pilot will be assured to support organisations in cryptographic discovery exercises, to identify priority services for migration, and to support the development of an initial migration plan.
- **Advice:** some companies will also be assured to offer direct advice on the use of PQC, in line with the NCSC's published positions.

Cyber Incident Exercising

The NCSC's **Cyber Incident Exercising scheme** has now assured 39 providers (a growth of almost 40% since the last Annual Review). The growth is timely, as Government Cyber Security Policy (aimed at lead government departments, their arm's length bodies and other public organisations) promotes that cyber incident response plans must be exercised at least annually. The scheme assures providers that offer exercising to test organisations' incident response plans in a safe environment and strengthen their incident management processes.

> **'Cyber incident exercises like these aren't just about following a script – they're about preparing for the unexpected. When you've got the right people in the room, you can identify gaps, challenge assumptions, and make sure the organisation is ready to respond effectively when it really matters.'**
>
> **Director Digital Security & Engagement, Department of Finance Digital, NI**

Cyber Incident Response

Our **Cyber Incident Response scheme** assures providers under two levels: 'Standard' (supporting organisations at risk of common cyber attack) and 'Enhanced' (for the most critical entities likely to be exposed to the most sophisticated threats). Since the launch of the new CIR Standard level, the scheme has grown – by over 25% since last year's AR – with 46 CIR providers now assured by the NCSC. The NCSC recommends that all UK organisations should use an NCSC-assured Cyber Incident Response provider when dealing with cyber incidents.

CHECK Penetration Testing

The NCSC's CHECK scheme sets standards for penetration testing that government departments, public sector bodies and the UK's CNI organisations can trust. There are currently 54 companies assured, delivering CHECK penetration testing engagements. Over the past 12 months our assured service providers have carried out over 2,684 penetration tests. As well as ensuring the resilience of some of the most critical sectors, the information gathered through these penetration tests helps the NCSC identify and better understand common vulnerabilities across organisations.

Smart Meter Assurance

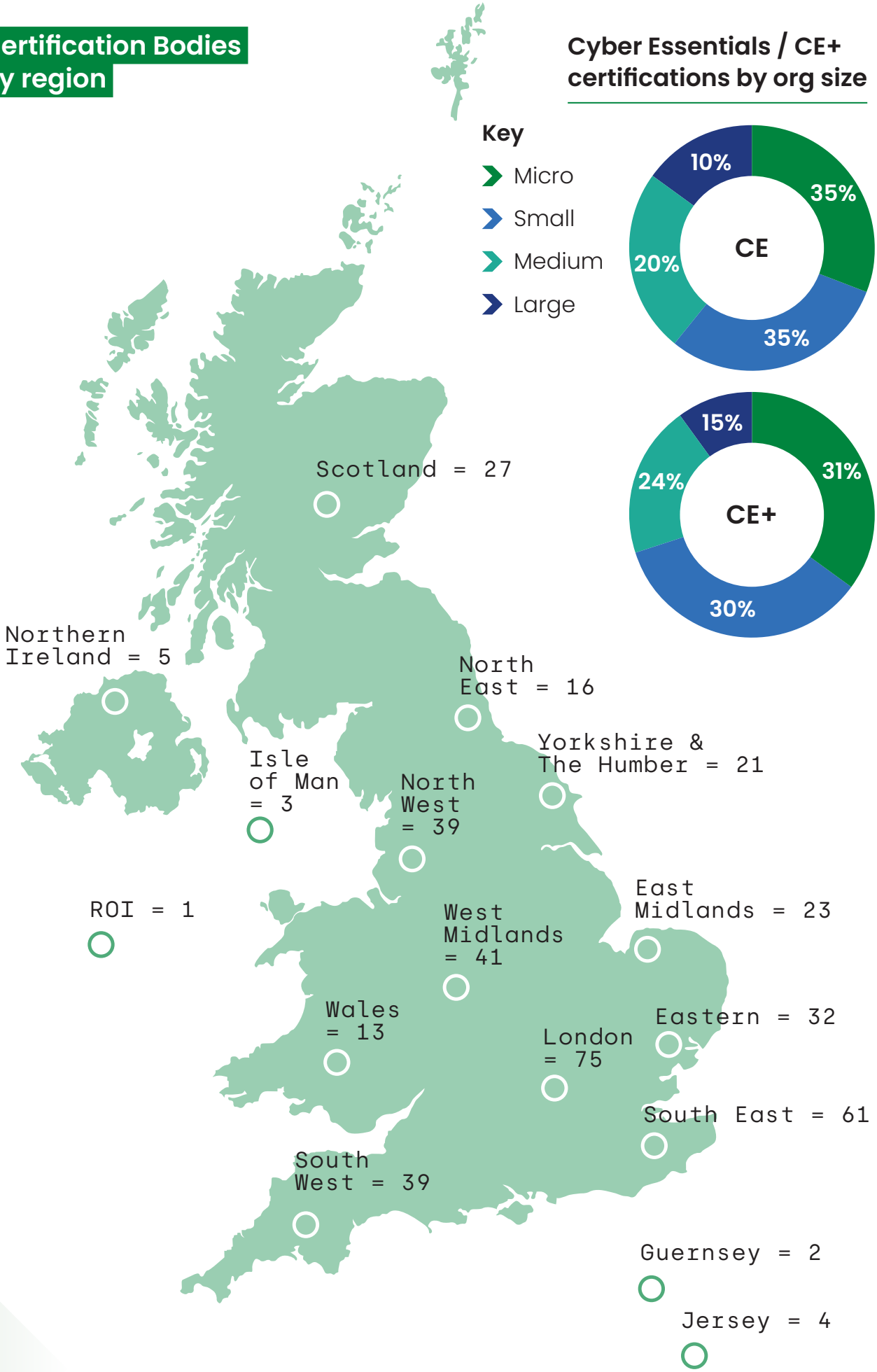
Over the past 12 months the NCSC has been finalising the transfer of the Smart Metering CPA scheme to a new owner. This sees the NCSC's day-to-day involvement in Smart Meter assurance drawing to a close after nearly a decade. In that time, millions of smart meter devices have been certified and deployed to UK homes. The transfer to CyTAL, the new scheme operator, has been a long-term, collaborative process, working alongside Department for Energy Security and Net Zero (DESNZ), The Smart Energy Code Company, SECAS and our CPA Evaluation Partners. This move aligns with the NCSC's goal to empower industry and place risk decisions and ownership with those that hold the authority.

Cyber Essentials Certification Bodies

The impact of Cyber Essentials reaches beyond basic cyber resilience, contributing to wider economic growth. Through our Delivery Partner, IASME, we continue to support the UK's cyber security industry by licensing the assessment process for Cyber Essentials to Certification Bodies across the UK. We now have 402 Certification Bodies employing 934 Assessors.

- over 75% of these companies are micro or small businesses
- the scheme stimulates company growth, with almost 50% reporting growth – some significantly – since becoming a Certification Body, leading to an increase in the number of trained and practising cyber security experts across regions
- Cyber Essentials offers a route into the cyber security profession. Recognising current industry requirement as a bottleneck, we're working with IASME to create an entry-level role linked to tech apprenticeships, providing a basic qualification as an alternative entry point

Certification Bodies by region



Cyber Essentials / CE+ certifications by org size

Building the cyber ecosystem

Scotland

The NCSC's proactive support in managing national cyber incidents has significantly strengthened Scotland's ability to respond swiftly and effectively to threats. We continue to support the evolution of the Scottish Cyber Coordination Centre (SC3) as it develops its national role in coordinating response to incidents in Scotland. Additionally, the success of the CyberFirst programme in many Scottish schools highlights the value of collaboration in building a cyber-aware and skilled future workforce.

Wales

Funded by the Welsh Government and delivered in partnership with the Welsh Local Government Association, we have supported the roll-out of the Cyber Assessment Framework (CAF) across all local authorities and Fire and Rescue Services. This collaborative approach has created a consistent foundation for strengthening cyber resilience across the country. Building on this, our guidance helped the Cyber Resilience Unit (CRU) develop a suite of bilingual videos focusing on phishing, ransomware, and social engineering. These resources are helping public sector staff better recognise and respond to the most common cyber threats. Our partnership with the CRU has also seen the launch of the Cyber Exercising Programme, giving Welsh public sector organisations a trusted and controlled environment to develop, test, and refine their Cyber Incident Management Plans. The programme also ensures senior leaders understand the strategic importance of maintaining readiness in the face of cyber threats. Complementing these efforts, we have worked closely with CymruSOC — Wales' Security Operations Centre — to share threat intelligence and examples of best practice. This collaboration is helping to create a faster, smarter, and more coordinated defence against cyber attacks.

Northern Ireland

Our collaboration with Northern Ireland has continued to grow this year. NI government departments have increasingly embraced free NCSC tools and services — such as Active Cyber Defence via MyNCSC — to strengthen their security posture and protect vital services. This spirit of partnership was showcased during CyberNI Week, an event highlighting the value of partnership between the public and private sectors. The NCSC played an active role in its success, with senior staff contributing to both the inaugural CyberNI Public/Private Sector Conference and the NI government cyber security conference. Building on this momentum, NI Cyber Security Centre — supported through NCSC funding — delivered the Cyber Essentials Programme, enabling 60 SMEs to access free cyber security support. This has helped increase resilience across Northern Ireland's business community. Our work also continues to support the next generation through the CyberFirst programme, which is flourishing in NI and opening new pathways for young people to explore careers in the fast-growing cyber sector.

Trust Groups

The NCSC's sector-specific Trust Groups have continued to grow. Over 350 delegates from over 200 leading companies are now meeting regularly to exchange threat intelligence, best practices and incident response strategies in a secure and confidential environment. Following the high-profile cyber attacks on retailers in mid-2025, our Retail Sector Trust Group was immediately mobilised to ensure the wider sector was aware of the evolving threat. This allowed companies to put immediate controls in place and likely reduced the chance of other organisations being impacted.

Industry 100 (i100)

The Industry 100 (i100) scheme has continued to strengthen the NCSC's mission with specialist skills, diverse perspectives and real-world insights from private sector experts. An additional 43 new participants joined this year, seeing the community grow to an all-time high of 160 strong.

Over 80% of i100 secondees were rated as 'valuable', 'highly valuable', or 'indispensable' to delivering mission outcomes by their NCSC hosts. Impact was highest within the national resilience mission, with the energy sector overtaking finance as the aspect of critical national infrastructure most heavily represented on i100.

We have also expanded i100 expertise around emerging technologies including post-quantum cryptography, artificial intelligence, and biometric authentication. Specific highlights from i100 this year included:

- technical research into cyber security risks to the aviation sector including in relation to satellite navigation systems
- pivotal contributions to the development of the NCSC's Share and Defend capability, particularly in relation to threat intelligence data and indicator sharing
- international engagement with over 15 countries - from Ukraine to the Republic of Korea – delivering workshops about the UK's world-leading approach to public-private partnership.

Cyber League

Cyber League is a new NCSC initiative which brings together a trusted community of NCSC and industry cyber experts to work on the biggest cyber threats facing the UK. Members of Cyber League are a diverse group of industry experts, working with NCSC analysts, to bring their unique knowledge and understanding to the threat picture. They take part in a range of engagements, including analytic workshops and discussion groups. Their work is a crucial part of improving visibility and tracking existing and emerging threats to the UK.

NCSC for Startups: Celebrating a cyber security milestone

Originally launched in 2017 as 'NCSC Cyber Accelerator', the 'NCSC for Startups' programme has officially concluded, leaving behind a legacy of innovation, collaboration, and impact.

It was created to harness the agility and creativity of startups to develop cutting-edge solutions to the nation's most pressing cyber security challenges. Over the last eight years, the programme evolved into a beacon for cyber innovation, opening doors to a traditionally closed sector and welcoming university spinouts, first-time founders, and non-traditional players into the fold.

The success of NCSC for Startups is a powerful model for public-private partnership. It proves what's possible when government and startups join forces to tackle complex challenges with speed, creativity, and purpose. Though the programme has reached its conclusion, its spirit lives on in the partnerships it forged, the innovative technologies it incubated, and a resilient UK cyber ecosystem that continues to flourish.

'NCSC for Startups' at-a-glance

- Over **70 startups** supported
- More than **£550 million** raised in investment
- Over **1,700 jobs** created across the UK cyber sector
- In March 2025, recognised in the Cyber Security Sectoral Analysis 2025 as a driver of sector growth

NCSC for Startups: alumni stories

One of the programme's most enduring legacies is its alumni network which comprises a trusted community of founders and technologists who continue to collaborate, share insights, and strengthen national resilience. Some of these are graduates of the successful CyberFirst programme, which was established to identify and nurture talented students. Graduates are not just building companies; they're shaping the future of UK cyber defence.

CounterCraft

Strategic collaboration driving innovation and impact.

Thanks to the support from the NCSC and Plexal, we've made significant strides in enhancing our product capabilities. Engaging directly with NCSC experts enabled us to uncover novel methods for detecting threat actor activity and refine our techniques for gathering actionable threat intelligence.

In addition to technical improvements, the programme provided invaluable insights into strategic positioning and messaging. With NCSC's guidance, we strengthened our approach to engaging with government, particularly in high-impact sectors such as public services and financial institutions.

A key milestone was our collaboration with the US Department of Defense (DoD) through an Other Transaction Agreement facilitated by the Defense Innovation Unit. This initiative successfully prototyped CounterCraft's deception technology, demonstrating its effectiveness in preventing cyber attacks targeting DoD infrastructure. Following the prototype phase, the project transitioned into full production, substantially improving the DoD's cyber security posture.

This programme has been a transformative experience for CounterCraft, accelerating our innovation, expanding our global reach, and reinforcing our commitment to securing critical infrastructure. We're proud to be a member of the NCSC alumni community.

Intruder

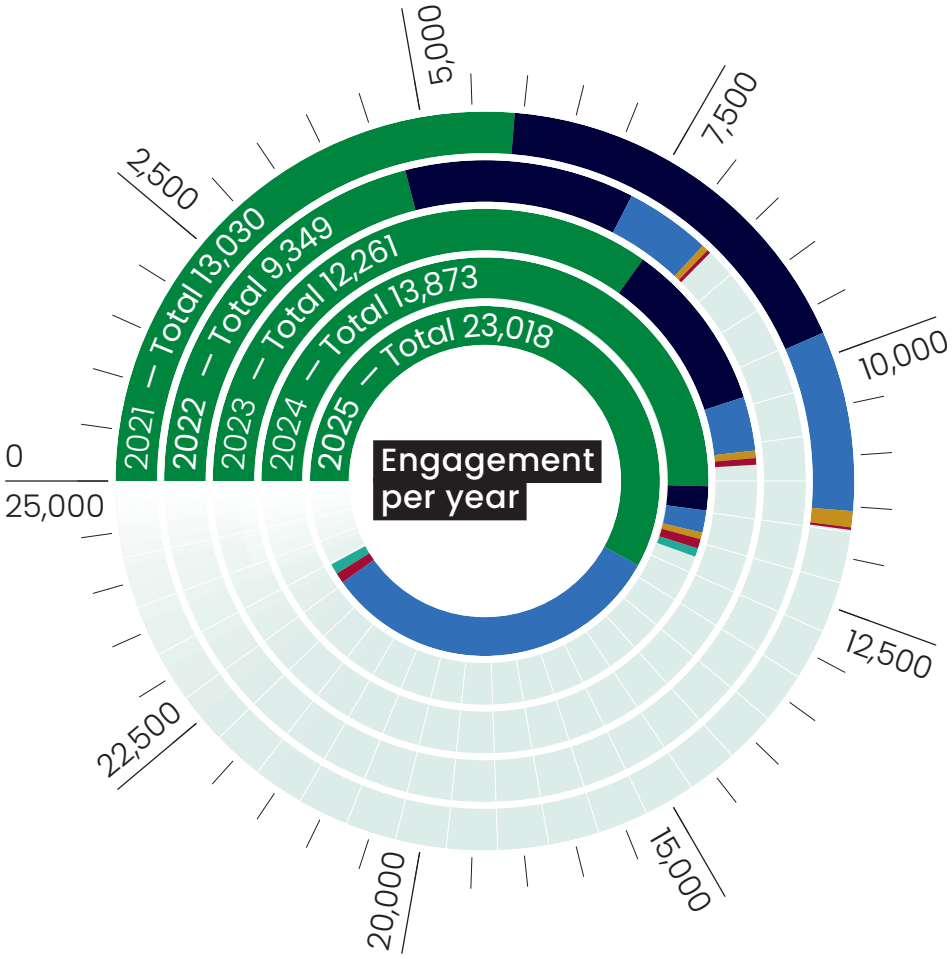
A cyber security success story sparked by NCSC for Startups.

In 2017, Chris Wallis's cyber security startup, Intruder, was in its early stages when it was selected to join the NCSC for Startups (then Cyber Accelerator) programme. The support provided enabled him to secure funding to hire a Chief Technical Officer and transition the business from a consultancy model to a product-focused company.

The programme also helped solidify Intruder's mission to protect small and medium-sized enterprises (SMEs), a goal closely aligned with the NCSC's own priorities. Chris noted that "in an industry like cyber security where credibility is everything, being selected by the NCSC helped us attract those crucial early customers and secure our first funding round."

Since completing the programme in 2018, Intruder has experienced remarkable growth. Based in London, the company now boasts a team of 60 professionals, serves over 3,000 clients globally, and generates annual revenues approaching £10 million. Intruder also remains an engaged and supportive member of the NCSC alumni community, actively contributing to its ongoing success and collaboration.

CyberFirst year-on-year analysis



Key

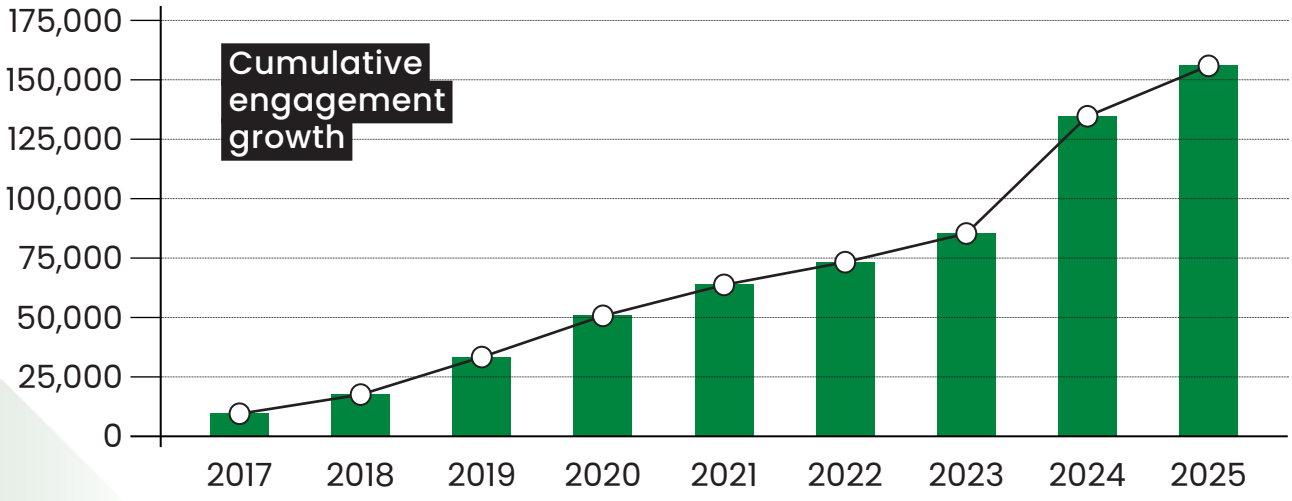
- Girls competition
- Courses applications
- Courses attendees
- Bursary
- Schools / colleges
- Ambassadors

Cyber First

Students engaged via CyberFirst Schools

2024 vs 2025

35,401 > 43,909



CyberFirst

10 years of inspiring the next generation of cyber security experts

CyberFirst was launched as an NCSC pilot in 2015, forming part of a wider DCMS strategy to increase cyber security awareness and create a pipeline of talent to the UK workforce.

Its decade-long journey is a testament to the power of collaboration, innovation, and a shared commitment to nurturing the next generation of cyber security professionals. In that time, CyberFirst has become a cornerstone of the UK's digital skills strategy, and has reached over 350,000 students across the UK, offering them the opportunity to engage in cyber challenges that build essential skills for future careers.

One of the most exciting developments over the last year was the announcement of the next generation of the CyberFirst Girls' Competition. This will be a collaboration between the NCSC, DSIT and global tech giant IBM, marking a significant milestone in the competition's evolution that builds on its growing popularity and impact.

In 2024–25, CyberFirst generated £41.4 million in social value—delivering £5.94 for every £1 invested, up from £4.06 the previous year. This rising return reflects the programme's expanding reach and its role in promoting inclusion, opportunity, and long-term impact across the UK.

CyberFirst moves to TechFirst

Following the Prime Minister's announcement at London Tech Week in June 2025, the UK government will invest £187m embedding AI, computer science, cyber security and technology throughout education. The TechFirst programme will be delivered by DSIT, and will build on the proven success of CyberFirst, further strengthening the UK's position as a global leader in cyber and tech education.

Scouts: Digital Citizen Badge

As part of Cyber Security Awareness Month, the NCSC partnered with the Scouts to launch four new activities under the Digital Citizen Badge, aimed at helping young people aged 8 to 14 develop essential cyber

security skills. Designed with NCSC experts, the activities focused on creating strong passwords, spotting phishing attempts, protecting personal data, and backing up digital assets and has proven popular with Scout groups across the UK. By equipping Scouts with essential knowledge about online safety, the NCSC is ensuring they can protect themselves against cyber threats and make informed choices in an increasingly digital society.

Higher education

NCSC-certified degree courses help universities to attract high quality students from around the world, and prospective students to make informed choices when considering the hundreds of institutions that now offer cyber security content. Following a thorough assessment by a panel of academic, industry and government experts against NCSC's high standards, there are now 92 certified degree courses (up 14 from last year), comprising 14 undergraduate, 73 post-graduate and 5 apprenticeships.

Since its launch in 2020, the programme for Academic Centres of Excellence in Cyber Security Education (ACEs-CSE) has recognised UK universities with gold and silver awards for showing their commitment to delivering first-rate cyber security education on campus and to their wider community. 13 universities are now recognised at the gold standard across the UK.

CSE Connect

CSE Connect is a national network of Cyber Security Education (CSE) strategists, practitioners, and learners. Through support from the NCSC, CSE Connect work to promote impactful CSE collaborations, knowledge sharing, skills acquisition, and good practice throughout all key stages of the education 'pipeline'. CSE Connect works closely with government, industry, and academia to establish a culture of innovative cyber security education across the UK. The support from partners has been fundamental to activities nationally and internationally. CSE Connect continues to build opportunities and stronger pathways for current and future generations of cyber practitioners to learn, engage and innovate.

The Cyber Security Body of Knowledge (CyBOK)

Supported by the NCSC and a wide range of national and international collaborators from government, industry and academia, CyBOK has continued to go from strength to strength. CyBOK is the standard for NCSC assured training and forms the basis of the pathways for the 15 specialisms in the Cyber Security Council's Career Framework. It surpassed 1.5m downloads this year, underpinning NCSC's certification of undergraduate and master's programmes in cyber security.

The CyBOK team has been developing the core Body of Knowledge and mobilising the community to

develop additional resources such as hands-on training materials, and guidance and support for learners and educators from schools to FE colleges through to universities and industry training programmes. The CyBOK Community Interest Company was incorporated in November 2024 and will become the long-term home of the CyBOK, providing sustainability and longevity to an 8-year research initiative supported by the National Cyber Security Programme.

CYBERUK 2025

In 2025, CYBERUK – the UK government's flagship cyber security event – returned to Manchester. The North West, with its growing digital economy and strong academic and industrial base, provided a fitting backdrop for a conference focused on resilience, innovation, and collaboration.

The event explored how the UK can seize the initiative from adversaries and transform its cyber ecosystem. The event featured 131 speakers across 36 sessions and the programme included technical masterclasses, workshops, and spotlight talks, offering 38 hours of content over two days.

CYBERUK 2025 at-a-glance

£2.3m boost

to the local economy

3,134 in-person attendees

from **36** countries

175 sponsors & exhibitors

including startups, SMEs, and global leaders.

94% of delegates

rated the event as good or excellent.

CYBERUK will be making its way back to Glasgow, 21–23 April 2026, as we celebrate its 10th anniversary.

Chapter 3

Keeping pace with evolving technology

Resilience is only as strong as the technology it's built on

The NCSC is focused on ensuring that our defences remain agile, adaptive, and future-ready. As technologies such as post-quantum cryptography (PQC), AI and passkeys redefine both the threat and the tools we use to build cyber resilience, the NCSC is playing an active role in shaping the development of these foundational technologies. Our contributions to global standards around AI and PQC will underpin cyber security for decades to come, and will help to make the internet, organisations that use it and UK citizens more secure.

Artificial intelligence

Over the past year, the NCSC has significantly advanced its work in artificial intelligence, focusing on securing AI systems, enabling autonomous cyber defence, and deepening collaboration across government, academia, and industry. This period marked the first full operational year of the Lab for AI Security Research (LASR), the publication of the AI Security Code of Practice, and major progress in understanding the potential of agentic AI for cyber defence.

Securing AI systems and establishing standards

A cornerstone achievement was the publication of the AI Security Code of Practice, developed jointly with DSIT. This lead to the development of the first global standard that sets minimum security requirements across the entire AI life cycle for all stakeholders in the AI supply chain, published by the European Telecommunications Standards Institute (ETSI). The Code of Practice builds on the NCSC's Guidelines for secure AI system development and has been widely adopted across sectors and internationally endorsed by 18 countries.

The NCSC contributed to workshops and consultations with stakeholders such as the Coalition for Secure AI, the Financial Conduct Authority, and the G7, helping shape global approaches to AI security, including Software Bills of Materials (SBOMs) for AI and conformity assessments.

Deliveries from LASR and Research Partnerships

The Laboratory for AI Security Research (LASR) has become a central pillar of the UK's AI security ecosystem, and the NCSC has played a leading role in its establishment, direction, and delivery. As the primary government sponsor and technical lead, the NCSC has shaped LASR's research agenda, coordinated cross-sector engagement, and ensured alignment with national cyber defence priorities.

The first year of LASR saw the delivery of impactful research from partners including the Alan Turing Institute, Queen's University Belfast, Lancaster University, and others. Key outputs included:

- research into secure federated learning, and adversarial patch mitigation
- a novel taxonomy of attacks and defences on AI systems, enabling systematic gap analysis
- the launch of an AI Security Demonstrator with Cisco, focused on CNI scenarios
- a new heatmap tool to visualise LASR research activity and identify priority areas

Other research partnerships supported the development of an agentic AI demonstrator for automated Sigma rule generation and refinement, and contributed to defensive AI red-teaming research, helping shape future cyber defence scenarios.

Human-AI collaboration and teaming

Recognising the importance of effective Human-AI teaming, the NCSC produced a dedicated problem book on Human-AI Collaboration for Cyber Defence, outlining research priorities and identifying potential collaborators. The BLUE HAI project from Lancaster University delivered a blueprint for dynamic task allocation in mixed teams, while

other initiatives explored emotional and behavioural responses to AI in high-stakes environments.

Autonomous cyber defence

The NCSC has made major strides in autonomous cyber defence, supporting the development of AI agents capable of defending networks with minimal human intervention. A foundational research plan, developed with MITRE and the Turing Institute, sets out a roadmap for experiments in evaluation, explainability, assurance, and adversary modelling.

Real-world experimentation platforms such as R3ACE and CAGE-Challenge-2 have enabled testing of reinforcement learning agents in dynamic environments. Collaborations with the Dstl ARCD programme, US National Labs, and international partners have provided high-quality datasets and experimental frameworks for advancing autonomous defence capabilities.

Agentic AI

A key strategic focus this year has been agentic AI systems that exhibit autonomous decision-making capabilities, including the ability to perceive, reason, act, and learn independently. These systems can operate without direct human oversight, pursue goals, and adapt to changing environments. While agentic AI offers powerful capabilities for cyber defence, it also introduces new risks related to control, alignment, and misuse.

The NCSC has:

- provided feedback on the OWASP Top-10 for Agentic AI Security
- participated in the Agentic AI Security Forum
- engaged with leading labs such as Anthropic, Google DeepMind, and Palo Alto Networks to define cyber risk thresholds and safeguards for frontier models

Joint exercises with Cybersecurity and Infrastructure Security Agency (CISA), the FCA, and the NSA explored the use of agentic AI in automating incident response and red/blue agent testing.

Research into multi-agent platforms for cyber security decision-making, iterative threat detection, and adversary emulation continues to push the boundaries of what is possible in AI-enabled defence. The NCSC remains committed to ensuring that agentic AI is deployed securely and responsibly, with robust safeguards and clear operational oversight.

Passkeys

Passkeys are a global effort to replace passwords and traditional second factors of authentication. Passkeys provide an easier, faster and more secure way to log in. The NCSC would like to see passkeys become the default authentication recommendation, recognising their critical role in strengthening the UK's cyber resilience at scale, and reducing

systemic risks associated with legacy authentication technologies.

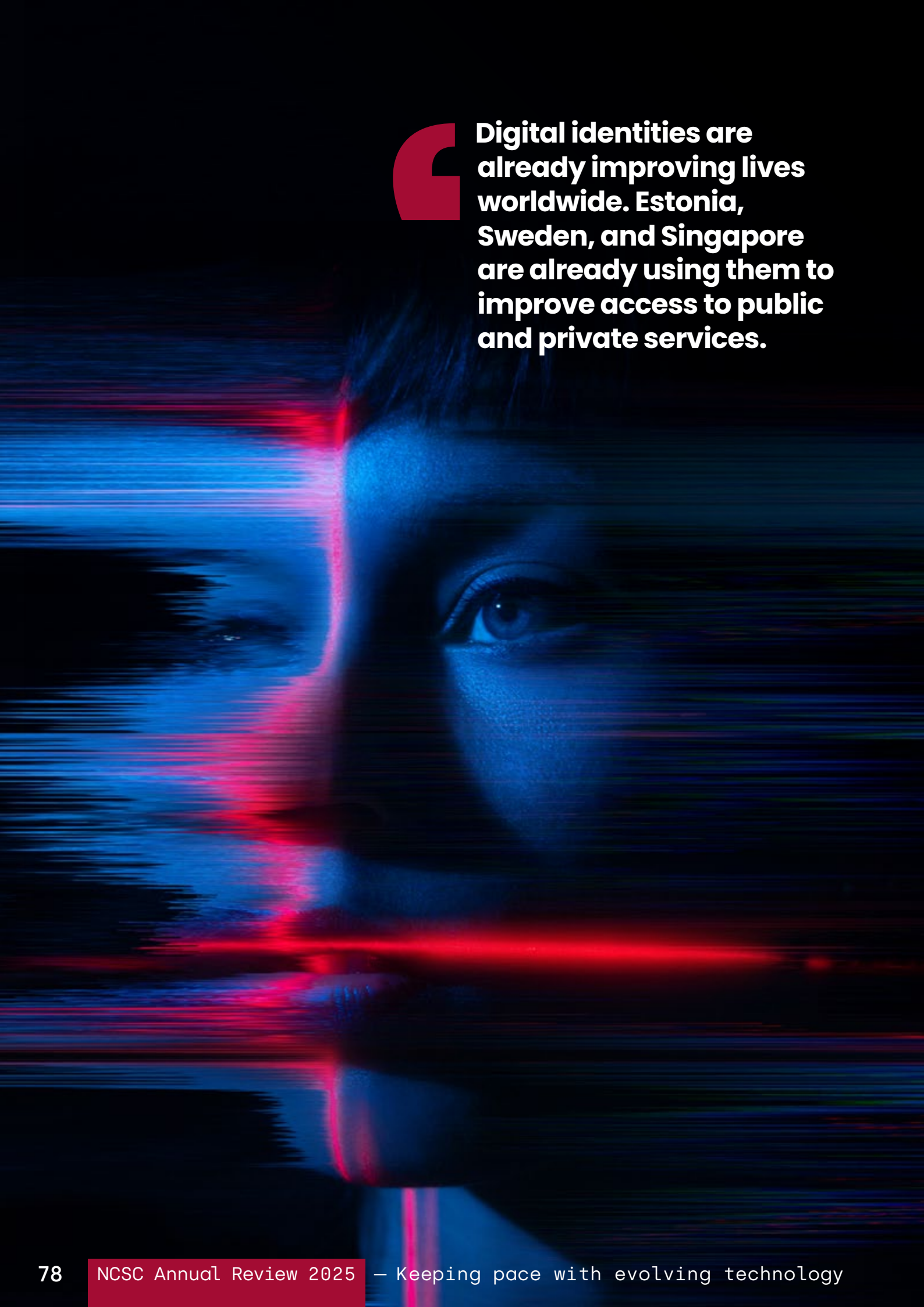
As with many new technologies, organisations need to understand passkeys to realise the benefits they offer. In the last year, the NCSC has established a virtual team to accelerate the adoption of passkeys in the UK, to enable faster, more secure online experiences for all. This team is encouraging providers to design good passkey experiences across their apps and websites, and working with other FIDO Alliance members (who own and develop the passkey standards) to generate national and international momentum for passkey adoption.

We have also explored where UK government can lead by example, such as by giving citizens the option to use passkeys to access a range of public services using the government's GOV.UK site.

This has also included reviewing the regulatory environment and updating rules and standards that underpin how UK organisations offer services to customers to ensure that sites can confidently and safely offer passkeys.

The team has also been gathering statistics and research from various parties, including research to understand personal attitudes towards online identity and account security. We have also been collecting data to understand a range of organisations' readiness, motivations, and concerns for passkey adoption.

In the coming year, the NCSC will be publishing content (such as implementation guides, security papers and guidance) to make it easier for organisations to adopt passkeys, as well as working directly with key organisations to accelerate adoption.



> **Digital identities are already improving lives worldwide. Estonia, Sweden, and Singapore are already using them to improve access to public and private services.**

The future of digital identity

Why digital identity is fundamental to supporting the transformation of the UK's 'digital-first' services.

Many aspects of our lives are increasingly conducted digitally to benefit from the speed and convenience this can provide. Everything from keeping in touch with friends and family, to shopping and banking, to renting or buying a property, to enrolling in university or starting a job, to managing long-term pension and healthcare choices.

Adding to this, the COVID-19 pandemic triggered a rapid acceleration of digitisation across many sectors, proving that previously in-person and paper-based services could be moved online to get these same benefits. In the years since, this continued digitisation of services has only increased the importance of having an effective 'digital identity' architecture that underpins them. This architecture needs to be easy enough to use whilst also strong enough to protect the privacy and provide the security that's required for people accessing all these services.

The future of digital identity is developing rapidly, but it is already clear that usability, privacy, and security will need to be balanced at the heart of it.

Before we go any further, it's useful to clarify what we mean by 'digital identity'. It can be described as a digital representation of a set of verified *attributes, derived attributes* and *properties*. With this representation, digital systems can use necessary attributes and properties during their decision-making. For example, a business being able to check if someone is over the age of 18 according to a mutually trusted source:

Date of Birth/Age

- attribute - **Date of Birth:** 2008-Feb-29
- derived attributes - **Over 13:** True; **Over 15:** True; **Over 16:** True; **Over 18:** False
- properties - **Issued by:** General Register Office, (HMPO) **Issue date:** 2024-Mar-04

Whilst the most common form of digital identity that we talk about is for a person, an identity can also apply to other entities, such as:

- a group, such as 'Occupier(s) of 32 Windsor Gardens' for proof-of-address, e.g. registering for the Electoral Register and accessing household streaming services

- an organisation, such as 'The Winchester' for proof-of-certification, e.g. VAT registration and business licence
- a device, such as 'Personal smartphone', 'Family tablet' and, 'Work laptop' to help establish trust and feed into a decision, e.g. making repeated payments from the same device
- a place, such as 'Home', 'School', and, 'Work' to help feed into a decision, e.g. making a request from a recognised or explicitly trusted location

Note that a digital identity should uniquely represent one entity, allowing a digital system to differentiate and address this entity from all others of its kind. A digital identity will be as complex as required, from a simple set that only comprises a unique username or account ID (such as on a personal membership), to a comprehensive set containing enough personal data to match an individual physical, natural-world identity (such as for meeting 'Know Your Customer' requirements).

Digital identities are already improving lives worldwide. Countries like Estonia, Sweden, and Singapore are already using them to improve access to public and private services. However, not all digital identities are equal; one may let you buy something from a shop, another may let you open a bank account, and another may help you vote or access healthcare. What is clear is that digital identities can work, and their benefits are already apparent.

Digital identity: underpinning the UK's digital services

Across a number of sectors, digital identity is a foundational building block in the 'digital-first' transformation that promises a faster, smoother, and more secure future, including:

Defence: The Strategic Defence Review 2025 highlights that 'data and digital systems are the fundamental underpinnings of all modern military capabilities'.

Government: DSIT's Blueprint for modern digital government defines 'a digital-first operating model', including the **One Login** and **Digital Wallet** services that can support the Digital ID scheme that will be mandatory for Right to Work checks and enable more personalised interactions with public services through the GOV.UK app.

Healthcare: NHS Digital has set out a 'nationally agreed approach to identity management' to encourage greater use of digitised health and care services accessible through NHS login and the NHS App.

Education: some universities such as Sheffield are beginning to issue signed transcripts to allow graduates to prove their qualifications.

As this pace of change continues, the ability of digital systems to make accurate decisions - for example, confirming the coordinates of an entity so supplies can be airdropped - is more important than ever. In such scenarios, gathering enough

confidence and trust in a digital identity is crucial. Looking ahead, further transformations including artificial intelligence and digital assistants are promising to make decisions at line-speed on behalf of its user.

Digital identity systems have the potential to be more difficult for attackers to compromise than traditional identity systems, if they are designed and implemented correctly. Naturally the increased use of digital identities attracts increased interest from threat actors, looking to take advantage of weaknesses for their own gains. Attackers of all capabilities are pivoting away from targeting individual devices in favour of targeting user identity. For example, impersonating a user on helpdesk calls to reset an identity's access credentials , or phishing for valid access credentials from an online identity provider to access its connected services.

Attackers are also quick in adopting novel technology to aid them, including the use of AI in the creation of 'deepfake' video and audio that be used for impersonation attacks, or to falsify identity documents that can pass weak examination and identity checks. Adding to this, the continuing trend in data breaches means the amount of 'secret answer' information that can be used to securely verify an identity (such as previous addresses, schools, and personal reference numbers) is diminishing.

All this to say that robust digital identity underpins the fundamental aspects of a modern and future-looking society.

The fundamentals of future-ready digital identities

At a high level, the challenges and problems of building a robust digital identity ecosystem breaks down into four core areas:

- registration
- authentication
- management
- secure channels

When building such a system, it must be determined what attributes and properties must be collected and verified to meet current and projected future requirements. However, it must be noted that only the necessary and sufficient information for the current usage is gathered and stored securely to meet privacy and data protection requirements.

Registration

When a new entity 'enrols in' or is 'onboarded onto' a system, the system must create an identity that it can assign to that entity. This assignment is built and registered by the system in a data store such as a User Directory or Device Management database.

The registration phase is the most security critical since it establishes the initial trust relationship and sets the foundation for all future trust between the system and the entity. It is not possible to add trust in an entity after registration,

without relying on trust established during registration. When designing registration mechanisms, the following are important to consider:

- How effectively must and can we verify these attributes and properties? How might this change in the future?
- How long should these attributes and properties be treated as valid for, before they must/should be re-verified?

> **'Modern solutions for authentication rely on the assumption that everyone owns a device capable of supporting modern cryptography.'**

A digital identity is most commonly used to represent a user of a system, either one 'natural person' or a group of people that are safe to appear as one to the system. When registering a personal digital identity, such as an employee or customer, a system needs to perform the necessary verification of the identity's properties and attributes. Knowing what exactly constitutes 'necessary' is a significant challenge, as it depends on the needs and sensitivity of the system. Unfortunately, this means that there isn't one universal digital identity architecture that can work out-of-the-box for all systems.

A digital identity future will include the challenge of sufficiently strengthening the processes for verifying *digital* sources of trust where we currently use *physical* (i.e. natural-world) ones. For example, building and scaling the processes that can provide the digital equivalent of checking the holograms and photographs of a UK passport or driving licence documents to detect the presentation of falsified identity attributes.

With digital identity, cryptographic verification and a digital web of trust can be used to meet this, and unlock even more opportunities. However, this must all be done without also infringing on privacy protections and unacceptably increasing the risk of fraudulent registration. One architecture for this is already being built out in the UK digital identity and attributes trust framework.

An important challenge in personal digital identity is making sure the ways we request and verify identity are as inclusive as possible. For example, an estimated one in twenty UK adults don't own a personal smartphone, and some people with disabilities are unable to use them. In any registration process, it is critical that the identity verification methods used are fit for all users that will be required to use them. This often means offering multiple methods and allowing users to opt in to that which is most agreeable to them.

Recall, digital identities are not only for people; there are also systems where registration of other kinds of entities or assets is needed. Depending on the system, this can be anything from registering the identity of an aircraft carrier to avoid friendly fire, down to

the identity of a wearable device like a smartwatch or pair of smart glasses that is trying to access personal data. Whilst registering a Royal Navy aircraft carrier seems relatively easy (there's two of them and they're quite distinctive), this process gets much more challenging for the likes of cars and drones and phones that have much greater numbers and whose ownership and integrity are much harder to verify.

Authentication

When an entity returns to a system claiming to be already registered, the system must discern if it is the same entity that was previously onboarded. In this workflow, we don't want to completely re-verify the identity every time they knock on the system's virtual front-door, so we try to prove ('authenticate') to a high-enough level of assurance that it really is the same entity, using a digital, often remote, challenge. This challenge uses a combination of digitised attributes and their properties, captured during registration, that only the 'authentic' entity should be able to complete. If the challenge of authentication is not strong enough, it provides a weakness that an attacker can exploit to gain unauthorised access.

In digital systems, this authentication needs to provide strong enough assurance to the service for it to accept the risk of allowing access. Increasingly, modern solutions for strong authentication are available that make better use of modern device hardware that includes secure elements with cryptographic modules. These modern solutions use the capabilities of digital technology to handle a digital problem. A perfect example of this is passkeys and their use of a trusted device's secure element and local authentication hardware to handle the complex cryptography and digital exchanges, providing a more secure and easier authentication process by only placing burden on the user when their choice and approval is required.

Modern, digital solutions for authentication can offer speed and security over traditional means, but they often rely on the assumption that everyone owns a device capable of supporting modern cryptography. If this assumption is not actively addressed or resolved, we risk people being left behind, or being unfairly placed at greater risk than those who do.

Management of a digital identity

As with a physical, natural-world identity, while some aspects of a digital identity are not expected to change (such as a person's confirmed Date of Birth), some aspects may change to a significant extent. For example:

- change of legal name or chosen username
- change of a contact and/or residence address
- change of payment details or financial account information
- change in biometric features
- reset of a forgotten password or replacement of lost passkey

This means that digital identities need management and maintenance to remain accurate and useful. Digital identities provide the benefit that the records of their attributes and properties are comparably easier and faster to create and update than paper-based records. For example, being able to confirm your address using an existing digital contract agreement, avoiding the need to wait for a letter to arrive in the post. However, this relies on strongly authenticating the request to change an identity record to verify its legitimacy, and then verifying the accuracy of the requested change before completing this process. With the relative ease and speed of changes also comes the drawback that mismanagement (accidental or intentional) can also cause greater harm. This must be risk managed in the future digital identity architecture being built.

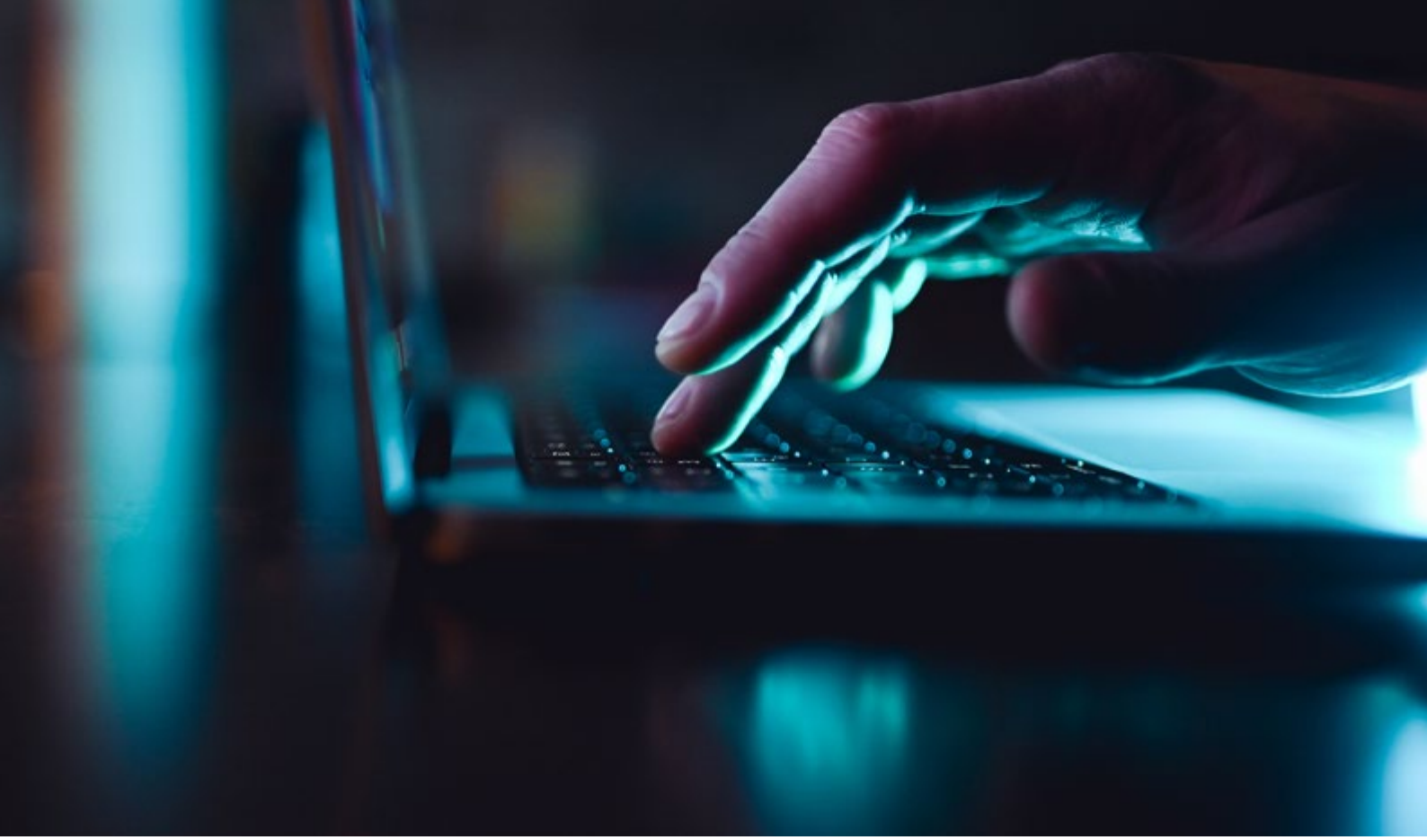
This includes making it known, where beneficial, that one or more attributes or properties of an identity have changed. This requires a communication framework that makes it secure and easy enough for a person to tell a service about a change. This can also include the option for this service to tell other related services of the change to inform their security decision making. A good demonstration of this is the UK government's 'Tell Us Once' service, which can simultaneously notify relevant services of a change in an identity's circumstances after it has been verified.

Secure channels

Registration, authentication, and management of digital identities require trusted digital communication channels. These cover communication between the entity and the verifier, and in modern systems, between a verifier and other verifiers. For example, a job applicant sharing necessary identity attributes with a prospective employer, and the prospective employer who is verifying these attributes to confirm the applicant's right to work and authenticity/validity of their claimed qualifications.

For the vast majority of people and public services, the communication protocols used in commodity devices and services are 'secure enough' against today's threats, and they have demonstrated that they can develop quickly enough to keep up with the latest best practices.

In spaces like military and critical national infrastructure systems, many use cases are more complex, and the effort attackers might use to undermine the security of these communications is significantly higher. This requires commensurately stronger confidence around the identity of each entity involved in these communications and their attributes, including how securely they can create, process, and store the communications that they will receive and transmit as part of these systems.



What the NCSC is doing

Robust digital identity is a long-term problem with a lot of moving parts. Within the defence sector, this is a multi-decade problem where systems and platforms commissioned now will be in service in 2050 and beyond. The NCSC's Crypt-Key mission is providing solutions to defence now, and is working in partnership to understand and meet the perceived future needs of these systems.

In wider UK public sector applications, the NCSC is working with DSIT on supporting better registration and on-boarding processes, through the issuing and use of digital credentials from the GOV.UK Wallet. This is part of a longer-term strategy to demonstrate the value that digital identities and trust verification can unlock in solving challenges across UK society.

To improve the security of authentication, the NCSC is working with DSIT and the FIDO Alliance on improving the adoption of passkeys across the public and private sectors. Accelerating the UK adoption of passkeys means we can migrate people off passwords and weak MFA methods, onto something that is more secure and makes interacting with companies and government more seamless.

And finally, the NCSC's work on advanced cryptography makes us the expert on where novel cryptography can help solve a problem within digital identity, such as by being able to securely enough prove that a person is eligible for a service without unnecessarily revealing other attributes about themselves.

Migrating to post-quantum cryptography

Migration to post-quantum cryptography (PQC) to protect against the threat from a future large-scale quantum computer, is an international, multi-year technology change programme.

In March 2025, the NCSC published new guidance setting timelines for key activities in the migration, which comprise:

- **2028** - the target date for completing an initial migration plan that covers the entirety of your estate, and identifies services dependent on cryptography that will need to be upgraded to PQC
- **2031** - the target date for migrating the highest priority services, and for refining your initial migration plan
- **2035** - the target date for completing migration to PQC for all your systems, services and products

These timelines are now included in many organisations' plans, and will underpin the work within government and regulated sectors to enable a smooth migration. But to ease this migration, we also need to grow the number of UK consultancies that have the right expertise.

In 2025, the NCSC launched a pilot PQC consultancy scheme, which assures providers offering independent consultancy services to organisations with complex or high-risk cyber security requirements. We have successfully on-boarded the first 8 companies, whose services government and industry will be able to use with confidence.

Growing skills by certifying consultancies is just is one way of supporting the PQC ecosystem. Another is by contributing to global standards. The NCSC has authored a global standard defining precise terminology for PQC*, which is already being widely used as a foundational reference in other standards. This enables accurate descriptions and comparisons of the security of PQC schemes, which is essential for understanding their cyber security benefit.

*RFC 9794: Terminology for Post-Quantum Traditional Hybrid Schemes.

Crypt-Key

The NCSC collaborates with UK and international partners to protect our most sensitive information using our cryptographic expertise, known as 'Crypt-Key'.

Crypt-Key enables our most important capabilities and ensures the UK has high confidence in critical systems against the most advanced cyber threats. The NCSC's National Crypt-Key Centre (NCKC) remains central to developing and maintaining secure communications for government, military, industry and national security partners within the UK, and to ensure interoperability with key allies as technology and threats evolve.

Throughout 2024, the NCSC produced and distributed thousands of highly secure cryptographic keys to protect the UK's most sensitive data whilst continuing to build capabilities to support and key the next generation of cryptographic devices. This is only achieved in concert with the UK's sovereign Crypt-Key industry, a national asset that has collaborated with us throughout 2024 to deliver world-leading encryption products.

Working with the MOD, the NCSC is also leading a major transformation in Crypt-Key that will benefit the UK's defence capabilities for many years to come. The Joint Crypt Key Programme (JCKP) is a £2.6 billion initiative that protects the MOD's people, platforms, networks and information and provides high-grade cryptography for mission-critical services, enhancing cyber security and trust among allies. 2024 has seen JCKP gain ministerial approval of the next major phase of Crypt-Key transformation. This phase will deliver an adaptable and innovative architecture, ready to face the threats to defence over the coming decades, through collaboration between government and the UK sovereign Crypt-Key industry.

‘Crypt-Key secures the nation’s most critical systems, and drives domestic innovation.’

From Bletchley to the battlefield

Crypt-Key and the evolution of UK cyber defence

In an era defined by geopolitical uncertainty and relentless cyber threats, Crypt-Key has quietly but decisively shaped the UK's national security posture.

Often operating behind the scenes, Crypt-Key is the cryptographic engine that secures the UK's most sensitive information across defence, government, and international operations. It's not just a tool – it's a strategic capability. And in 2025, it is as important as ever that this work continues to evolve and keep pace with changing threats and emerging technologies.

This important capability is built on a legacy of excellence. Throughout its history, GCHQ has attracted and developed world-class expertise in information assurance and security, notably in cryptography.

From its origins in 1919, through the legendary work at Bletchley Park, to the pioneering creation of public key cryptography by James Ellis and colleagues in the 1960s, the UK has consistently been at the forefront of cryptographic innovation. Crypt-Key is built on that legacy, and we must continue to evolve, operationalise and deploy to meet today's most complex security challenges.

Crypt-Key predates the internet, yet it remains at the forefront of cyber defence. Designed to withstand the most advanced and persistent threats, it operates in highly contested environments, from battlefield networks to government communications. Its ubiquity across military platforms and civil infrastructure speaks to its enduring relevance.

But Crypt-Key is not standing still. Under the leadership of the NCSC, it is evolving to meet new challenges. In 2025 alone, the NCSC approved a dozen new Crypt-Key products and variants for operational use, each one reflecting the UK's commitment to staying ahead of the threat curve.

Growth through sovereign capability

One of the most striking developments this year is the acceleration of Crypt-Key innovation through UK industry. The NCSC now partners

with four specialist UK suppliers to develop the next generation of network cryptographic devices. These technologies are not only securing classified UK networks, they're being adopted by friendly governments, turning Crypt-Key into a quiet export success story.

> **'The UK has consistently been at the forefront of cryptographic innovation.'**

The approval of the first Secure Key Management (SKM) component marks a major milestone. For the first time, the UK has full over-the-network keying capability[1], dramatically enhancing operational flexibility and resilience. This growth reflects a strategic focus on high-tech investment, sovereign capability, and the 'edge' of the UK's domestic cyber ecosystem that leads on the global stage.

Global standards, international trust

Crypt-Key is also a diplomatic asset. In 2025, the NCSC led a landmark demonstration of secure interoperability between approximately 20 secure voice crypto devices from eight NATO nations.

Powered by Crypt-Key standards developed in the UK, this achievement underscores Britain's leadership in setting the benchmarks for secure multinational communications.

The NCSC continues to work closely with allied national security agencies to ensure mutual confidence in the protection of shared information. In an increasingly interconnected world, trust in cryptographic standards is not just technical – it's strategic.

Joint delivery for the next decade

The **Joint Crypt Key Programme** (JCKP), jointly led by the Ministry of Defence (MOD) and the NCSC, is delivering key management solutions to support operational access to Crypt-Key protected networks. This includes future defence platforms such as the Future Combat Air System (FCAS), where Crypt-Key remains a core component of secure communications.

The NCSC's leadership in design and assurance ensures these solutions meet the operational demands of the next decade and beyond. The integration of Crypt-Key into major defence programmes reflects its centrality to the UK's long-term strategic planning.

1 A method of distributing authentication keys over the network to ECUs, removing the need for central key generation and physical key distribution / installation.

Operational backbone and resilience

Beyond development, Crypt-Key is a daily operational reality. The NCSC provides critical support through entropy generation and key provision, enabling mission and network managers to control access to protected services. In 2025, the UK Key Production Authority (UKKPA) produced thousands of operational keys across a wide range of Crypt-Key systems, ensuring continuity and resilience.

Investments in secondary sites and contingency capabilities are also underway, reinforcing the UK's ability to maintain secure operations under any circumstances.

Meeting the challenge head-on

As the UK deepens its investment in cyber resilience and technological growth, Crypt-Key stands out as a quiet but powerful enabler. It secures the nation's most critical systems, supports international trust, and drives domestic innovation. In 2025, Crypt-Key is not just keeping pace but setting the pace. And in doing so, it's helping to shape a future where the UK remains a global leader in cyber defence.

Crypt-Key is not without its challenges. It demands constant vigilance, technological agility, and strategic foresight. The NCSC continues to navigate this complex area, guided by clear priorities: strengthening UK industry partnerships, enhancing interoperability with allies, driving innovation in cryptographic design, and ensuring resilient delivery across defence and government.

Initiate

'Initiate' is part of the NCSC's extensive research portfolio. That portfolio contributes to our advice and guidance, shapes the services we provide and the future products that will continue to protect the UK's most sensitive information and capabilities.

Innovating for a secure tomorrow

Bright Sparks is the term we use to describe the innovative products that will be commercialised to significantly improve cyber security. While our focus is predominantly for use across government, some products - such as the two here - may be able to deliver UK wide value.

WIRED GLASS is a small, low-cost device that prevents digital video connections being used to attack connected devices. It essentially acts as a firewall – ensuring that any data going in either direction, from laptop to monitor and back again, is what you expect to see. Anything unexpected is blocked. This stops the display cable being used to attack your devices or exfiltrate your data. Using the WIRED GLASS device, a user can (for example) safely connect laptops that contain sensitive information to external projectors or monitors, removing the need for multiple screens on a desk.

Retransmit is a new hardware sleeve for mobile phones which looks very similar to a normal battery sleeve. The use of the sleeve reduces the risk of baseband attacks from a fake cellphone tower, or when operating in locations where local cell and wifi connections can't be trusted. This is achieved by offboarding connections from the mobile phone to dedicated chips within the sleeve, allowing the mobile phone to remain in flight mode.

NCSC Engineering: Practising what we preach

The NCSC doesn't just advise others on how to build secure systems. We design, develop and support our own systems too. In line with the NCSC's own guidance, we continuously evolve our business-critical and research platforms to ensure they remain secure, resilient, and fit for purpose. We apply the same principles we advocate to others, leading by example and embedding security into every stage of our engineering life cycle.

For example, for our highly sensitive Crypt-Key mission, we adopt the NCSC's Design Guidelines for high assurance products.

For our 'internet-facing' research and business projects, we put theory into practice using the principles found across the 10 Steps to Cyber Security and use the Cyber Assessment Framework.

Compliance through continuous assurance

We strive to continuously review and amend our policies and compliance stance. The devices that NCSC staff use must meet strict criteria to access environments, and non-compliant ones are automatically restricted from accessing key environments. Criteria include:

- patch management (devices must be up-to-date with the latest cumulative updates; falling behind triggers access restrictions)
- endpoint protection (all devices are enrolled in endpoint protection systems)
- encryption & access control (on-device encryption, secure boot, and code integrity are enforced, and MFA is mandatory)

NCSC Engineering exemplifies the principles we advocate. For us, security is not just a checklist, it's a mindset, and we foster a culture of secure engineering through exercising. By embedding security into every layer of our platforms, we strive to ensure that our systems are not only compliant but also robust, agile, and secure. Platform security is a never-ending challenge, and we face it head on. As threats evolve, so do we. Our roadmap for the next year includes; expanding zero-trust architecture, enhancing automation, and adopting a posture of 'Verify explicitly, least privilege, and assume breach'

We're not just advising the UK on cyber security - we're living it!

NCSC guidance

The NCSC's clear, timely advice helps businesses of all sizes, charities, security professionals and members of the public, to understand and mitigate cyber threats. From best practice frameworks to incident response support, the NCSC's resources empower organisations to make informed decisions, build robust security strategies, and respond effectively to emerging risks.

This year, we set out clear timelines for migration to post-quantum cryptography, complemented by technical papers exploring advanced cryptographic methods and quantum networking technologies, laying the groundwork for long-term resilience.

In support of the next generation of Active Cyber Defence (ACD) services, we published the results of the first ACD 2.0 experiment, focusing on external attack surface management. On the human side of cyber security, we released a set of cyber security culture principles, new guidance on effective communication during incidents, and board-level training materials to strengthen cyber governance. We also provided practical advice on how to engage boards in meaningful cyber discussions.

Collaboration remained central to our approach. Working with international partners, including the Five Eyes alliance, we co-authored guidance on digital forensics and protective monitoring. We also contributed to the growing conversation around passwordless authentication, publishing three blog posts on passkeys—a key theme at CYBERUK 2025:

- **Trust the tech**: Using password managers and passkeys to help you stay secure online
- **Passkeys**: Not perfect, but getting better
- **Passkeys** and their promise: A simpler alternative to passwords

In total, we published or refreshed **64 guidance and blog products**, including **35 blog posts** and **29 formal guidance documents**.

Key guidance highlights

Among the major guidance published or updated this year were:

- Cyber Assessment Framework (CAF) 4.0
- Security principles for protecting sensitive personal information (SPI)
- Software Security Code of Practice
- Securing HTTP-based APIs
- Good security practice for domain registrars
- Principles for secure privileged access workstations (PAWs)
- Network security fundamentals
- A method to assess 'forgivable' vs 'unforgivable' vulnerabilities
- Guidance for brands to help advertising partners counter malvertising
- Multi-factor authentication for your corporate online services

‘Radical transparency’

The key to enabling better cyber security outcomes

Technology is currently opaque, and that leads to adverse cyber security outcomes, which favour malfeasant threat actors.

Understanding in detail the cyber security of a modern technology product or system requires expert knowledge, time and skill. Security professionals must patiently conduct deep analysis, identify weaknesses, and then work with vendors and systems integrators on a resolution.

This approach obviously does not scale, leading to the worrying observation that it is easier for an attacker to get useful data – either through reverse engineering or internet scanning – than it is for a defender. The former only needs to dive deep on one part of a system in order to identify any weakness, and exploit it. In contrast, defenders require a complete understanding in order to the protect the entire system (or system of systems).

The NCSC believes we have to address this imbalance in cost and complexity that at the moment favours malfeasant threat actors.

Previous initiatives have encouraged the adoption of Software Bills of Materials (SBOMs). And whilst SBOMs (and HBOMs) can provide organisations with better insight into their supply chains, they are not enough on their own. We need to be much clearer about which cyber security decisions are important, and work hard to make better supporting evidence available. A lot of those decisions do not concern technology; they involve management of business/legal risk or organisational governance. Our job is to translate technical insights to justify investment, to support a different direction or to defend a course of action, potentially in court.

Sausages and incentives

For some time now, the NCSC has been calling for more effort to improve transparency in technology to enable better cyber security outcomes. This is across hardware, software and services.

At this year's CYBERUK technology plenary, the NCSC's Ollie Whitehouse quipped that "we know more about what's in our sausages than our software, and that's probably not right for 2025". The serious point here, is that making it easier to identify the technology products in the supply chain (and what those products comprise) would enable developers to compete on security, and support better-informed decision making by customers.

Clearly there are limits; details of vulnerabilities can accelerate exploitation, and commercial sensitivities need to be respected. Nonetheless, there must be more we can do to expose information needed in the appropriate way to provide evidence and insights for impactful cyber security decision making.

Here are some of the 'important questions' which the NCSC – and other cyber defenders – would like to be able to answer in a timely, consistent, and accurate manner.

Prior to purchase:

- Do you have evidence that this product is secure by design and secure by default?
- How long will the product be supported for?
- Will it be updated automatically?
- Will all the components also be updated automatically?
- More generally, what is the burden of secure operation, and who has to shoulder that burden?
- Does it need to be rebooted/ reflashed to install updates?
- What information (telemetry) could be collected by the manufacturer? What level of security monitoring is provided in return?
- How easily can a device recover from a given exploit? Can recovery be completed remotely?
- How are vulnerabilities in the product managed? Is there an audited record of decisions made on how/if to fix particular issues?
- Is there a product/ support roadmap?

During operation:

- What is the most recent version available?
- How will I know a new update/ version is available? How will I know it has been successfully installed?
- How can I easily and remotely get the version information / asset management information?
- Is the product exposed to vulnerability XYZ, and if so what should I do about it?
- How can I check the integrity of the product?
- Do I need to replace the product?
- Is the product internet-facing? Does it need to be?
- How is the product configured and is this as expected?
- What software version is loaded?

Organisations that make it simple to answer these questions could be described as being 'radically

transparent.' Most of these questions should not be difficult to answer, in theory. *In practice*, however, they may involve manual processes and spreadsheets, or tracing queries through a product's supply chain.

All of which are likely to be time consuming. A complex system comprising many products, services and third parties adds further layers of complexity.

> **'Radical transparency allows vendors with sound practices to demonstrate their commitment to cyber security more convincingly.'**

Improving and automating the process of asking these questions (and getting answers to them) has many benefits. Data collected becomes more accurate, and up to date (potentially even near real time). Suppliers have clarity in terms of what information they have to provide and when. Information can be shared appropriately (for example, one can confidently ask if a given product is up to date without having to personally check each sub-component, or revealing potentially sensitive product details).

In the longer term, radical transparency allows vendors with sound practices to demonstrate their commitment to cyber security more convincingly. This information is not just of value to individual customers, but could also inform longer term decisions by potential investors.

Transparency is also required in hardware, which is increasingly complex and comes with many of the same considerations that apply to software. In contemporary semiconductors there may be intellectual property from many organisations present in a single chip, each with distinct security considerations.

Creating standards to formalise the above would ensure clarity on vendor responsibilities at each stage of the supply chain. System owners could more rapidly aggregate consistent data and use it to inform operational decisions.

Our approach should be to keep initial queries relatively simple, and concentrate on aggregating accurate and useful information at scale and at speed. It is important to be clear about vendor responsibility to provide this information; it will need to be propagated via the contractual relationships that underpin all stages of the supply chain.

Getting this right will mean that information will be available when needed, but not aggregated unnecessarily. It will be important for vendors to demonstrate ability (and commitment) to providing timely information. We will then be taking steps towards greater confidence in the ability of our digital ecosystem to provide the resilience society requires.

Open your eyes to the imminent risk to your economic security.

Cyber attacks are designed to disrupt society with real human costs.

Take cyber security seriously or risk exposing your customers' data.

National Cyber Security Centre
a part of GCHQ

Designed and produced by Big+Bold

Follow us

@NCSC

@cyberhq

National Cyber Security Centre