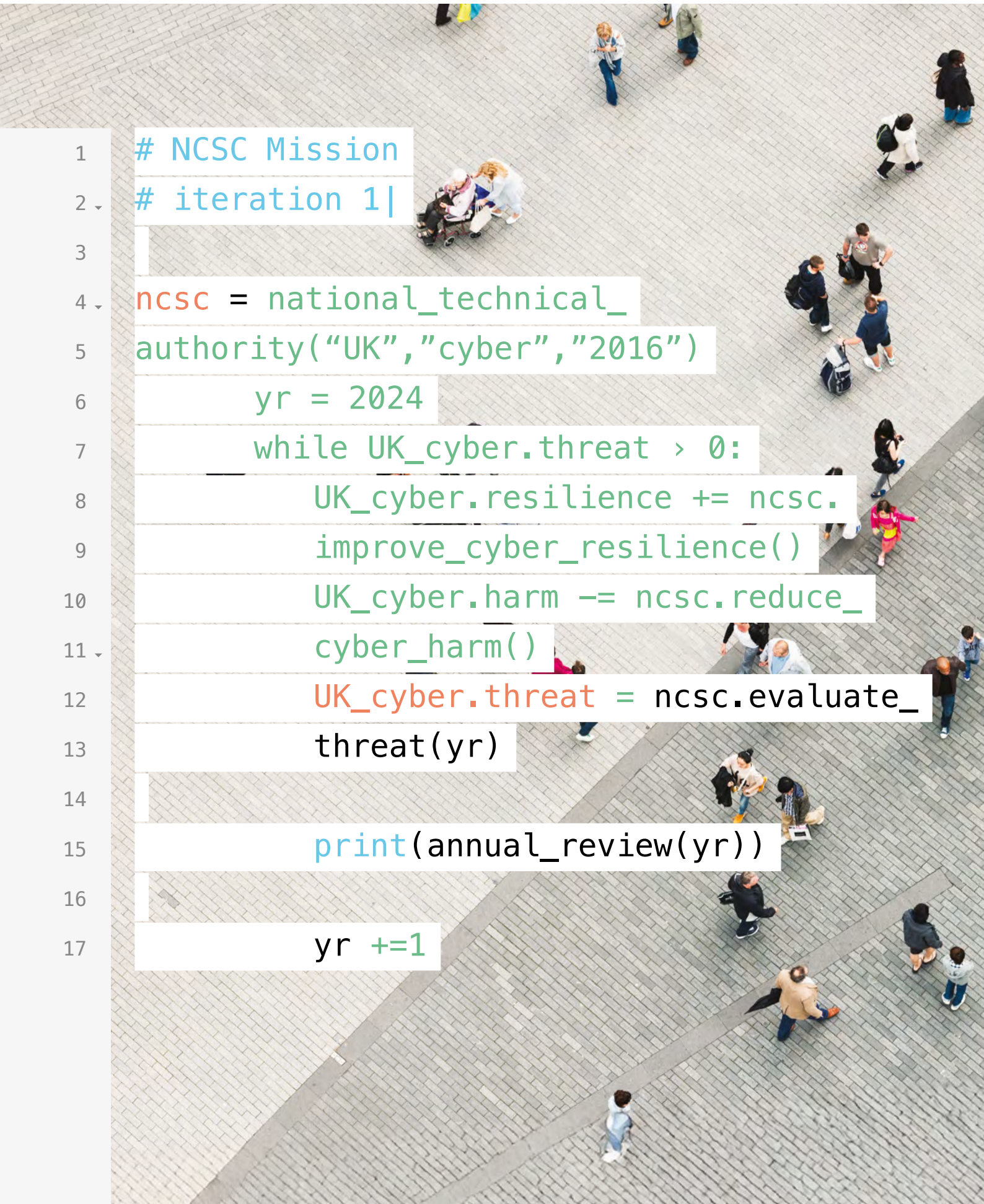
National Cyber Security Centre
a part of GCHQ

Annual Review 2024



```
contents = {

# Overview:
            Ministerial foreword = 02
            Director GCHQ foreword = 04
            NCSC CEO foreword = 06
            Timeline = 08
            The NCSC at a glance = 12
            The NCSC, working with... = 14

# Chapter 01:
            Countering the cyber threat = 16
            Staying in the race: keeping up with
            increasingly complex cyber attacks = 24

# Chapter 02:
            Building the UK’s cyber resilience = 28
            Realising a more secure and
            prosperous cyber future = 42

# Chapter 03:
            Developing the UK’s cyber ecosystem = 46
            Market incentives and the future
            of technology security = 54

# Chapter 04:
            Keeping pace with evolving
            technology = 58
            Post-quantum cryptography = 69
}
```

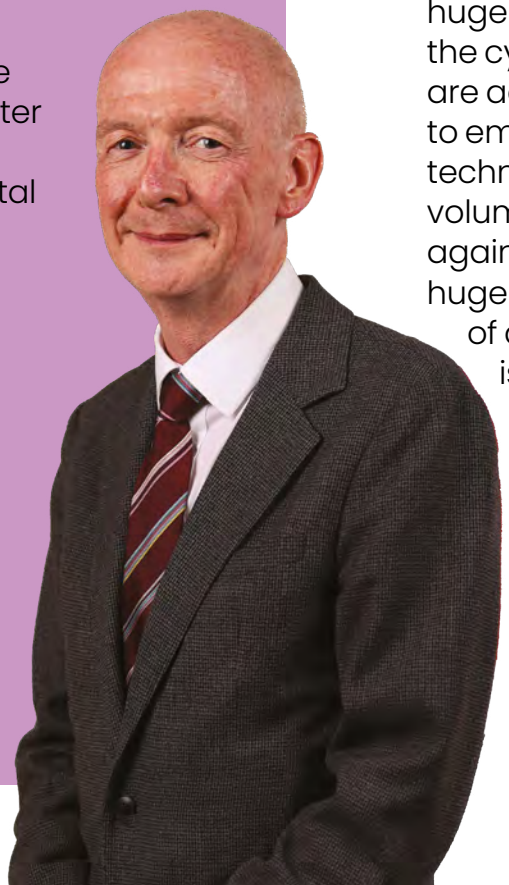
Ministerial foreword:

```
# Define the
message
message =
“Start here”
```

Cyber now underpins every aspect of everyday life. It is central to our economy and society, offering huge potential for the Government’s number one mission for growth and prosperity. But alongside its huge benefits there are also risks and vulnerabilities, making it more important than ever that we secure our online world.

The UK has a world-class reputation in cyber, and we are determined to stay one step ahead - remaining alive to the threats for the UK while embracing the benefits of the digital future.

The Rt Hon Pat McFadden MP
Chancellor of the Duchy of Lancaster and Minister for Intergovernmental Relations



The Government has taken a number of steps to strengthen our national security in the cyber realm, but we can’t do it alone. We need businesses and other organisations to boost their own cybersecurity where they can. While we have made significant progress, this report shows that the cyber threat is dynamic and grows more complex each year.

As this report shows, while AI presents huge opportunities, it is also transforming the cyber threat. Cyber criminals are adapting their business models to embrace this rapidly developing technology - using AI to increase the volume and impact of cyber attacks against citizens and businesses, at a huge cost. Meanwhile the proliferation of advanced cyber intrusion tools is lowering the barrier for entry to criminals and states alike.

We need to combat these threats and increase our overall resilience. One key way of doing this is by driving up the adoption of our "Cyber Essentials" scheme; stats show those businesses who implement Cyber Essentials are 92% less likely to make a claim on their cyber insurance. We are also working closely with businesses and industry through the National Cyber Security Centre and the National Protective Security Authority to offer practical ways that organisations can strengthen their own security and help defend the nation from cyber attacks.

Developing international partnerships is a priority and the Government is strengthening relationships with countries around the world. You'll see in this report how NCSC and UK law enforcement are working with partners internationally to counter the threat from cybercrime. We are also disrupting malicious cyber actors emanating from hostile states. In October, we sanctioned 16 members of the prolific Russian cyber-crime gang Evil Corp, delivered in coordination with the US and Australia.

We know we cannot keep pace with the threat or seize opportunities without a skilled and professionalised workforce that represents the breadth of talent across the UK. The NCSC has significantly contributed to increasing diversity, especially through the CyberFirst Girls Competition. But there is much more to do - including by increasing interest in the computing curriculum and plugging the cyber skills gap.

As ever with cyber, new challenges will arise as the threat continues to evolve. The UK has a world-class reputation in cyber, and we are determined to stay one step ahead - remaining alive to the threats for the UK while embracing the benefits of the digital future.

The Rt Hon Pat McFadden MP
Chancellor of the Duchy of Lancaster and Minister for Intergovernmental Relations

Director GCHQ foreword:

As Director GCHQ, I have the privilege of leading an organisation that is integral to our nation's security. In this review, you will read many examples of the real-world impact our work has had over the past 12 months.

```
# Define the
message
message =
"Start here"
```

> **"The ransomware attack on Synnovis, and the impact this had on thousands of procedures and appointments across six NHS trusts, illustrates why – in our increasingly interconnected world – we must remain ahead of the threat."**

Anne Keast-Butler
Director GCHQ

The world is growing more complex, more unstable and more unpredictable. We have seen persistent aggression from Russia as it continues to wage its unjust war against Ukraine. Ongoing tensions in the Middle East are a stark reminder of the volatility across the globe, and the ever-present risk for miscalculation. And while much of this conflict is playing out on the frontlines, there's been an increase in cyber operations against Ukraine and its allies in support of Russia's military campaign and its wider geopolitical objectives.

Meanwhile the pace and scale of technological change shows no sign of slowing down. In everything from AI to quantum computing, there are both opportunities and challenges. New technologies transform and improve our lives, but they can also be used by malicious actors to carry out more effective cyber attacks. We must prepare for a future where these capabilities are an integral part of life and also become part of how we continue to keep the country safe.

Against this backdrop, this year's report describes numerous examples of how the NCSC's work has helped to keep the country safe. The ransomware attack on Synnovis, and the impact this had on thousands of procedures and appointments across six NHS trusts, illustrates why – in our increasingly interconnected world – we must remain ahead of the threat.

The general election this summer was another significant moment for the UK's cyber resilience. The security of the election was front and centre, and I'm proud of the NCSC's contribution to the government's Election Cell, which brought together experts from the security and intelligence agencies to ensure the integrity of both the campaign and the election results.

I've experienced first-hand the importance and impact of international collaboration, working with allies to keep us safe across cyberspace and in the real world. And at CYBERUK earlier this year in Birmingham, I saw the UK cyber community come together in a thought-provoking and energising conference. We will be heading to Manchester for CYBERUK 2025, and I'm looking forward to welcoming the brightest minds from across government, industry, academia and the intelligence community.

GCHQ's wider skills and intelligence informs our NCSC-led cyber security mission, and vice versa. The mission 'making the UK the safest place to live and work online' applies not only to the NCSC, but to the whole organisation. There is huge power and potential in greater partnership, and I ask you to join us on the journey, in making this mission a reality day to day.

Anne Keast-Butler
Director GCHQ

NCSC CEO foreword:

It is with huge pride that I present the National Cyber Security Centre's eighth Annual Review, and the first in my role as CEO.

```
# Define the
message
message =
"Start here"
```

> **We face enduring threats from hostile states and cyber criminals looking to exploit our dependency on the technology that now underpins all aspects of modern life."**

Richard Horne
CEO NCSC

In the few short months since I joined the organisation, I have been astounded by the breadth and depth of expertise and creativity within the NCSC. I am similarly struck by the magnitude of the challenge ahead, as we strive to 'make the UK the safest place to live and work online'. That was the NCSC's founding mission eight years ago, and it remains the same today. But we should be under no illusion that the challenge is getting harder.

We now find ourselves in a contest for cyberspace.

We are all using digital technology to our benefit: to drive growth, drive innovation, drive productivity, drive better public services, drive prosperity. However, we face enduring threats from hostile states and cyber criminals looking to exploit our dependency on the technology that now underpins all aspects of modern life. From ransomware attacks to AI-enabled intrusion, malicious actors are looking to maximise their disruptive and destructive efforts in an increasingly connected world.

In recent years, the NCSC has produced world-leading cyber security guidance and frameworks, such as our Guidelines for secure AI system development. Cyber Essentials and the Cyber Assessment Framework (CAF). The reality is, not enough organisations are **implementing** our guidance, nor **applying** these frameworks.

We have a responsibility to ensure that the whole of the UK rises to the challenge. We will encourage businesses across the UK to use the NCSC's frameworks and guidance to drive up our national defences at scale. We will also help organisations of all sizes to be better prepared so they can quickly recover when cyber attacks do get through.

We will work with our partners across government to explore how we can influence the technology market to adopt more secure behaviours, which may include new legislation (such as the Cyber Security and Resilience Bill) and regulation to drive through the step change we believe is required to keep the UK safe.

Everyone has a role to play when it comes to improving cyber security. Whether you are working for the UK's critical infrastructure ensuring that the lights stay on, or a parent unboxing and setting up your child's tablet, we can all contribute to our national online resilience.

Since its inception, the NCSC has maintained that the UK's collective cyber resilience depends upon everyone – from individuals and families to SMEs and large enterprises – playing their part. This starts by acknowledging the scale of the challenges we face and identifying the urgent interventions that we need to implement now. Only then we can stay ahead of the cyber criminals and hostile states that seek to do us harm.

I'm aware that the important work of the NCSC can only happen with the support from our friends across government, industry, academia, and international partners for which we are so grateful. I look forward to meeting more of you in the coming months and in Manchester for CYBERUK 2025.

Richard Horne
CEO NCSC

Timeline:

2023

1 September

NCSC announces new CTO NCSC announces Ollie Whitehouse as new Chief Technology Officer

11 September

Evolution of Cyber Crime Publication of a white paper by the NCSC and NCA examining the rise of 'ransomware as a service' and extortion attacks

12 September

NCSC and ICO sign Memorandum of Understanding Memorandum sets out how both organisations will cooperate in the future

28 September

UK and US host international dialogue NCSC CEO and CISA Director lead talks with international partners to boost the cyber resilience of global democracies

11 October

Principles for ransomware-resistant cloud backups NCSC publish best practice to ensure cloud backups are more resistant to ransomware

12 October

Supply chain guidance published A new collection of resources for understanding the impact of supply chain cyber security risks

18 October

NCSC at Singapore Cyber Week NCSC CEO delivers speech on 'Reshaping cyber security in the era of generative AI'

23 October

Cisco advisory published Organisations are encouraged to take action to mitigate vulnerabilities affecting Cisco IOS XE

26 October

PDNS for schools launched The first phase rollout of a protective DNS (PDNS) service for schools

27 October

Logging Made Easy (LME) with CISA LME relaunched by the Cybersecurity and Infrastructure Security Agency (CISA)

28 October

British Library cyber attack: Major ransomware attack compromises most of its online systems

1-2 November

AI Safety Summit, Bletchley Park: NCSC support first ever global AI safety summit

9 November

Black Friday Cyber Aware campaign launched: Aimed at helping shoppers protect themselves online in the run up to the festive period

23 November

DPRK advisory: UK and Republic of Korea issue warning about DPRK state-linked cyber actors attacking software supply chains

27 November

Guidelines for secure AI system development: NCSC publishes first global guidelines to ensure the secure development of AI technology

30 November

Unitronics statement: NCSC publish mitigation advice following exploitation of Unitronics programmable logic controllers

5 December

Launch of Cyber Incident Exercising scheme: Providing organisations with access to NCSC assured CIE service providers able to create bespoke, structured cyber incident exercises

7 December

Star Blizzard advisory: Joint advisory to raise awareness of the spear-phishing techniques Russian FSB cyber actor Star Blizzard are using to target individuals and organisations

7 December

Defending Democracy guidance: A collection of guidance published to help counter the cyber threat

15 December

Culture sector summit: NCSC and DCMS met with representatives from the UK cultural sector to discuss what can be done to protect institutions' digital collections

2024

11 January

Ivanti advisory: Advising organisations to take immediate action to mitigate vulnerabilities affecting Ivanti Connect Secure

24 January

Cyber Threat Assessment: How AI will impact the efficacy of cyber operations and the implications for the cyber threat over the next two years

6 February

Pall Mall Process: UK and France host conference on proliferation and irresponsible use of commercial cyber intrusion capabilities and sign the Pall Mall Process declaration.

7 February

Living off the land advisory: A joint advisory and guidance warning CNI operators about the threat from cyber attackers using sophisticated techniques to camouflage their activity on a victims' network

20 February

LockBit statement: NCSC statement on law enforcement's disruption of LockBit ransomware operation

26 February

Five Eyes joint SVR advisory: Revealing evolving tactics used by Russian state-linked cyber actors as more organisations move to cloud-based infrastructure

1 March

Vulnerability Researchers event: NCSC Challenge Coins presented to researchers who have contributed to vulnerability disclosure programmes across government

2024 continued

4 March

***CyberFirst Girls Competition awards ceremony*:** Winning teams from across the UK recognised for their success at an awards ceremony hosted at the University of Oxford's Robotics Institute

25 March

***APT31 advisory*:** UK calls out China state-affiliated actors for malicious cyber targeting of UK democratic institutions and parliamentarians

17 April

***PDNS partner announced*:** A three year contract was awarded to Cloudflare Inc.

18 April

***NCSC podcast live*:** NCSC Cyber Series went live with a total of 5 episodes

19 April

***NCSC announces new CEO*:** Richard Horne appointed as new CEO of NCSC and GCHQ Board Member

22 April

***Palo Alto Advisory*:** NCSC encourage organisations to take immediate action to mitigate a vulnerability affecting Palo Alto Global Protect Gateway

24 April

***CISCO advisory*:** The NCSC advises organisations to take immediate action to mitigate vulnerabilities affecting Cisco firewall platforms

2 May

***UK local and mayoral elections*:** NCSC worked with partners to ensure elections were resilient

6 May

***Director for National Resilience and Future Technology attends RSA Conference*:** Roundtable with CISA to discuss joint 'global guidelines for AI security'

3-15 May

***CYBERUK 2024*:** The UK government's flagship cyber security event convened over 2,000 cyber security leaders, professionals and international delegations in Birmingham

14 May

***Cyber insurance guidance*:** Joint guidance from the NCSC with ABI, BIBA, IAU to help organisations faced with ransomware demands minimise disruption and cost of an incident

14 May

***Share and Defend capability launched*:** A capability designed to enable protection to the UK public and businesses from cyber attacks and cyber-enabled fraud

15 May

***Launch of Personal Internet Protection service*:** The service provides an extra layer of security on personal devices for high-risk individuals

5 June

Cyber Essentials celebrates 10th anniversary

21 June

***Synnovis incident*:** NCSC working with Synnovis, NHS and law enforcement to fully investigate reports of sensitive data being published online following cyber attack

4 July

***UK General Election*:** NCSC work with partners to help deliver a safe and secure election

9 July

***APT40 advisory*:** Australian-led joint advisory exploring how China state-sponsored actors have evolved their techniques for launching cyber attacks

10 July

***Carolyn Ainsworth recognition*:** NCSC's Chief Engineer named as one of the top 50 women in engineering

19 July

***CrowdStrike outage*:** Following the global IT outage NCSC issued guidance and a warning of an increase in phishing

25 July

***DPRK advisory*:** Joint advisory exposing a global cyber espionage campaign carried out by attackers sponsored by the DPRK to further the regime's military and nuclear ambitions

2 August

***ACD 2.0 blog*:** Introducing ACD 2.0 and the principles that have been set

7 August

***NCSC CEO attendance at BlackHat, USA*:** NCSC CEO took part in CISA's panel focused on election security

12 August

***Building a nation-scale evidence base for cyber deception*:** The NCSC invited UK organisations to contribute evidence of cyber deception use cases and efficacy to support our long-term research goals

14 August

***Post-quantum cryptography blog*:** NIST published three algorithm standards: ML-KEM, ML-DSA, and SLH-DSA. The NCSC has updated its PQC white paper to reflect this milestone

The NCSC at a glance:

```
# Define the
message
message =
“Start here”
```

The population and vast majority of organisations in the UK are dependent on digital technology to live and work. Cyber security ensures individuals and businesses can operate effectively in our connected world, and is central to national resilience.

What is cyber security?

Cyber security is how individuals and organisations reduce the risk and impact of cyber attacks.

Its core function is to defend the services we rely on and the devices we use – both at home and at work – from disruption, theft or damage. It's also about preventing unauthorised access to the vast amounts of data and personal information stored online and on these devices.

Cyber security is important because most organisations in the UK are dependent, directly or indirectly, on digital technology to function. Cyber security ensures organisations, including the UK's critical national infrastructure, can operate effectively in our increasingly connected world, and that governments can continue to provide the essential services that citizens depend upon.

Crucially, good cyber security facilitates better cyber resilience; the ability of an individual or institution to protect itself from, respond to, and recover from a cyber attack, data breach or service outage. All of these can cause huge financial losses and reputational damage.

On an individual level, smartphones, internet of things (IoT) devices, computers and the internet are now such a fundamental part of modern life that it's difficult to imagine how we would cope without them. Cyber security can prevent cyber criminals from accessing our accounts and services, keep our devices secure, and help us to navigate our online lives, safely and with confidence.

What is the NCSC?

The National Cyber Security Centre (NCSC) was formed in 2016 by combining separate parts of government, MI5 and GCHQ, to create the UK's technical authority for cyber security. Our mission is to make the UK the safest place to live and work online.

The NCSC supports the most critical organisations in the UK, the wider public sector, industry, small and medium-sized organisations and the general public. We also work collaboratively with law enforcement organisations, the UK's intelligence and security agencies, the National Protective Security Authority (NPSA), international allies and government partners.

The NCSC reduces cyber risks to the UK by helping secure public and private sector networks, and reduces the cyber threat by seeking to understand and disrupt it. When incidents do occur, we provide effective incident response to minimise harm to the UK and help victims to recover.

We also coordinate activities across industry, government and academia to develop the UK's cyber security skills, technologies and capabilities.

Who is at risk?

Any organisation relying on digital technology, directly or through its supply chain, is at risk of a cyber incident. The majority of cyber attacks are untargeted and opportunistic in nature. As the high profile cyber attack on the British Library illustrates, criminals will exploit weaknesses in an organisation without any regard for the sector it operates in, its size, or who is impacted.

Who is behind cyber attacks?

Despite how they are frequently described in the media, most cyber breaches are not a result of 'complex and sophisticated attacks'. The vast majority of cyber attacks are still based upon well-known techniques exploiting commonly understood weaknesses. This means that organisations employing basic cyber security standards, such as Cyber Essentials, can successfully defend themselves from the most common online threats. Some cyber attacks are highly sophisticated, and these are usually conducted by hostile foreign states for espionage or wider state objectives.

The NCSC, working with...

National Partners
International Partners

The NCSC's collaborative efforts with these partners (not exhaustive) are crucial for enhancing the UK's cyber resilience and addressing the global nature of cyber threats.

National Partners

A. Government departments

- Home Office
- Cabinet Office
- Foreign, Commonwealth and Development Office
- Ministry of Defence
- Department for Science, Innovation and Technology

B. UK intelligence community

- Government Communications Headquarters (GCHQ)
- Secret Intelligence Service
- National Cyber Force (NCF)
- Security Service (MI5)
- National Protective Security Authority (NPSA)

C. Devolved administrations

- Northern Ireland Executive
- Scottish Government
- Welsh Government

D. Law enforcement

- National Crime Agency (NCA)
- Regional Organised Crime Units (ROCUs)
- Local police forces

E. Regulators

- Office of Gas and Electricity Markets (OFGEM)
- Health and Safety Executive (HSE)
- Civil Aviation Authority (CAA)
- Office of Communications (OFCOM)
- Information Commissioner's Office (ICO)
- Financial Conduct Authority (FCA)

F. Public sector

- National Health Service (NHS)
- Local government authorities
- Educational institutions

G. Industry

- Critical national infrastructure (CNI)
- Financial services
- Telecommunications
- Technology companies

H. Academia

- Universities and research institutions
- Academic Centres of Excellence in Cyber Security Research (ACE-CSRs)

I. Non-governmental organisations (NGOs)

- Think tanks and advocacy groups
- Charities

International Partners

A. Government agencies

- US Cybersecurity and Infrastructure Security Agency (CISA)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- European Union Agency for Cybersecurity (ENISA)
- National Security Agency (NSA)

B. International bilateral partners

C. International organisations

- NATO
- United Nations (UN)
- Organisation for Economic Co-operation and Development (OECD)

D. International certification bodies

E. Industry and private sector

- Global technology firms
- International financial institutions
- Multinational corporations

F. Law enforcement

- Europol
- INTERPOL
- Federal Bureau of Investigation(FBI)

```
# Chapter title
chapter_title =
  “Countering the cyber threat”
```

Chapter:

01

Introduction

We face real and enduring threats from hostile states and cyber criminals targeting our critical national infrastructure.

The NCSC continues to analyse and respond to the cyber threats facing the UK. From hostile states and commercial cyber proliferation, to ransomware and the challenges of AI-enabled intrusion, the NCSC leverages its technical expertise and unique position in government to counter conventional and unprecedented cyber threats, working alongside law enforcement and international partners.

Ransomware attacks continue to pose the most immediate and disruptive threat to our critical national infrastructure (CNI), with some state-linked cyber groups now targeting the industrial control systems that infrastructure relies on.

The NCSC's Incident Management team worked with the Information Commissioner's Office and the legal and insurance sectors to produce joint guidance on 'ransom discipline', which aims to reduce the number of ransomware payments being made by victims of cyber crime and has since been internationalised through the Counter Ransomware Initiative (CRI), with 40 members and 8 insurance bodies globally endorsing it. It's just one example of how we're partnering with government and private organisations to improve the UK's cyber resilience.

China

China continues to be a highly sophisticated and capable threat actor, targeting a wide range of sectors and institutions across the globe, including in the UK.

In February 2024, the NCSC and international partners co-signed an advisory on observed compromises of US CNI by 'Volt Typhoon', a China state-sponsored threat actor. The targeting of energy, transportation and water sectors could be laying the groundwork for future disruptive and destructive cyber attacks, and is a clear warning about China's intent to threaten essential networks.

In March 2024, the UK government and international allies called out China state-affiliated threat actors for targeting UK institutions that underpin our democracy. The NCSC assessed that:

- threat actor APT31 was almost certainly responsible for conducting online reconnaissance activity against UK parliamentarians' emails in 2021
- a separate threat actor was almost certainly responsible for the compromise of computer systems at the UK Electoral Commission between 2021 and 2022

The NCSC continues to work across government, and in partnership with international allies, industry and academic colleagues, to deter, degrade and detect the cyber threat posed by China.

Russia

Russia continues to act as a capable, motivated and irresponsible threat actor in cyberspace. Russian threat actors almost certainly intensified their cyber operations against Ukraine and its allies in support of their military campaign and wider geopolitical objectives.

Through its activities in Ukraine, Russia is inspiring non-state threat actors to carry out cyber attacks against western CNI. These threat actors are not subject to formal or overt state control, which makes their activities less predictable. However, this does not lessen the Russian state's responsibility for these ideologically-driven attacks. The NCSC continues to publicly expose Russian cyber activity, which makes it a more challenging environment for them to operate in.

Iran

Iran-based threat actors remain aggressive in cyberspace and continue to achieve their objectives through less sophisticated cyber techniques (including prolific use of spear-phishing), but also targeting industrial control systems. In August 2024, US government agencies issued an advisory highlighting ransomware attacks by Iran-based threat actors on organisations in the education, finance, healthcare, and defence sectors in the US and other countries.

Although much of Iran's cyber activity has likely been focused on the Israel/Hamas conflict throughout 2024, it is developing its cyber capabilities and is willing to target the UK to fulfil its disruptive and destructive objectives. 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 (also known as North Korea) continues to prioritise raising revenue to circumvent sanctions and intelligence collection in its cyber activity. 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. In July 2024, the NCSC co-signed an advisory on a group sponsored with the DPRK's overseas intelligence agency that has targeted defence, aerospace and nuclear entities globally.

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. 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.

```
# Define the
message
message =
“Start here”
```

Defending democracy

The UK general election in July 2024 presented an attractive target for a range of threat actors, due (in part) to the UK's membership of NATO, the G7 and our continued support for Ukraine. More generally, threats against UK officials and election candidates – particularly their personal devices and accounts – are seen as a softer target by adversaries, and were highlighted in public attributions that included APT31 and Russian FSB threat actors 'Star Blizzard'.

Ransomware

Ransomware remains one of the most pervasive cyber threats to UK organisations.

Ransomware is a type of malware which prevents organisations from accessing their systems or data, usually by encrypting files. More recently, threat actors are choosing not to encrypt systems and simply threatening to publish sensitive data, using the potential reputational and financial damage to leverage a ransom payment.

The nature of modern supply chains means that a ransomware attack on one organisation can have a significant impact on many others. In June 2024, the financially motivated ransomware attack on Synnovis, a pathology laboratory supplier to the NHS, had significant impact on citizens, delaying elective procedures and outpatient appointments.

The NCSC provides guidance to help reduce the risk of ransomware attacks (and how to recover if you've been infected), whilst our Cyber Incident Response scheme helps victims to identify trusted providers of commercial incident response services should the worst happen.

In addition:

- the NCSC's Cyber Essentials scheme has been proven to reduce an organisation's vulnerability to cyber attacks (including ransomware)
- the NCSC's Cyber Advisor scheme can provide cyber security consultancy tailored to small and medium-sized organisations

Disrupting global ransomware operators

The NCSC and the National Crime Agency (NCA) assessed that the cyber crime group LockBit was the leading global ransomware threat since the demise of the Conti ransomware strain in mid 2022. In 2024, the NCA, alongside international law enforcement partners, led activity against the LockBit group, including taking control of their infrastructure and naming the primary operator. The NCSC works with government, law enforcement and international partners to disrupt and impose costs on high harm cyber criminals with targeted sanctions. In October, the UK sanctioned 16 members of the Russian cyber-crime gang 'Evil Corp' alongside coordinated action taken by the US and Australia. The NCSC is also an active participant in the multilateral body, the Counter Ransomware Initiative.

Artificial intelligence

Many nation-state threat actors and cyber criminals are already using artificial intelligence (AI) to increase the volume and heighten the impact of cyber attacks. In January 2024, the NCSC released an assessment of the near-term impact of AI on the cyber threat, highlighting how it can be used for reconnaissance, social engineering and analysis of exfiltrated data.

Generative AI (that is, AI tools that can produce different types of content, including text, images and video) will make it harder for defenders to identify social engineering attacks without the development of new mitigations. At the same time, the shrinking time between the exploitation of certain unpatched software vulnerabilities and the release of security updates to patch systems, is already challenging network managers. AI is expected to further narrow this interval, as reconnaissance to identify vulnerable devices becomes more precise.

Highly capable state actors, in terms of both AI and cyber operations, will most likely be able to exploit the potential of AI to create more advanced cyber attacks. The NCSC continues to work closely with government, international, industry and academic partners to understand the impact on cyber threat to inform the UK's response.

Cyber proliferation

Over the next five years, expected increased demand for commercial cyber tools and services, coupled with a permissive operating environment in less-regulated regimes, will almost certainly result in an expansion of the global commercial cyber intrusion sector. The real-world effect of this will be an expanding range and number of victims to manage, with attacks coming from less-predictable types of threat actor. Many of these will have access to commodity cyber tools that require low skill to weaponise, and will be operating from countries with scant regard for international norms and regulations.

The Pall Mall Process declaration

In February 2024, the UK and France hosted the first, dedicated conference on tackling the threat from commercial cyber proliferation. It brought together a wide range of organisations and views – states, tech companies, civil society representatives, academia, cyber security, investors, researchers and private industry – to establish guiding principles for the legitimate development, facilitation, purchase, and use of commercially available cyber intrusion capabilities.

The result was the signing of the Pall Mall Process declaration; a new international initiative across governments, industry and civil society to address the proliferation and irresponsible use of commercial cyber intrusion tools and services, providing consensus on what constitutes responsible behaviour in cyberspace. The NCSC supported the Foreign, Commonwealth and Development Office (FCDO) led initiative through robust assessment of the threat, technical expertise, engaging closely with industry, civil society groups and think tanks.

```
# Define the
message
message =
“Start here”
```

Incident management

The NCSC’s Incident Management (IM) team responds to serious cyber incidents impacting UK organisations. The IM team is responsible for triaging incidents, providing support to impacted organisations, and coordinating the NCSC and cross-government response.

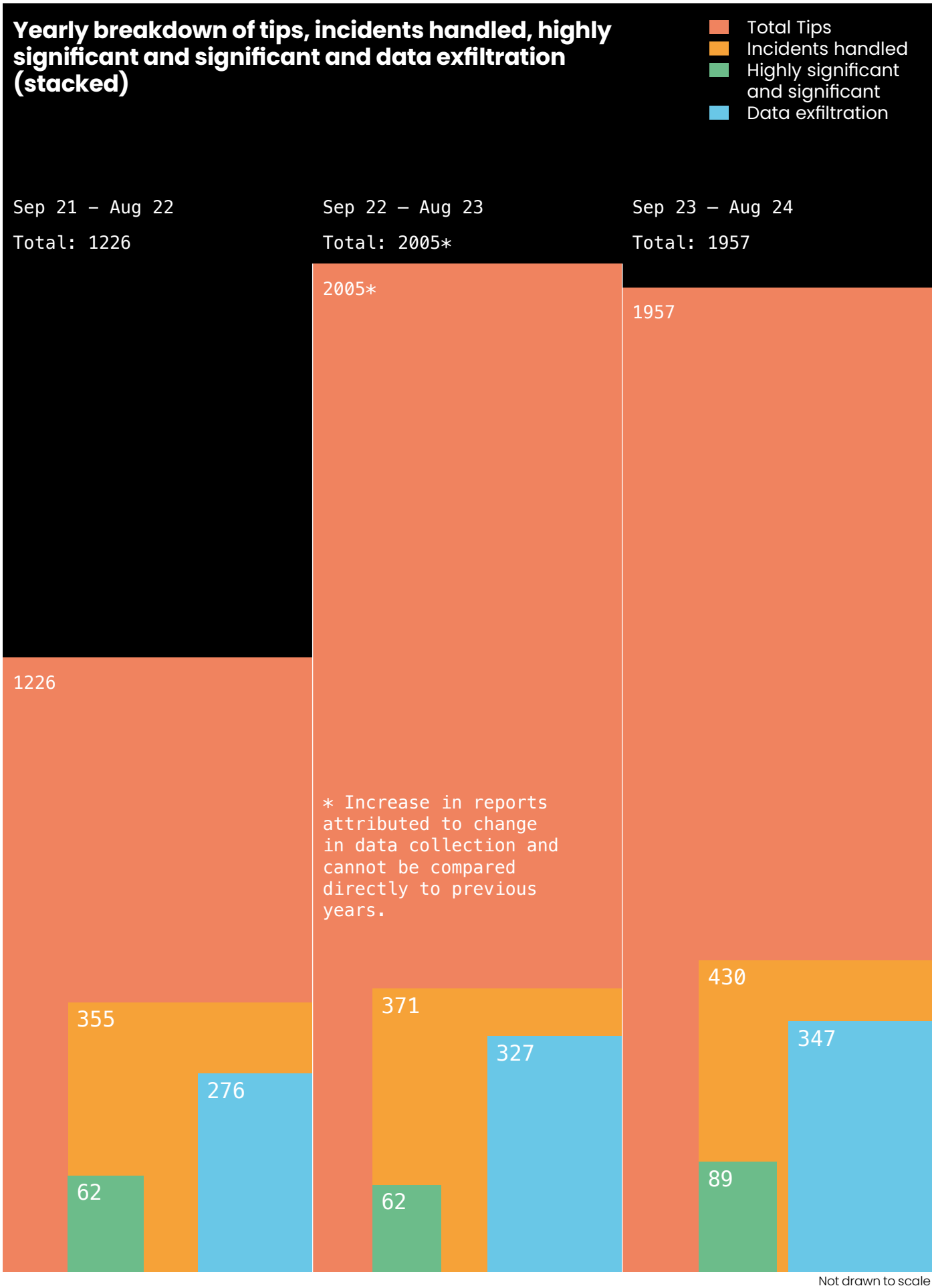
This year the IM team received 1,957 reports of cyber attacks covering a range of sectors. These were triaged into 430 incidents requiring support from the IM team, an increase on the 371 last year. Of these incidents, 89 were nationally significant, 12 of which were at the top end of the scale and more severe in nature (which is a three-fold increase on last year).

The IM team issued 542 bespoke notifications informing organisations to a cyber incident impacting them and providing advice and guidance on how to mitigate it. This was more than double the 258 bespoke notifications issued last year. Almost half of the bespoke notifications sent this year related to pre-ransomware activity, enabling organisations to detect and remove precursor malware before ransomware was deployed.

The top sectors reporting ransomware activity into the NCSC this year were academia, manufacturing, IT, legal, charities and construction. We received 317 reports of ransomware activity, either directly from impacted organisations, or from our partners (an increase on 297 last year). These were triaged into 20 NCSC-managed incidents, of which 13 were nationally significant. These included high-profile incidents impacting the British Library and NHS trusts.

Commercial and sensitive data continues to be attractive to threat actors, hoping to extort victims or use the data for other criminal or espionage activities. This year, the NCSC was made aware of 347 reports of activity that involved the exfiltration/ extortion of data.

Vulnerabilities continue to pose a cyber security risk to organisations. This includes known vulnerabilities, for which a mitigation exists, and newly discovered/zero-day vulnerabilities. Over the last year, the IM team issued approximately 12,000 alerts about vulnerable services through its Early Warning service (a free, automated NCSC threat notification service). Exploitation of zero-days CVE-2023-20198 (Cisco IOS XE) and CVE-2024-3400 (Palo Alto Networks PAN OS) also resulted in six nationally significant incidents for the IM team to manage.


Yearly breakdown of tips, incidents handled, highly significant and significant and data exfiltration (stacked)
Total Tips
Incidents handled
Highly significant and significant
Data exfiltration
Sep 21 – Aug 22
Total: 1226
Sep 22 – Aug 23
Total: 2005*
Sep 23 – Aug 24
Total: 1957
1226
355
62
276
2005*
371
62
327
1957
430
89
347
* Increase in reports attributed to change in data collection and cannot be compared directly to previous years.
Not drawn to scale

Staying in the race: keeping up with increasingly complex cyber attacks

Organisations must step-up their cyber resilience to protect the UK's economic wellbeing and critical national infrastructure.

```
# Define the
message
message =
“Start here”
```

Every year, the cyber threat landscape grows more complex. In 2024 it is best characterised as 'diffuse and dangerous'. We face a spectrum of threats where persistent activity by capable hostile states compounds the acute challenges posed by organised crime.

The number of cyber incidents is increasing, as is the impact of those incidents. Ransomware attacks, network intrusions, cyber espionage and theft of intellectual property are all commonplace. These have significant consequences for our economic and national security, as well as personal and professional costs for individuals.

Our collective ability to defend against cyber attacks – and to be resilient enough to remain operational when attacks do get through – has not kept up with the threat. The strategic advantage that network defenders have historically enjoyed in cyberspace is diminishing. The UK's national cyber resilience is under pressure, and organisations should take the necessary measures needed to defend themselves.

The NCSC believe that the severity of the risk facing the UK is – widely – underestimated by organisations from all sectors. Basic cyber security practices need to be implemented right across the country. Mass adoption of these measures remains the best way to defend, respond, and recover. But it must happen now.

Advances in cyber intrusion technologies

Ransomware continues to be the most significant, serious and organised cyber crime threat faced by the UK, with global ransomware payments in 2023 topping $1 billion. Critically, the cyber criminals behind ransomware continue to mostly operate from foreign jurisdictions that refuse to take action against them, providing a permissive and enabling environment for these groups.

The commercial proliferation of advanced cyber intrusion tools against an increasing range of devices will almost certainly be transformational in the years ahead. There is now a global, skilled, commercial cyber intrusion sector. This proliferation of cyber tools, combined with advances in technology, is lowering the barriers to entry and putting sophisticated tradecraft in the hands of a far wider range of relatively unskilled actors. This enables actors to access cost-effective capabilities and intelligence that would otherwise take decades to develop. It will no longer just be states buying a few high-end, off-the-shelf products; by 2030, a cyber intrusion ecosystem will be available, putting surveillance, espionage, and possibly even effects capabilities into the hands of new actors.

This hugely increases the scale and scope of global threat actors, and with it the number of attacks to defend against (and risks to mitigate). The diffusion of previously high-end tradecraft is also making it harder for defenders to establish with a high level of certainty who might be behind attacks. All this is happening against a backdrop of an expanding attack surface, where opportunities for bad actors increase at scale as our dependence on technology grows, our supply chains become more complex, and more services and data move to the cloud.

The complexity of the threat landscape is also almost certain to intensify with the use of AI technology. States that can develop an advanced sovereign AI capability will pose a cyber threat of real scale and sophistication. Publicly available models will continue to make all types of threat actor more efficient and effective, exacerbating the challenges of defence and response. AI will also almost certainly enhance actors' abilities to extract intelligence value out of exfiltrated data. And so, as more data is stolen and systems are compromised, state and non-state proxy actors use this stolen data to generate information campaigns in support of their wider competitive goals.

Geopolitics as a driver of cyber threat

On top of a more complex picture of actors, the overall cyber threat is amplified by geopolitical risks from global conflicts. Through the last year, we have repeatedly seen heightened use of cyber activity in areas of wider competing influence around conflict zones. In direct conflict, Russia has routinely deployed wiper malware to delete data from inside Ukrainian government and critical national infrastructure to hinder their operation. Additionally, Russia is routinely seeking to compromise the systems of NATO states and aiming to shape the information space globally around Ukraine as it erroneously sees itself in conflict with NATO.

Autocratic nation states continue to pose a fundamental and persistent threat to the UK by using advanced cyber capability against our most critical sectors, seeking to undermine our society. Highly sophisticated tools, techniques and procedures, including use of covert networks, helps to obfuscate the activity of these states, increasing the overall impact of their activities and making it harder to attribute attacks.

The operating environment inside a country can itself be an enabler to state cyber activity. An advanced ecosystem of cyber criminals, hacktivists, data brokers, access brokers and cyber intrusion companies now enables access to data and systems across the globe which can support and benefit nation state aims. While these groups are not always subject to formal or overt state control, this does not lessen states' responsibilities for their actions.

China remains a highly sophisticated cyber actor, with increasing ambition to project its influence beyond its borders through both cyber and information operations. China state-affiliated actors have routinely sought to gain access to networks across the world that enable their collection of bulk data and follow-on compromises. This includes actively targeting a wide range of networks for espionage, and prepositioning on critical national infrastructure for future disruptive and destructive purposes. Earlier this year, the US stated that China affiliated actors had compromised networks at multiple telecommunications companies to enable the theft of customer call records data revealing a broad and significant cyber espionage campaign.

Russia and Iran both engage in hostile cyber activity, not just to degrade, damage and compromise data and systems, but to

Felicity Oswald speaking at Blackhat USA Conference

support or trigger direct physical threat activity, broader espionage, and hybrid warfare activities. These regimes have also looked to encourage a new wave of state-aligned hacktivism. The NCSC has seen a stark increase in the focus on critical national infrastructure systems, as hacktivist groups strike to compromise these systems for political effect and propaganda victories. From the Cyber Army of Russia Reborn to the Islamic Hacking Army, these groups pose an active threat to poorly-defended critical systems far beyond their traditional activities of DDoS attacks, as evidenced by the US advisory in April 2024 on the hacktivist threat to US water facilities.

North Korea continues to use cyber operations for a range of activities, including the acquisition of digital assets and other operations which result in monetary benefit. This is done in a variety of ways, of which supply chain attacks are one.

The widening gap

There is a widening gap between the increasingly complex threats (outlined above) and our collective defensive capabilities in the UK, particularly around our critical national infrastructure.

That widening gap will only become more pronounced over time as the scale and capability of cyber actors proliferates, the relationship between state and non-state actors becomes more obfuscated, and states' abilities to understand cyber activity becomes fraught. It is therefore vital we increase our cyber resilience across the whole of the UK, and that we do so with urgency. Elsewhere in this review, we have outlined what organisations must do, and how they should do it. The NCSC stands ready to help.

```
# Chapter title
chapter_title =
    “Building the UK’s cyber resilience”
```

Chapter:

02

Introduction

```
# Define the message
message = "Start here"
```

From critical national infrastructure to emerging technology, cyber resilience underpins the UK's economic future and safety.

The speed at which new technologies – such as artificial intelligence – are being used to facilitate cyber attacks continues to rise, as does the volume and sophistication of cyber threats from a range of capable adversaries.

The NCSC is prioritising the cyber resilience of the UK's critical systems against the most advanced and sophisticated threats. At the same time, we're raising our national resilience to commodity cyber attacks across the whole of the UK's economy, using the unique insights we get from being a part of GCHQ, and by working with partners across government, industry, and academia.

More specifically, the NCSC is building UK cyber resilience by:

- delivering transformational active cyber defence services and interventions
- supporting legislative and regulatory reform
- growing the UK's cyber ecosystem
- influencing the security standards for new and emerging technologies

This year the NCSC, working with the Cabinet Office Election Cell and alongside policing, central and local government and private sector organisations, helped to deliver safe and secure elections. We worked with the NPSA to provide dedicated support and services to high-risk individuals and organisations targeted by nation-state actors wishing to disrupt the democratic process. The general election was delivered smoothly and securely. No major information operations, cyber or concurrent incidents that caused a notable impact on the election and its outcome were observed.

Securing government

The NCSC has continued to strengthen cyber resilience across government, by supporting the establishment of the Government Cyber Coordination Centre (GC3) in September 2023. GC3 is a joint venture between the Government Security Group, the Central Digital and Data Office and the NCSC. It is the coordination point for operational cyber security efforts across the government sector relating to vulnerabilities, threats and incidents, enhancing government's resilience and ability to 'Defend as One', meaning that government cyber defence is far greater than the sum of its parts.

2024 also saw the first set of annual GovAssure returns from government departments, which provide an assessment of the cyber security of critical systems underpinning government's essential services. GovAssure is run by the Cabinet Office and uses the NCSC's Cyber Assessment Framework (CAF) as its assurance methodology.

The NCSC has piloted new approaches to collaborating with security researchers from across the public sector, and accessing operational cyber security event data, at scale. This included hosting a workshop with researchers from across the public sector

to conduct threat hunting across shared datasets, and to develop new tradecraft for detecting threats.

The NCSC is driving a transformational journey, moving away from traditional, anecdotal, incomplete and slow approaches to cyber resilience and instead embracing data-driven methods where insights inform our decisions and enable us to respond more effectively and more efficiently to emerging threats. By applying the standard data science toolkit to the cyber resilience problem, the NCSC will have better situational awareness, prioritisation and agility. This transformation will enable us to minimise harm by avoiding or mitigating more incidents faster.

The NCSC have developed joint cyber security priorities with the Ministry of Defence to increase the cyber resilience of our armed services. We have also been working with international partners to ensure the cyber security of joint projects to deliver the next generation of defence capabilities including the Global Combat Air Programme (GCAP) and AUKUS submarines.

Sector resilience

Over the last year, we have evolved our approach to the NCSC's sector-specific Trust Groups; industry-specific communities of Chief Information Security Officers (CISOs) in businesses and organisations. This has involved taking a more thematic approach to common risks and vulnerabilities such as supply chain resilience and the security of overseas travel.

Nearly 300 CISOs now actively participate in the NCSC's sector-specific Trust Groups. As of 31 August 2024, over 70% of the UK organisations that are Trust Group members had signed up to the NCSC's Early Warning service, which is designed to inform organisations of potential cyber attacks on their network.

We also provide bespoke support where required, including the creation of a suite of practical resources for schools which, this year, passed over half a million combined views on YouTube and downloads from our website. In addition, we also extended our 'Protective DNS' offering into the school sector, which helps to prevent malware, ransomware, phishing attacks, and other online threats from reaching school networks. This will mean more schools – regardless of their resources – can now benefit from enhanced cyber resilience.

```
# Define the message
message = "Start here"
```

Defending democracy

The integrity of the general election is fundamental to our democracy. Securing the election was a top priority for the NCSC. We played a part in the UK's Defending Democracy Taskforce, made up from representatives from across government, the UK Intelligence Community (UKIC) and the NPSA.

The taskforce's aim was to ensure protection of our democratic institutions, processes and civil society, which included a establishing the constructs for free and transparent elections in 2024. The Defending Democracy Taskforce then established the Joint Election Security Preparedness unit (JESP), which took overall responsibility for coordinating electoral security and drove the government's election preparedness. Looking beyond the election the NCSC will continue to support the Defending Democracy Taskforce's priorities.

Before the election, the NCSC helped secure digital infrastructure, working with devolved governments and the Ministry of Housing, Communities and Local Government to ensure local authorities were resilient. We extended Active Cyber Defence (ACD) services and offered expert advice to political parties and electoral management service providers.

Recognising that personal digital services (such as email) are seen as softer targets by our adversaries, the NCSC developed a comprehensive cyber offer for high-risk individuals including briefings and the development of innovative individual cyber defence services, which were made available to all parliamentary candidates. These services included 'Account Registration' (a service to provide rapid notifications if we become aware of a cyber incident affecting a registered account) and 'Personal Internet Protection' (a service which helps manage the risk of visiting malicious domains).

Post-election, the NCSC worked with parliamentary security and the Cabinet Office to deliver cyber security briefs and facilitated the adoption of individual cyber defence services.

The 2024 general election took place in a complex information environment. The NCSC partnered with colleagues across government to offer expert technical advice on how to protect against and respond to information-based incidents. This included using our expertise in exercising to test a number of scenarios and our collective readiness to respond to any incidents, as well as participating in JESP's Election Security Exercise Programme.

Defender Communities

In support of the 'Defend as One' objectives, the NCSC has piloted new approaches to engage and collaborate with security practitioners across the public sector. Successful projects like NHS England's Cyber Security Operations Centre (CSOC), Police Digital Service's National Management Centre (NMC), and CymruSOC (Security Operations Centre) have made expertise accessible to many organisations.

The NCSC's work with these communities has identified opportunities to support experts by tailoring analytic products and engagements for wide distribution. Regular engagements have facilitated the sharing of actionable intelligence, encouraging proactive defences and knowledge sharing. Over half of all actionable insights come from external contributors.

Threat hunting workshops have developed and shared tradecraft for detecting threats, enabling coordinated threat hunting on critical systems. The NCSC has invested in developing subject matter expertise and technical innovation, working closely with Five Eyes partners.

Research and innovation

In early 2024, the NCSC set up a new team dedicated to enhancing the resilience of the UK's research and innovation (R&I) sectors, in partnership with the NPSA. The work focuses on enhancing cyber resilience in critical emerging technologies including quantum, AI, engineering, biology and semiconductors. A new Emerging Technology Trust Group spans universities, incubators, spin-outs, funders, investors and larger tech companies. This provides us with direct, one-to-one engagement with the most significant and strategic R&I organisations, which helps us to:

- influence funders and investors in these critical sectors
- encourage them to incentivise or mandate cyber security best practice

The NCSC have also worked with the NPSA and published the 'Secure Innovation' guidance, which provides emerging technology companies with a set of cost-effective measures that they can use from day one to better protect their ideas, reputation and future success. The international launch of the Secure Innovation campaign highlights the join up across our 5 Eyes community.

Cyber Essentials

Cyber Essentials can help every organisation – from micro businesses to large corporations – guard against the most common cyber attacks whilst signalling to potential customers that they take the cyber threat seriously. The technical controls defined in the Cyber Essentials scheme continue to be the minimum standard of security that the NCSC advise all organisations strive for. In 2024, Cyber Essentials celebrated its tenth anniversary.

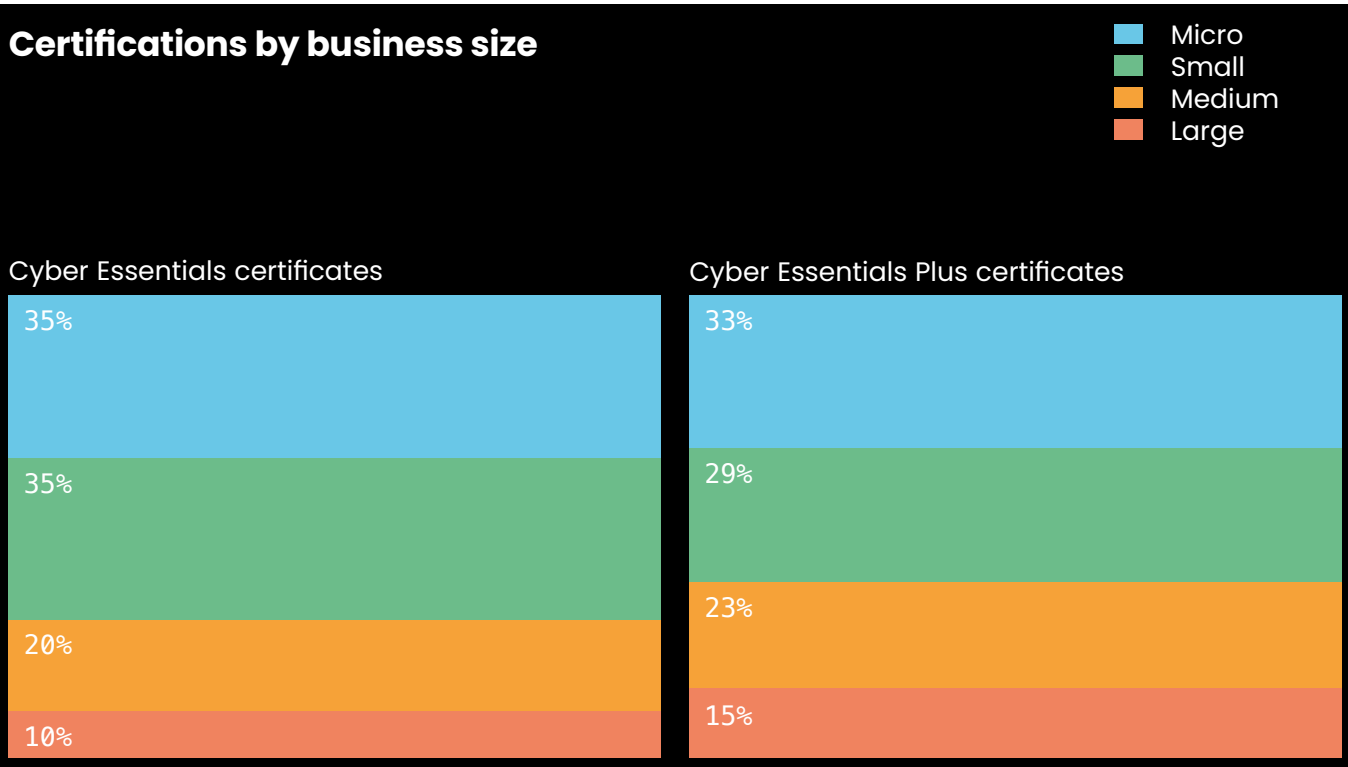
Research from insurers show that organisations implementing the Cyber Essentials controls are 92% less likely to make a claim on their cyber insurance than those which don't have Cyber Essentials. We've also launched the Cyber Essentials Knowledge Hub, to provide a central, up-to-date source of authoritative information, and it's already received great feedback from customers and certification bodies.

33,836
Cyber Essentials certificates awarded (+20%)

10,939
939 Cyber Essentials Plus certificates awarded (+20%)

358
Certification Bodies right across the UK (+12%)

Certifications by business size



Top 4 reasons given for certification

As recommended by users

- **91%** of customers would recertify to Cyber Essentials next year.
- **89%** would recommend certifying to other organisations like theirs.
- **40%** of smaller organisations implemented the controls for the first time.
- **2%** failure rate for Cyber Essentials; dropping for the third straight year.
- The estimated fail rate for Cyber Essentials across all organisation sizes has dropped from **2.45%** to **2.0%**.
- This year saw an increase (of 6%) in renewals of CE certifications **72%** compared to the previous year.
- Of sole traders, micro and small organisations, around **40%** told us it was the first time that they'd implemented the Cyber Essentials controls. This figure is an increase of **10%** on last year.
- The proportion of organisations that say they will recertify (**91%**) and those saying they would recommend the scheme (**89%**) have both increased.
- Achieving Cyber Essentials Plus compliance across their partnership network has helped St James Place reduce cyber security incidents by approximately **80%**.

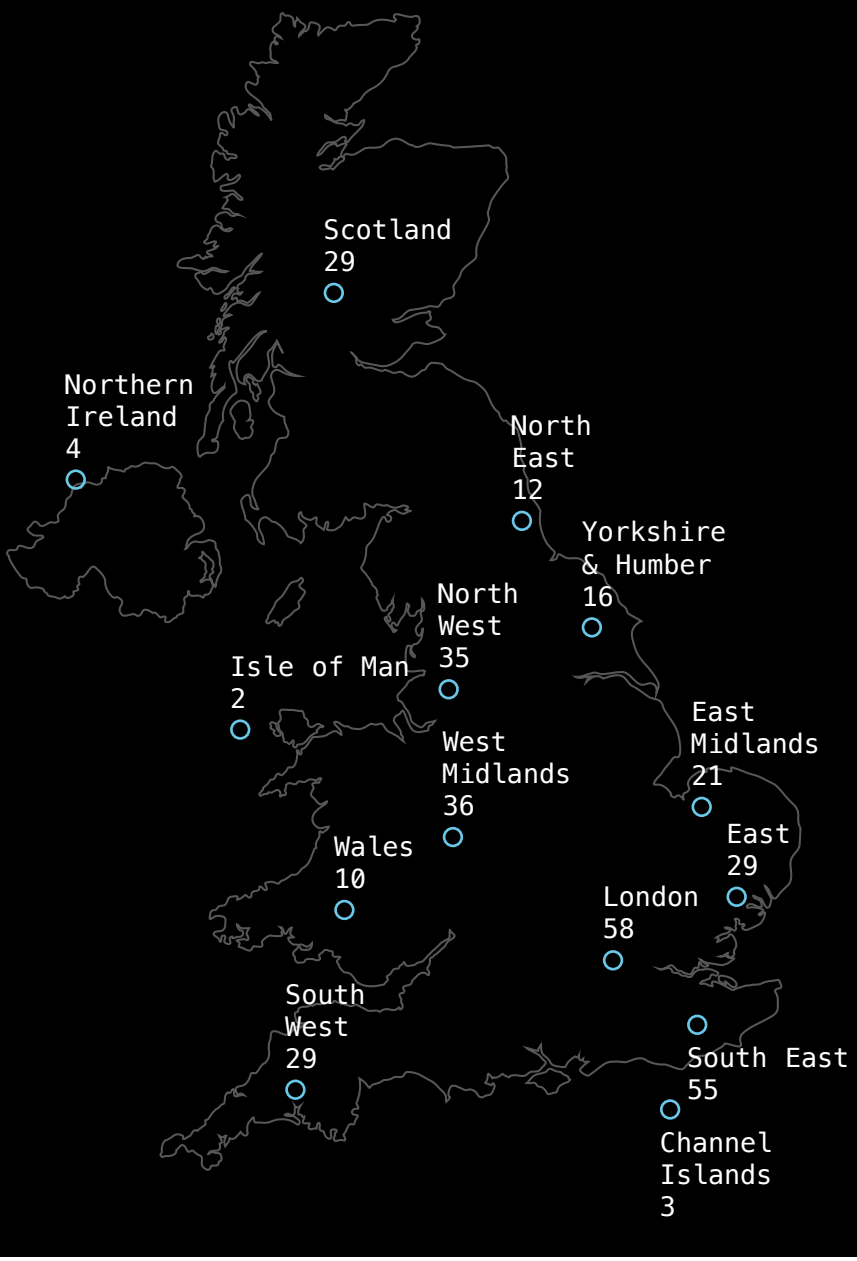
Growing the cyber ecosystem

Cyber Essentials is also fuelling growth across the wider cyber security sector. Through our Delivery Partner, IASME, we support the UK's cyber security industry by licensing the Cyber Essentials assessment process to 'Certification Bodies' across the UK. We now have 358 cyber security companies right across the UK (up 12% on last year), who are licenced to deliver Cyber Essentials.

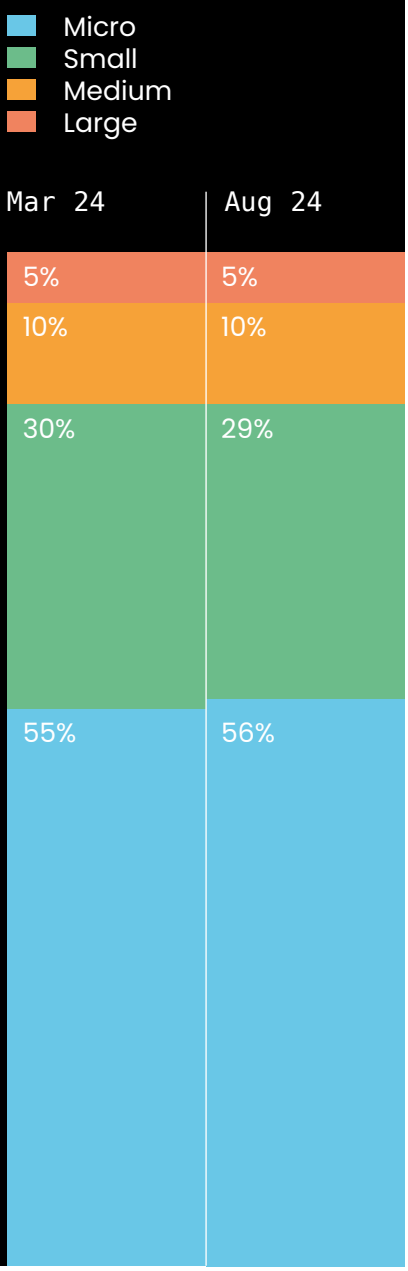
Cyber Essentials Plus

Cyber Essentials Plus offers a higher level of assurance of the standard Cyber Essentials scheme, as it includes a technical audit, carried out by an approved third party, to ensure the technical controls have been correctly implemented. This year, St James's Place, one of the UK's largest advice-led wealth management companies, asked its partnership network of over 2,800 independent business to certify to Cyber

Certification Bodies by region (March 24)



Certification Bodies by size



Essentials Plus. In such a large supply chain this had its challenges, but the decision is already showing a positive impact with an 80% reduction in cyber security incidents.

The Funded Cyber Essentials Programme

The NCSC has continued to deliver its three-year Funded Cyber Essentials Programme, by supporting small organisations that work in those sectors that are at greater risk of cyber attack than others. This may be because of sensitive information they deal with, or because they're seen as an 'easy target' for cyber criminals.

Since beginning the programme, 525 small organisations have benefitted from the opportunity to access free Cyber Essentials support. Initially targeting small organisations in the legal aid and charity sectors (that is, organisations handling sensitive data that would have significant impact if disrupted), we expanded in 2023 to the 'emerging technology' sector, widening our offering to small businesses working in AI, engineering biology, quantum engineering and semi-conductors.

Between September 23 and August 24, 204 applications were approved (29 charities, 99 legal aid and 76 emerging tech companies). Since its launch 90% of organisations responding to feedback feel more confident about cyber security after completing the process.

CyberFirst event

Cyber Advisor

The Cyber Advisor scheme provides small and medium-sized organisations with access to local, reliable and cost-effective cyber security advice and practical support, all based on the implementation of the Cyber Essentials technical controls. Every Cyber Advisor must work for a company which has met the NCSC's standards, and pass an independent assessment that measures their:

- knowledge and understanding of the Cyber Essentials' technical controls
- competence in providing practical, hands-on support
- ability to understand and work with small and medium-sized organisations

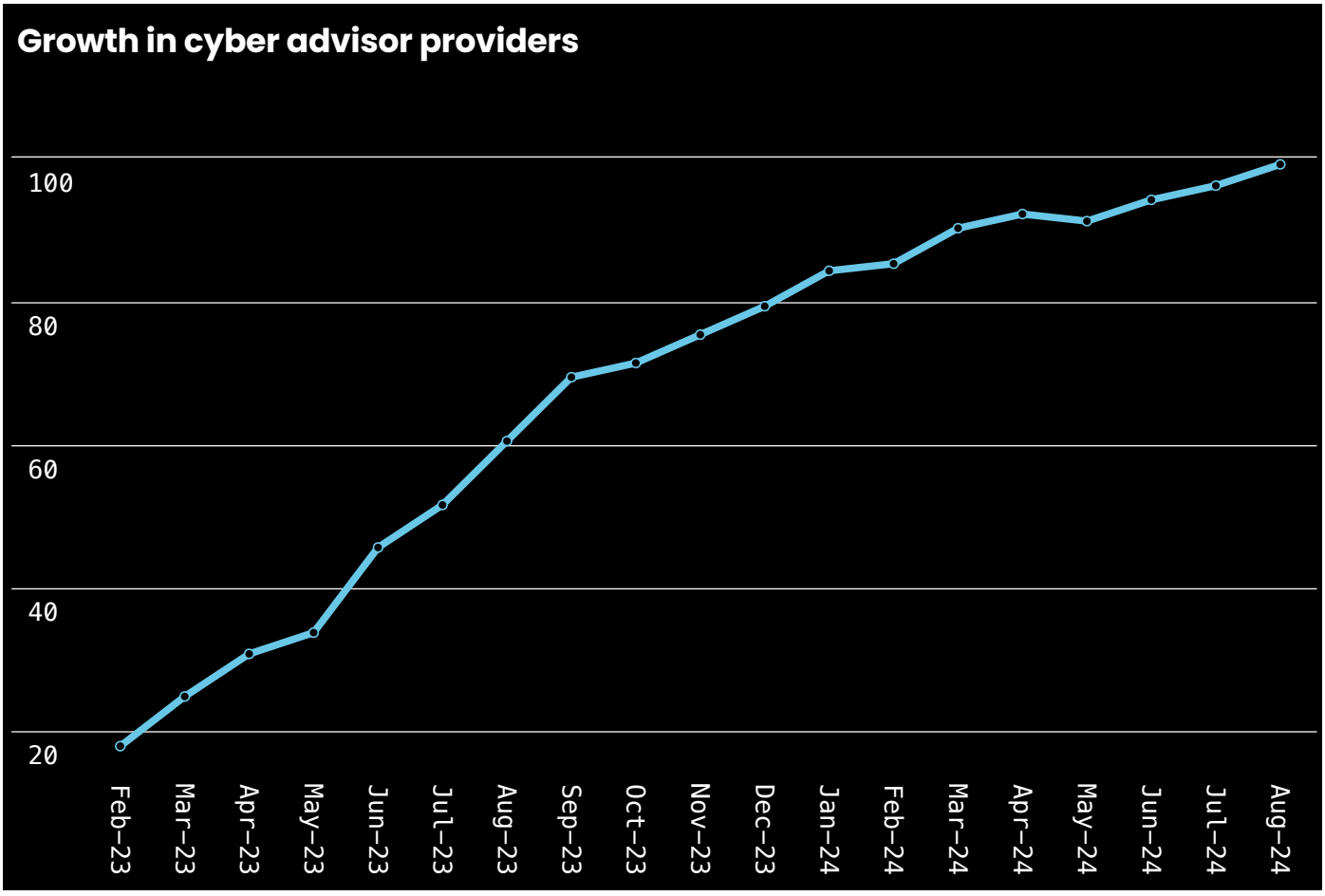
Launched in 2023, Cyber Advisor has continued to grow this year, with 100 individual Cyber Advisors now employed by 93 NCSC assured service providers.

Industry assurance

The NCSC, working with partners, offer certified assurance that covers a range of products, services and organisations. We continue to develop our range of industry assurance schemes and have launched new services to help grow the cyber security industry, leveraging the NCSC brand so consumers can choose products and services they can trust. This all means that more organisations than ever before can have confidence in the cyber security solutions they rely on to grow their businesses.

Cyber Resilience Audit

In August 2024 we announced the opening of a new Cyber Resilience Audit (CRA) scheme. CRA will assure providers who can conduct independent CAF-based audits. These audits are primarily delivered to government departments, the wider public



sector, and organisations operating in critical national infrastructure or specifically regulated sectors, although other organisations may also buy Cyber Resilience Audits for their own benefit.

Cyber Incident Exercising

Last year we made an effort to make our schemes more accessible to a wider range of organisations. This included the launch of a Cyber Incident Exercising (CIE) scheme. CIE allows organisations to test the effectiveness of their incident response plans in a safe environment and strengthen their incident management processes. CIE doesn't test cyber defences, but helps organisations to explore and evaluate their response plans, understand what risks they are holding from a cyber perspective, and how they can be managed. There are now 28 providers assured by the NCSC under CIE.

'Standard' Cyber Incident Response

As part of our aim to support a wider range and larger number of organisations, last year a new 'Standard' service level was introduced to our Cyber Incident Response (CIR) scheme. The requirements of the Standard level are designed to support target organisations which are at risk of common cyber attack, and are likely to include most private sector organisations, charities, local authorities and smaller public sector organisations. There are now 36 providers assured across the CIR scheme.

CHECK

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 53 companies assured, delivering CHECK penetration testing engagements. Over the past 12 months our assured service providers have carried out over 2,700 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. Meanwhile, CHECK has completed the first phase of a digital transformation programme, automating the management of the scheme and allowing service providers the ability to carry out many day-to-day business activities themselves, while fuelling the ability to further explore relevant datasets.

Cyber Resilience Test Facilities (CRTFs)

To further develop Principles Based Assurance (the NCSC's evidence-based method for technology assurance), initial work to establish Cyber Resilience Test Facilities (CRTFs) was completed, being the mechanisms that will deliver assurance for a wide range of internet-connected products using the Principles Based Assurance methodology. The objective is to set up a network of commercially operated CRTFs across the UK to assure these products at scale. Not only will this raise the bar for cyber-resilient product development, it will also widen the range of products being assured whilst driving private sector growth.

The CRTF pilots are now complete, with the results being analysed to determine what the future assurance model will look like ahead of a small-scale CRTF operating capability launch planned for 2025. Opportunities to scale the capability further will then be considered and implemented where feasible.

Active Cyber Defence

Active Cyber Defence (ACD) – a collection of NCSC services designed to protect UK citizens and organisations from commodity cyber attacks – continues to play an important role in building resilience. This year we announced ACD 2.0, which aims to build the next generation of ACD services in partnership with industry and academia.

As we embark on ACD 2.0, our first step is to look at our attack surface management suite (currently Web Check, Mail Check and Early Warning) and apply evidence-based scrutiny to our existing ACD services. This will ensure we have ongoing justification for the continuation of a service, along with a responsibility to evidence impact and be transparent about whole life costs, driving them down where possible. As a result, the NCSC will look to divest most of our new successful services within three years for the private sector to run on an enduring basis.

Share and Defend

Share and Defend is a new ACD service that shares feeds of known malicious domains with internet service providers (ISPs) and others so that they can be blocked or taken down, protecting UK citizens in near real time from high volume cyber crime and cyber-enabled fraud. The platform is already enabling the protection of approximately 50% of the UK public by sharing these known malicious domains with ISPs.

Share and Defend works with threat intelligence providers and security vendors to consume data sets which contain malicious indicators (such as domains and URLs). Share and Defend also uses data from the PDNS and Takedown services.

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.

>3,800

organisations are now using Mail Check

- Over **34,600** domains, **60%** of which are protected by DMARC

Web Check helps users find and fix common security vulnerabilities in their websites.

>64,000

assets subscribed

- Service now has over **4,000** organisations utilising Web Check

Check Your Cyber Security offers a range of tools to help users identify common vulnerabilities in their public-facing IT.

>33,000

IP checks completed in review period (82% increase on previous year)

- Over **7,300** IP vulnerabilities detected
- Over **25,800** browser checks completed in review period (76% increase on previous year)
- **30%** of checks detected an out-of-date browser

Suspicious Email Reporting Service (SERS) allows the public to report potential scam messages for removal.

>10.5m

reports received

- Total number of reports since April 2020 reached over **34.4 million**
- **351,000** scam URLs removed by the NCSC since April 2020

The Takedown service works with hosting providers to remove malicious sites and infrastructure from the internet.

2.2m (+22%)

cyber-enabled commodity campaigns removed (up from 1.8m last year)

- Share of global phishing has remained on average between **1–2%** throughout the last year. In 2016 the figure was over **5%**

Early Warning allows system owners to receive email alerts from the NCSC tailored to the cyber threats for their organisation's IP address.

181,180

vulnerable systems on the internet were notified

- Notified about malware infections on **117,700** IPs
- Notified about **47,739** hacked internet servers
- There were **11,190** organisations signed up at the end of the period, an increase of **29%** on the previous year

Realising a more secure and prosperous cyber future

```
# Define the
message
message =
"Start here"
```

The gap between the threat and the UK's ability to defend against it is growing. We can address this through immediate practical actions while developing long-term strategic measures to outpace our adversaries and secure the UK economy's growth.

The UK has one of the world's most advanced digital economies which relies on having a secure digital infrastructure. Our reliance on the technology that underpins much of society comes with a growing threat from nation states, cyber criminals and other malicious actors. Hostile activity in UK cyberspace has grown in frequency, sophistication and intensity.

The NCSC believes that the severity of the risk facing the UK is being widely underestimated, and that the cyber security of critical infrastructure, supply chains and the public sector must improve. There is a growing disparity between the resilience of our infrastructure and the threat we face. The gap between the threat and the cyber resilience of the UK needs to close as a matter of urgency.

Not a technical challenge

The majority of cyber attacks rely on techniques and vulnerabilities that are well known to us. We have the knowledge and the capability to defend against them. For example, we know that the five technical controls defined in the NCSC's Cyber Essentials Scheme – the minimum standard of security we advise organisations to achieve – can stop the vast majority of commodity cyber attacks.

However, too many organisations are not implementing the most basic protective measures. Schemes like Cyber Essentials are effective; the evidence described in this Annual Review is clear, and it is corroborated by similar data from a range of industry partners. However, the NCSC only issued 30,000 Cyber Essentials certificates last year, which means millions of organisations are leaving themselves open to cyber attacks that we know how to prevent.

So improving the cyber resilience of the organisations, at scale, is **not** a technical challenge.

The UK needs to wake up to the severity of the cyber threat. We need all organisations, public and private, to see cyber security as both an essential part of operational resilience, and a driver for business growth. To view cyber security not just as a 'necessary evil' or compliance function, but as a business investment and catalyst for innovation. Safeguarding systems and preventing data breaches, but at the same protecting reputation and building customer trust and retention.

This challenge is exacerbated by a technology market that does not incentivise organisations to develop secure products (which is discussed in depth on page 54 of this review). To re-emphasise, the barriers we need to overcome are not technical in nature. Defective and flawed software, sometimes rushed to market, is often at the heart of cyber incidents. We have the expertise and know-how to build a future where products are secure, private, resilient, and accessible to all. The technology to achieve this exists, but the commercial incentives to encourage adoption are flawed. We need to ensure there are market incentives to make this happen.

The NCSC advocates that immediate action is required to enhance the cyber security practices across the whole of society so we can:

- build a national infrastructure that is better prepared to withstand all but the most advanced cyber threats
- create an environment that imposes higher costs on adversaries targeting the UK and its interests
- foster the development of a market for secure technology and services

This is our aspiration for a more secure and prosperous future.

Protecting our digital way of life: the role of legislation

The NCSC raises awareness of the cyber threat and clearly guides citizens and organisations towards trusted cyber security advice, tools and services, promoting best practice, preparedness and mitigation. As the national technical authority for cyber security and critically, an integral part of GCHQ, the NCSC will continue to benefit from and leverage its unique insights to carry out this work. But this will not be enough. There is more to do.

One of the strategic levers that we can use to improve cyber security outcomes is legislation. The Network and Information Systems Regulations 2018 (NIS Regulations) went some way to enhancing the security of critical network and information systems in the UK, covering both 'operators of essential services' (OES) and 'relevant digital service providers' (RDSPs).

As the UK's only cross-sector cyber legislation, NIS regulations boost cyber and physical resilience. However, more could be done to build greater resilience into the UK's critical national infrastructure, to better withstand or recover from attacks by the most sophisticated state-level cyber threats. This government has committed to introducing the Cyber Security and Resilience Bill (CSRB) in this year's King's Speech, and we believe it's a crucial step towards hardening the UK's cyber defences. The UK government are using this opportunity to broaden the scope

of current regulations to protect more digital services and supply chains, to put regulators on a stronger footing, and to strengthen reporting requirements to build a better picture across government of cyber threats to the UK.

The new legislation won't be an end in itself. First, the implementation of the legislation – across government, across regulators, and across the economy – is a collective challenge. This may not be the only time we need new legislation to protect our infrastructure and economy. We need to listen to organisations working in the sector, to learn from our international partners, and ensure we have the legislation we need to give the nation the tools it needs to contest the threats we face. The scope stretches beyond the confines of our most critical infrastructure, with the Minister for Security recently committing to reviewing the 1990 Computer Misuse Act to combat cyber crime.

As well as strengthening regulation, policy and legislation to accelerate progress on raising resilience, the NCSC is planning to work across government to develop new capabilities to harden defences around our highest priority systems in response to changes in the geopolitical environment. This work will help us to prepare for crises and ensure that our national posture can keep up with what's going on in the real world. This will include how we communicate the threat, and what is expected of operators to prepare for, respond to, and recover from a cyber incident.

The UK cannot underestimate the severity of state-led threats, or the volume of the threat posed by criminals. The resilience of critical infrastructure, supply chains and the public sector must improve. But so must our wider economy.

We believe that cyber security legislation and regulation in the UK needs to be comprehensive, forward-looking, and responsive to an increasingly dangerous and diffuse threat landscape. Globally pioneering work done in the context of the Telecommunications Security Act has shown how effective legislation can be. We are bringing our technical expertise to bear in shaping and enabling these outcomes.

The NCSC has always believed that cyber security is a team sport, and right now, our collective efforts are not enough. Only when we are clear about what needs to be done, and then together are committed to actually doing it, will we succeed.

```
# Chapter title
chapter_title =
    “Developing the UK’s cyber ecosystem”
```

Chapter:

03

Introduction

The NCSC is future-proofing the UK's national security by building a self-sustaining ecosystem of cyber talent.

```
# Define the
message
message =
"Start here"
```

The NCSC plays a key role in strengthening the UK's cyber security ecosystem, which now contributes around £11.9 billion per year to the economy.

We harness the power of government, industry and academia to cultivate a fertile ground for excellence that supports the ecosystem at every level. From inspiring school pupils and providing opportunities in higher education, to funding research and bringing together innovative tech startups, we are future-proofing the UK's national security by developing a sustainable cyber ecosystem that now employs almost 61,000 people.

To sustain this ecosystem, we need to ensure skilled people, quality products and trusted services are on hand to help organisations stay resilient and develop their digital offerings. The NCSC works closely with partners to define standards, assure products and services, and to grow the pipeline of talent that the cyber security sector needs to thrive.

CyberFirst Girls Competition 2023/24

The CyberFirst Girls Competition aims to inspire girls aged 12-13 to explore the world of cyber and technology, helping to address the lack of diversity in the UK cyber workforce, where women currently make up just 17%. Since its inception in 2017, over 69,000 girls have taken part in CyberFirst Girls Competitions. The 2024 competition attracted more teams and schools than any other year, with 3,608 teams participating from over 750 schools, a 28.6% increase from last year. 84% of all participating schools were state schools.

61,000

employed in cyber security related roles

CyberFirst Regional Ecosystem

The CyberFirst Regional Ecosystem has experienced remarkable growth this year, which now includes 173 recognised schools and colleges, 140 CyberFirst Ambassadors, and over 35,000 engaged students. This growth has been driven by the regional and home nation partners offering in-school and extra curricula courses to schools within their region. All courses emphasise the ethics and legalities of 'messing around' with computers and the internet, and offer practical, hands-on learning and applied teamwork.

The partnerships approach is a model that delivers real impact, providing national and local employers with a trusted framework where they can engage with local schools and students in some of the most deprived parts of the country, releasing untapped potential and helping to keep the most talented young people within their local communities.

CyberFirst Ambassadors

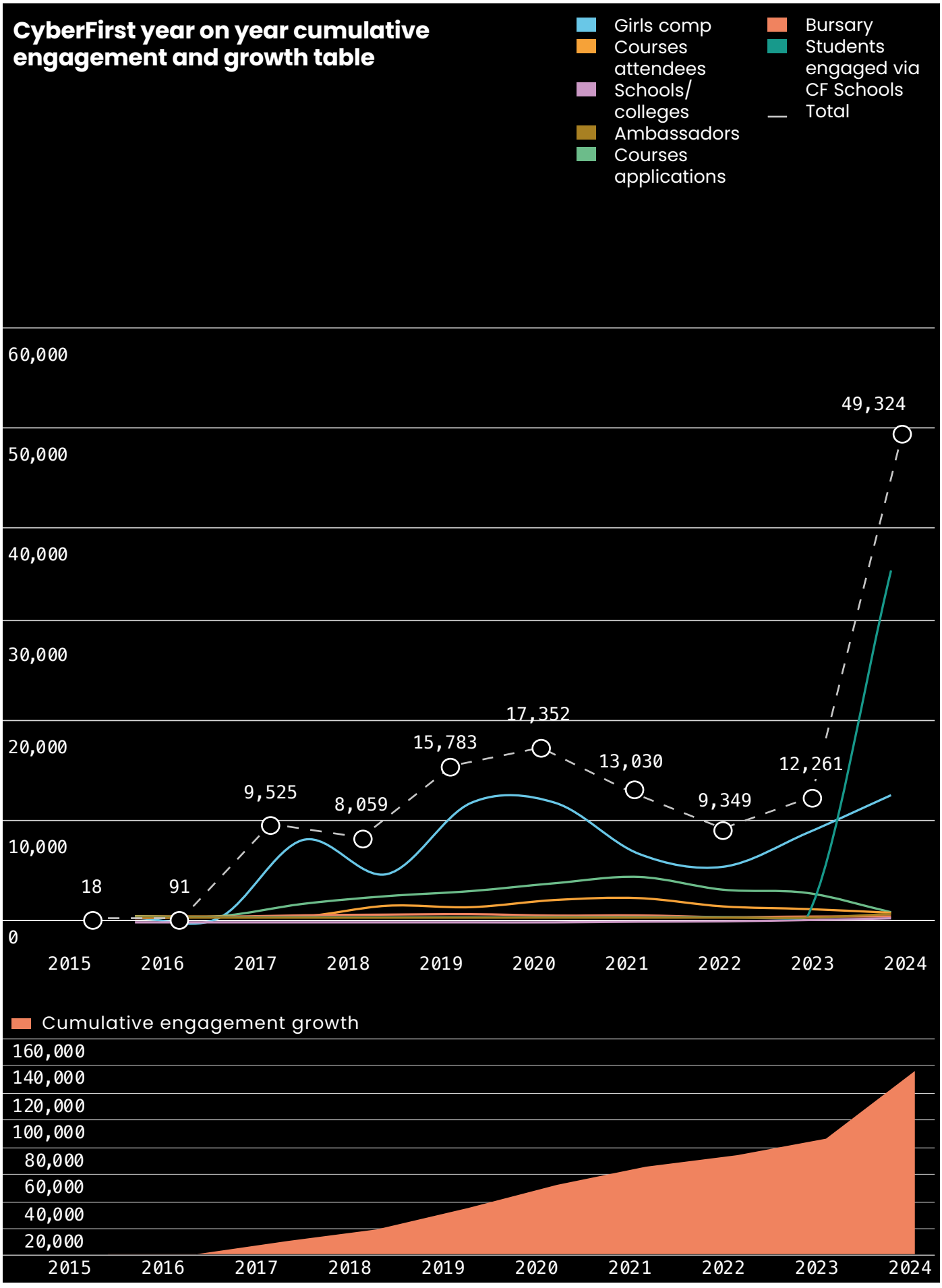
The CyberFirst Ambassador network was launched this year, and there are now over 100 CyberFirst Ambassadors signed-up from within academia and across a variety of businesses, from small startups to large-scale multinationals. The ambassadors are a key part of the ecosystem, and support the CyberFirst programme by:

- forging trusted relationships between schools and industry
- delivering CyberFirst activities in schools and colleges
- representing the regional and home nation partnerships, the NCSC and the CyberFirst brand
- being involved in assessment panels for CyberFirst schools and colleges
- encouraging schools and colleges that are not yet part of CyberFirst to apply

The social value of CyberFirst initiatives

Like many organisations, social value is an ongoing priority for the NCSC. This year, the NCSC commissioned (for the first time) a study to examine the social value of the CyberFirst programme. The study revealed that for £1 invested in CyberFirst there was a £4.06 social return on investment (SROI), which equated to £31m of evidenced social value.

The Regional Ecosystem work has a particularly high SROI, and showed a £6.52 SROI against every £1 invested. This indicates how the ongoing commitment from industry, academia and government enables CyberFirst to continue to provide opportunities to empower and develop talented students.


CyberFirst year on year cumulative engagement and growth table
Girls comp
Courses attendees
Schools/ colleges
Ambassadors
Courses applications
Bursary
Students engaged via CF Schools
Total
60,000
50,000
40,000
30,000
20,000
10,000
0
18
91
9,525
8,059
15,783
17,352
13,030
9,349
12,261
49,324
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
Cumulative engagement growth
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024

CyberFirst Bursary

The CyberFirst Bursary scheme continues to support the next generation of cyber talent, offering undergraduates a £4,000 per year bursary and a paid cyber security placement each summer to help kickstart their career in cyber. This year, a total of 111 students enrolled in the CyberFirst bursary scheme. Of these, 37% were female and 20% came from ethnic minority backgrounds.

The bursary program has a total of 1,280 students, supported by over 240 industry, academic and government institutions. Graduates finish the course with invaluable work experience, new skills, a better understanding of their career options and the confidence to succeed in the world of cyber. 88% of the 742 graduates are now employed in cyber security roles.

CyberFirst Champion scheme

A CyberFirst Champion is an alum of the CyberFirst Bursary Programme, working in a company and acting as the point of contact for current bursary students. The scheme has expanded from 30 to 41 members, serving as a vital link between current and former students, and CyberFirst members. Last year, the NCSC also introduced 'Cluster Events', a series of regionally organised gatherings providing a unique platform for networking among the alumni community. Attendees participate in lightning talks and engage with guest speakers from across government and industry.

CyberFirst Hackathon

In close collaboration with the NCF, NCSC co-delivered the inaugural CyberFirst Hackathon. The event marked a significant stride in the novel ways NCSC and NCF are collaborating across Government to nurture the UK's cyber talent. Hosted at Lancaster University, this event brought together 40 NCSC CyberFirst university students to tackle real-world cyber challenges in a collaborative environment. By focusing on wearable tech, Internet of Things, and data insights, the Hackathon bridged academia, industry, and government to create opportunities for hands-on learning and innovation.

The hackathon initiative not only enhances participants' technical skills, but also provides a gateway to future employment within the NCSC and NCF, and is a testament to the collective commitment to cultivate a robust UK cyber ecosystem that supports national security and technological advancement.

Higher education

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 beyond. This year saw Greenwich University added to the list of recognised institutions across England, Wales, Scotland and Northern Ireland.

The ACE-CSE programme builds on the NCSC's Certified Degree Programme, which certified eight new degree courses, bringing the total to 85. 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.

16

Academic Centres of Excellence in Cyber Security Education (ACEs-CSE) up 1

21

ACE-CSR

85

Certified degrees up 8 (61 PG, 18 UG and 6 apprenticeships)

Cyber Security Body of Knowledge (CyBOK)

Since 2017, the NCSC have sponsored Cyber Security Body of Knowledge (CyBOK), a free resource that codifies the foundational knowledge in cyber security for education and professional training, born out of a desire to bridge a well-recognised skills gap within the cyber security sector.

CyBOK is also supported by the UK Cyber Security Council, who set the professional standards adopted by the NCSC's Industry Assurance Schemes. Since 2021, we've been using CyBOK as the basis for describing the course content of the NCSC-certified undergraduate and postgraduate cyber security degrees programme, and for NCSC-certified training.

NCSC For Startups

The NCSC For Startups programme provides young businesses with insights, support and access to help them shape their cyber security products and services. The programme has supported startups at different all stages of maturity, from those developing a minimum viable product (MVP) to businesses with established solutions looking to develop, adapt and pilot their products. All supported projects are aligned to specific technology or cyber challenges that are set by the NCSC.

Created to engage corporations, consultants, investors and national security agencies, NCSC For Startups helps businesses to take breakthrough technologies to market faster than would be possible in a purely commercial model. To date, the programme has helped more than 70 tech companies and raised over £526m in investment, whilst creating over 1,700 new jobs delivering security and growth for the UK.

The NCSC For Startups alumni community

The NCSC For Startups alumni community has grown over the 8 years of the programme to include over 60 startup members, as well as government and industry partners from the cyber security sector.

The alumni community includes a powerful network of entrepreneurs who have faced similar business challenges. Members share valuable insights with each other on key issues, from securing investment and international growth to achieving successful company exits.

The community also provides access to the wider cyber ecosystem, giving startups the opportunity to engage and collaborate with industry, academia and government partners, bringing their unique perspective and innovative approaches to difficult cyber security challenges.

Industry 100

The NCSC's Industry 100 (i100) initiative brings together public and private sector talent to challenge thinking, test innovative ideas and enable greater understanding of cyber security. i100 encourages a variety of companies (with unique insights and capability in cyber security) to loan staff to the NCSC to help us defend the UK. The secondees are given security clearance that enables them to work alongside the NCSC's staff, including on sensitive projects and investigations.

This year, an additional 45 new participants joined the scheme, growing the community to 132. Highlights from i100 this year included:

- technical advice to modernise cyber security best practice for data infrastructure and managed service providers (MSPs)
- expert support in the NCSC's open source research, and in the development of critical guidance around industrial control systems (ICS) and operational technology (OT)
- endorsement from delegates from Japan and India at CYBERUK 2024, citing i100 as a stand-out example of the UK's world-leading approach to public-private partnership in cyber security

CYBERUK 2024

CYBERUK, the UK government's flagship cyber security conference, was held in Birmingham for the first time. Worth over £15.3 billion, the West Midlands has the fastest-growing tech sector in the UK, with specialist university research centres, innovative startups, world-class R&D infrastructure, and a cluster of major cyber security enterprises. This success story mirrors the essence of CYBERUK, where innovation converges with tradition.

CYBERUK 2024 examined how future technology represents significant opportunity, from employing AI in pioneering healthcare research, to using quantum computers to solve problems like climate change and food security. The 150 speakers across 45 sessions included Harry Coker (National Cyber Director for The White House), Sir Roly Keating (CEO, The British Library) and Heather Adkins (VP Security Engineering, Google).

£2m

boost to the local economy

2,380

in-person delegates from 55 countries

150

speakers across 45 sessions, including Harry Coker, National Cyber Director for The White House

137+

companies sponsored or exhibited with over 90% stating that CYBERUK met or exceeded their expectations

⅔

Nearly two thirds of attendees on average would consider using NCSC products and services following CYBERUK 2024 (24% increase from 2023)

93%

rated the event as good/excellent

87%

felt more informed on how to build a cyber security ecosystem that can manage the threats and opportunities of the future

Market incentives and the future of technology security

Technology markets do not incentivise the investments required to secure the foundations of cyberspace.

```
# Define the
message
message =
"Start here"
```

The modern three-point seat belt, designed by a Volvo engineer over 60 years ago, has doubtless saved millions of lives. Yet the patent for it was given away for free for the betterment of all, because Volvo chose not to compete on safety.

Just as seat belts are not a premium feature that users pay extra for, we should not have to pay for 'safety features' across the software and hardware sectors. Unfortunately, many cyber security features (such as multi-factor authentication, single sign-on or even access to certain logging) are deemed 'premium add-ons'; functionality that involves additional cost for organisations (or users), rather than being a fundamental component of the offering.

Products and services are produced by commercial enterprises operating in mature markets which – understandably – prioritise growth and profit rather than the security and resilience of their solutions. Inevitably, it's small and medium sized enterprises (SMEs), charities, education establishments and the wider public sector that are most impacted because for most organisations, cost consideration is the primary driver.

Put simply, if the majority of customers prioritise price and features over 'security', then vendors will concentrate on reducing time to market at the expense of designing products that improve the security and resilience of our digital world.

The NCSC want to build a future where products are secure, private, resilient, and accessible to all. The technology to achieve this exists, but the business and commercial incentives to encourage adoption are not present. So how can we ensure there are **market incentives** to make this happen?

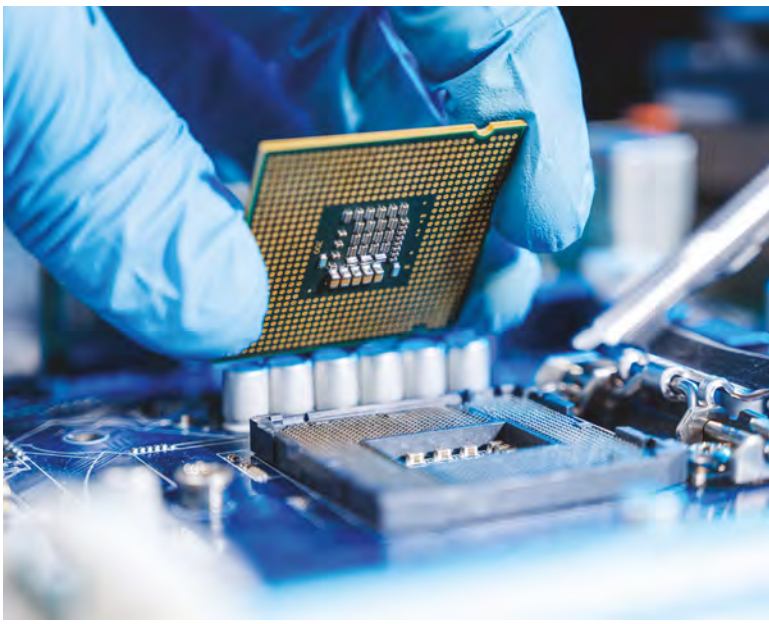
The roots of digital architecture

For some time now, the NCSC has used the term 'secure by design' to describe an approach that encourages organisations to 'bake' cyber security into all stages of the development life cycle, rather than adding it as an afterthought. Doing this addresses cyber security problems at root cause and prevents costly redesigns later on. We can improve the overall resilience of systems by encouraging investment in 'secure by design' practices. This is particularly true at the 'foundational layer' of our digital architecture, as any software or systems built on those foundations will benefit.

When we follow a 'secure by design' approach, we fix classes of vulnerability, rather than having to address the symptoms of a particular issue (typically through software patching). Memory safety vulnerabilities, for example, are one of the most prevalent types of disclosed software vulnerabilities, and investing in 'secure by design' development could drastically reduce onerous patch management and incident response activities. But with few incentives in current market structures for organisations to fix the root cause, memory safety vulnerabilities will continue to proliferate.

The NCSC believe that fixing these foundational insecurities will improve digital resilience across the globe, which is why we fully support a paper by the White House's Office of the National Cyber Director, 'Back To The Building Blocks: A Path Toward Secure and Measurable Software'. Like the NCSC's principles based assurance initiative, this paper stresses the need to solve security problems at root cause, and to explore the incentives required to re-align the market.

The backdrop to this is a threat landscape that reveals increased intent from nation-state actors and cyber criminals, both with access to enhanced capabilities such as AI-enhanced vulnerability scanning. The increased **appetite** and **ability** to rapidly scan for and exploit these foundational vulnerabilities means we are presenting adversaries with an increasingly exploitable attack surface. One which we could harden by fixing vulnerabilities at root cause.

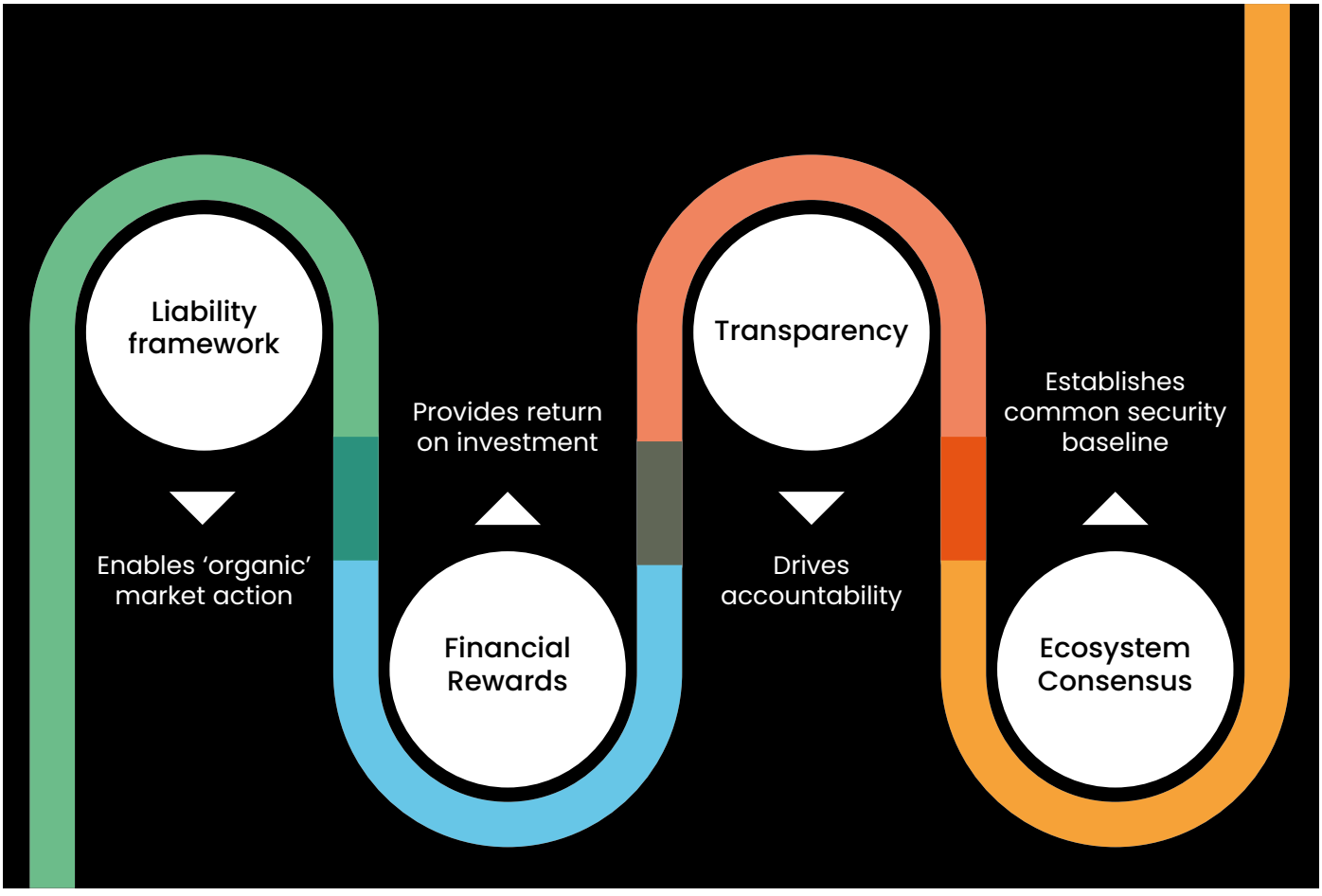


Creating the right market incentives

As mentioned earlier, the software and hardware market does not incentivise investment in security. The reasons for this are due to a wide set of market behaviours and incentives, including:

- 'information asymmetry' between vendors and customers (a situation where sellers are better informed than buyers about the quality of the goods or services)
- vendors will prioritise reducing time to market over designing products that are 'secure by design' (which takes longer and requires increased engineering costs)
- customers will usually prioritise price and features over security
- the adverse cyber security outcomes from an ever-growing mountain of technical security debt, exacerbated by mergers and acquisitions which inherit legacy technologies
- a belief by some that the risks of insecure technology and digital infrastructure should be borne by wider society, rather than by those making investment decisions

A series of discussion groups, expert panels and academic research led the NCSC to develop an understanding of four key drivers that we believe could shift the incentive structures that underpin technology markets and their attitude to security. These drivers are: **liability**, **financial reward**, **transparency**, and **consensus**.



Leveraging these drivers to develop policy options would use network effects, the drive for profit and the desire to maintain reputation to incentivise enterprises to prioritise security. We believe that a range of incentives are required to encourage commercial enterprises to focus on security for their own benefit, which will mean better security outcomes for everyone.

The NCSC wants to build an alliance of stakeholders across HMG, industry, academia and with our international partners. Creating the desired market incentives will require further research into the dynamics of our most important technology sectors and markets. Strategic policy will need to be developed across government. We must:

- work with DSIT to develop the underpinning strategic policy
- signal to markets that nations are fully committed to increasing the transparency and visibility of poor cyber security standards that organisations have grown used to accepting
- make those responsible for those decisions accountable for investing in 'defective products' [1]

Two visions of the future of security...

The future of technology security will evolve somewhere along a spectrum. At one end, the market continues as it is now, where security remains an afterthought and consumers and wider civil society bear the brunt. In this scenario, consumers will find their data compromised, their systems held at ransom, and their privacy invaded. They will have no means of holding to account those responsible for the defects that failed to prevent such attacks.

Furthermore, it will be increasingly difficult to know where defective products have allowed vulnerabilities to be exploited, such is the increasing complexity of interconnected digital systems. Entire swathes of our critical infrastructure could be severely impacted by exploitation of simple vulnerabilities, affecting the UK's ability to have consistent flows of electricity, clean water and a functioning transport system. The UK won't be economically prosperous if we can't trust the integrity of our critical sectors.

At the other end, entire classes of exploitable bugs could be mitigated by organisations investing in basic digital resilience through foundational security and 'secure by design' technology.

Improving the resilience of our software and hardware technology stacks in ways that can scale globally is a multi-faceted challenge. The technology to raise resilience at scale exists, but it will require – amongst other things – a strategic policy agenda that fundamentally alters the dynamics of the existing market.

1 CISA chief Easterly calls software vulnerabilities a 'product defect,' urges liability regime (https://insideaipolicy.com/share/16704)

```
# Chapter title
chapter_title =
    "Keeping pace with evolving technology"
```

Chapter:

04

Introduction

```
# Define the
message
message =
“Start here”
```

The NCSC’s expertise across the technology stack helps the UK respond to emerging threats and opportunities.

As the national technical authority for cyber security, it’s vital that the NCSC keeps pace with evolving technology, particularly where significant changes affect our critical technologies, systems and sectors.

Some of these changes directly impact end users, such as understanding how we can reduce our reliance on passwords for authentication and move to passkeys. Other changes impact developers, for example improving software development practices to reduce vulnerabilities in the apps and devices embedded throughout our connected society. The NCSC requires expertise throughout this technology stack to help the UK prepare and respond to emerging opportunities, risks and threats.

The NCSC invests in extensive internal research into emerging technologies to explore new ways to reduce harm at scale. Some new technologies – such as AI – are potentially disruptive, and their development cannot be ignored. Many others evolve more slowly, but continue to have a huge effect on how resilient our systems are. For example, cloud and the ‘internet of things’ (IoT) can no longer be described as new, but they’re so ubiquitous that small changes to the standards or technologies they incorporate can have far reaching impact.

Research is long-term work that doesn't always result in short-term benefits. However, the expertise we gain informs everything we do and allows us to provide expert authoritative input to drive our strategic aims which manifest elsewhere in government, such as our work supporting research into semiconductors led by the Department for Science, Innovation and Technology (DSIT). Similarly, our expertise in IoT platform security informed the development of the PSTI (Product Security and Telecommunications Infrastructure) Act, which came into force in April 2024. The act requires manufacturers of UK consumer connectable products (or 'smart' products) to meet minimum security requirements.

The global technology landscape is vast. The NCSC's technical teams are small by comparison, so we work closely with national and international partners in industry, government and academia to meet the challenge and maximise our impact. The NCSC's research institutes (based at the University of Bristol, University of Surrey, Imperial College London and Queen's University Belfast) provide focal points for foundational research into critical aspects of cyber security. The communities they generate span all of our technical partnerships, and allow us to collaborate on a larger scale.

Artificial intelligence (AI)

The NCSC is pioneering research in the secure development of AI technologies, both through our own insights and through engaging with industry and academia.

In February 2024, the NCSC hosted the fourth iteration of WAIST (the Workshop on AI Security Technologies). This is an annual event delivered by the NCSC's data science research team, and aims to build understanding of AI security vulnerabilities and strengthen the community working to mitigate them. This year's delegates included partners from across the Five Eyes and UK intelligence community, as well as industry, academia and other international agencies. By working together in this way, we can drive global security improvements in a critical technology whilst supporting UK entrepreneurship.

At the same time, the NCSC has deepened its cooperation with US counterparts, including the Cybersecurity and Infrastructure Security Agency (CISA), the AI Security Center (AISC), and the US AI Safety Institute. In November 2023, the NCSC published the Guidelines for Secure AI System Development in cooperation with industry experts and 21 other international agencies and ministries from across the world, including those from all members of the G7 group. The UK-led guidelines, the first of their kind to be agreed globally, aim to raise the cyber security levels of AI and help ensure that it is designed, developed, and deployed securely.

The NCSC are now working closely with DSIT to deliver the next stages of this work, developing the guidelines into a voluntary Code of Practice and global standard.

In the past year, the NCSC has also advanced its collaboration with the UK AI Safety Institute (AISI), which was set up by DSIT in November 2023. This partnership has focused on developing robust AI safety protocols. These efforts aim to ensure that AI technologies are deployed responsibly, reducing the risk of cyber harm due to AI models.

Post-quantum cryptography

In August 2024, a major milestone in post-quantum cryptography (PQC) was reached when NIST, the US national standards organisation, published three PQC algorithm standards. The same month, the NCSC published a paper describing what this means for UK organisations planning their migration to PQC. This is covered in more detail on page 69 of this review.

In addition to hosting an event on PQC with UK regulators, on the international front we have ensured that the NCSC's technical positions are prominent in work that the Central Digital & Data Office (part of DSIT) have led in the multi-national Digital Government Exchange, and offered a well-received thought leadership paper on the likely computational cost of quantum attacks on cryptography within standards bodies.

Crypt-Key

The NCSC collaborates with UK and international partners to protect our most sensitive information and enable our most important capabilities using our cryptographic expertise, known as 'Crypt-Key'. Crypt-Key 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 as well as supporting NCSC directly has collaborated with us throughout 2024 to deliver world-leading encryption products to protect the UK's most sensitive data, and that of our partners.

Working with the MOD the NCSC is also leading 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.

Principles Based Assurance

Principles Based Assurance (PBA) is the NCSC's chosen approach to determining if a technology product is 'secure enough' for its intended use. This approach is a quite radical departure from traditional methods of 'technology assurance', in that the principles describe 'what' needs to be achieved, rather than 'how' this is carried out. For us, PBA describes the overarching aim, as opposed to providing specific granular instructions for users to follow.

The flexibility of PBA means it can be used to assure a wide range of different technology products. This year we've developed a range of new assurance services that use PBA for specific technology classes or customer needs, including those facing elevated threats. The first of these at-scale services will be Cyber Resilience Testing (CRT), which is designed to assess how resilient any connected technology is to attack from a connection to a less-trusted environment, such as the internet. PBA is applied to consider the engineering processes used to develop and support the technology throughout its life cycle, limiting vulnerabilities at every stage.

The CRT service (and associated services for cyber resilience when facing elevated threats) has been successfully piloted, laying the ground for formal launch. These services will be closely aligned with initiatives from international partners, and will prove a valuable tool in uplifting the cyber resilience of technology across all sectors.

Individual Cyber Defence

In response to the UK general election, we accelerated our development of the Individual Cyber Defence (ICD) service to provide practical support for high-risk individuals for UK officials and election candidates, as part of our Defending Democracy initiative (see page 32 of this review). This followed the government's announcements of attempts by the Russian Intelligence Services and China state-affiliated actors to carry out malicious activity targeting UK institutions and individuals, including parliamentarians.

The two new opt-in ICD services comprise:

- the **Personal Internet Protection** service, which adds an extra layer of security against spear-phishing by blocking access to known malicious domains on individual's personal devices
- the **Account Registration** service, which alerts individuals if the NCSC becomes aware of a cyber incident impacting a personal account

The Personal Internet Protection service builds on the NCSC's Protective DNS service which was developed principally for use by organisations. Since 2017, PDNS has provided protection at scale for millions of public sector users, handling more than 2.5 trillion site requests and preventing access to 1.5 million malicious domains.

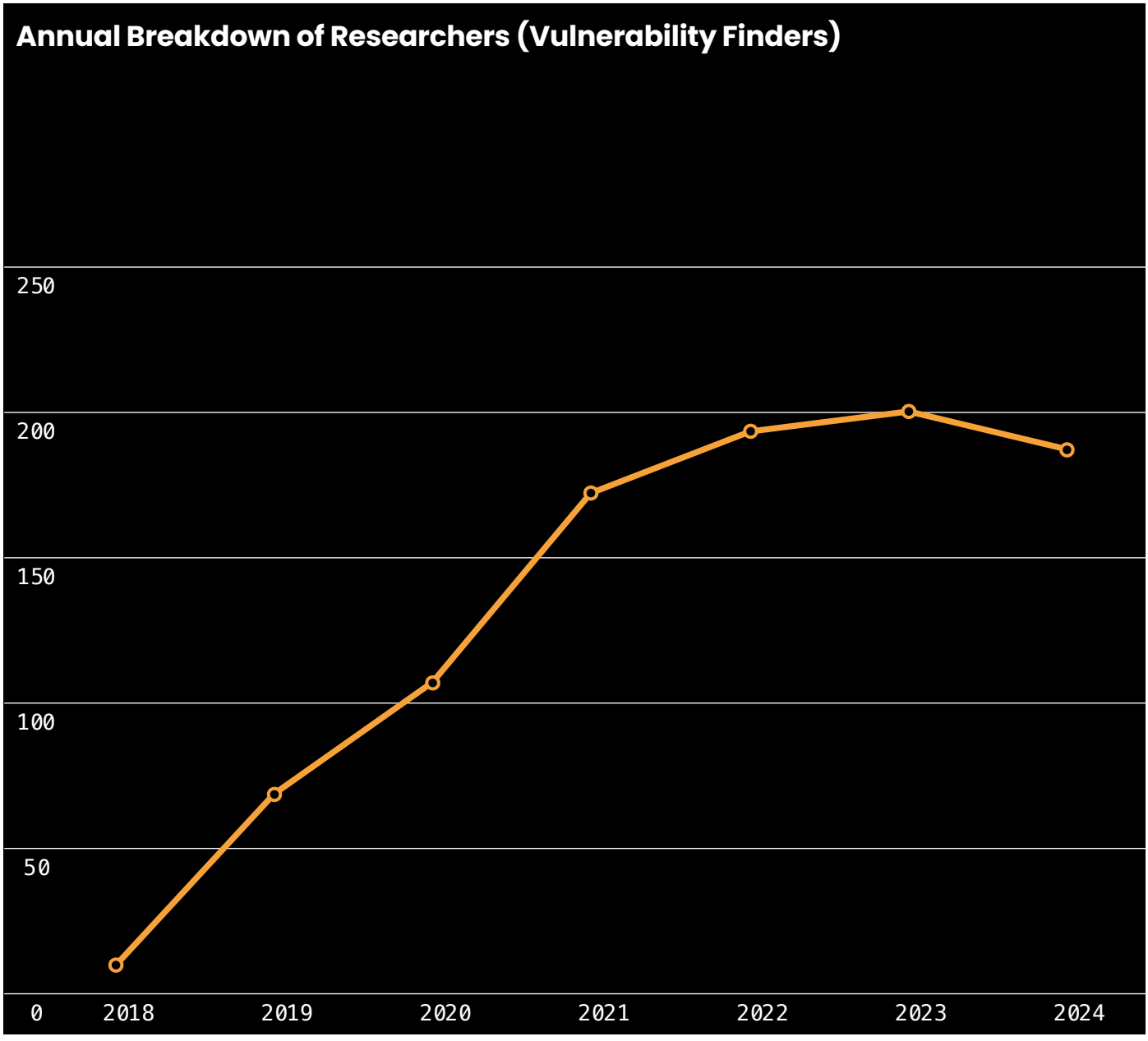
Vulnerability Reporting Service

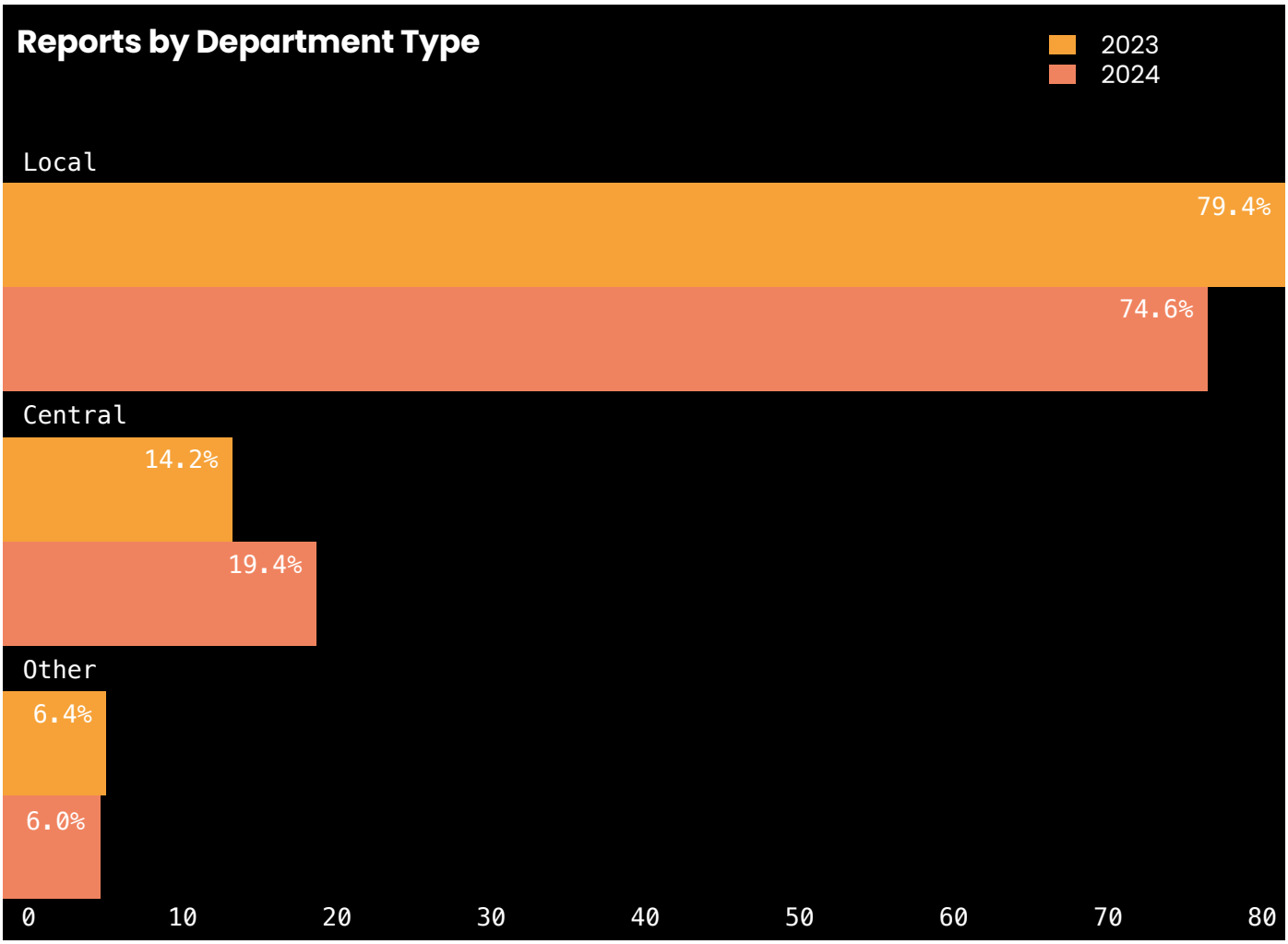
Since 2018, the NCSC Vulnerability Reporting Service (VRS) has allowed individuals to report vulnerabilities in government online services to the NCSC. As a thank you to those who submit vulnerabilities, finders are awarded HackerOne reputation points. In select cases we have also presented them with an NCSC challenge coin.

In addition, the NCSC also runs the Disclosure for Government Scheme, which enables government departments to manage their own vulnerability disclosure process while making use of the shared platform and triage service the VRS offers. We now have over 40 government organisations running their own disclosure programme through the scheme with a further 30 more currently being onboarded.

The VRS and the Disclosure for Government Scheme have both successfully been transitioned to the Government Cyber Coordination Centre (GC3). The NCSC, as part of GC3, will continue to support and encourage vulnerability disclosure across government. Of course, this wouldn't be possible without the continued support of the finder community and the value they bring to government.

In the last 12 months we have seen the number of finders who have submitted vulnerabilities continue to grow to the highest numbers we have had so far. The graph below shows the trend continuing, and it is predicted by the end of 2024 we will see an even higher number of individual finders participating in the VRS. We are working as part of GC3 to take feedback from the finder community and working with our platform and triage partners to continue to improve this engagement and encourage best practice amongst the vulnerability disclosure community.





Finders can report a vulnerability they find in any UK government online service. The bar chart below shows a breakdown of submitted reports by department type. Three quarters of all reports submitted to the VRS are related to services run by local authorities. However, this is to be expected as the UK is split into over 10,000 local councils, each with an online presence and any number of digital service offerings.

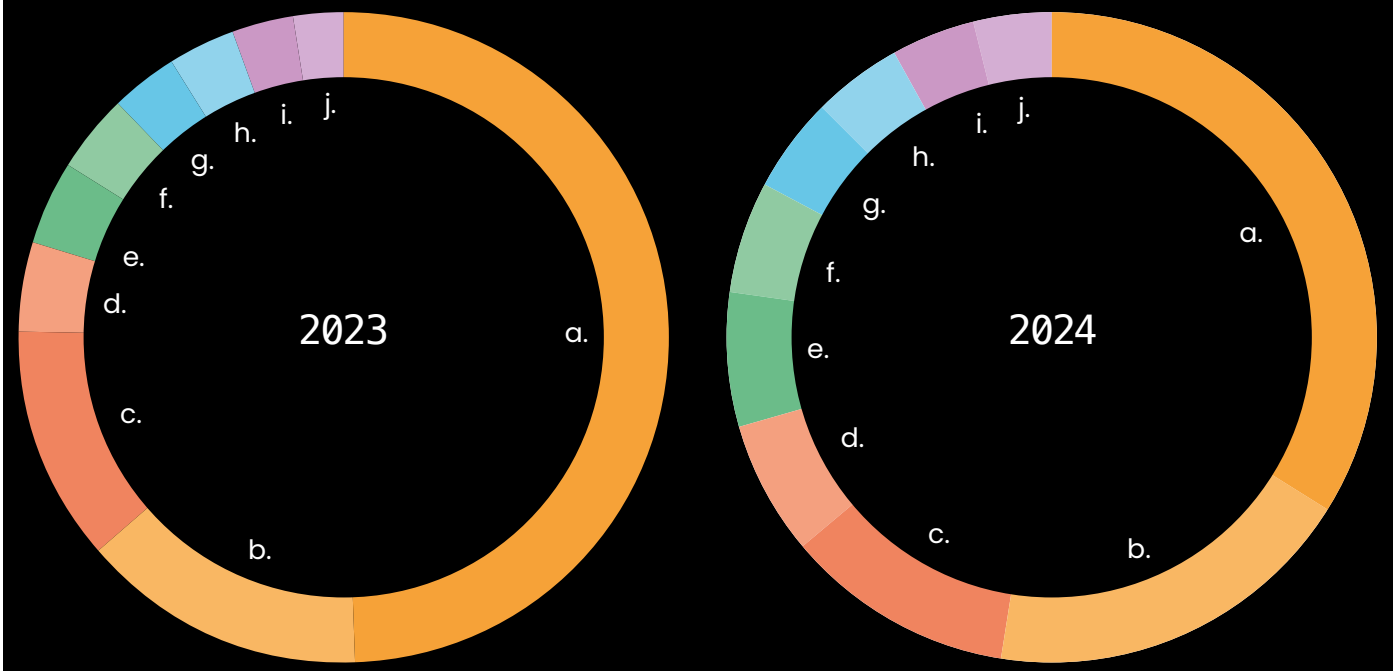
Local government providing services at local level from county level, down to town or parish councils. It can also include local public services such as GP surgeries, and fire and police services.

Central government departments with overall governance at a national level, such as national regulatory bodies. Some central government departments have their own vulnerability disclosure programme (VDP) through the Disclosure for Government scheme.

Other departments that comprise significant but out-of-scope cases, such as critical national infrastructure. 'Other' will also include any spam reports.

Cross-site scripting continues to be the most reported vulnerability, although the total is down from last year. Vulnerabilities that result in information disclosure have also decreased. We have also seen insecure direct object reference (IDOR) vulnerabilities break into the top 10. Of course, the most encouraging aspect is that these vulnerabilities are being reported and remediated as soon as possible.

Breakdown of top 10 (2023/24)



A.	49.61%	Cross-site Scripting (XSS) - Reflected	33.99%
B.	14.27%	Information Disclosure	18.50%
C.	11.52%	Open Redirect	11.55%
D.	4.45%	Path Traversal	6.69%
E.	4.32%	Code Injection	6.56%
F.	3.80%	Improper Access Control - Generic	5.64%
G.	3.27%	Privilege Escalation	4.59%
H.	3.27%	Information Exposure Through Directory Listing	4.59%
I.	3.01%	SQL Injection	4.20%
J.	2.49%	Cross-site Scripting (XSS) - Generic	3.67%

NCSC guidance

The NCSC produced a suite of 'Defending Democracy' guidance in advance of the general election, which included:

- new guidance for high-risk individuals (such as parliamentarians and election candidates) to help them improve the security of their personal devices and accounts
- guidance for political organisations offering advice to help IT practitioners implement security measures that will help prevent common cyber attacks
- guidance for organisations involved in coordinating elections, such as local authorities on steps to take to protect electoral management systems

In addition to the Guidelines for Secure AI System Development (which was jointly published by the NCSC, CISA, and 20 other partner agencies from around the world) the NCSC also updated the principles for the security of Machine Learning to reflect recent developments in the rapidly advancing world of AI. This included new sections on risks to large language model (LLM) systems, the importance of supply chain security and lifecycle management.

Other major guidance published this year included:

Vulnerability management

Principles to help organisations establish an effective vulnerability management process.

Principles for ransomware-resistant cloud backups

Helping to make cloud backups resistant to the effects of destructive ransomware.

Private Branch Exchange (PBX) best practice

Guidance helping organisations to protect their telephony systems from cyber attacks and telecoms fraud.

Info as follows:

- **19** new or revamped pieces of guidance published
- **1.5** million user visits
- **58** blogs on a range of subjects

Top searched terms:

- Cyber aware **1441**
- Password(s) **1376**
- Phishing **858**

Most accessed topics:

- Phishing **397k**
- Education **200k**
- Passwords **167k**
- CNI **102k**
- AI **60k**

Post-quantum cryptography

```
# Define the
message
message =
“Start here”
```

Migration to post-quantum cryptography (PQC) may feel daunting, but it also promises major opportunities. The NCSC explains how it will help organisations plan their migration.

Cryptography is everywhere.

It protects our data when we access online services and shops. It's used when you electronically sign legal documents. It's a critical part of our military and emergency services' communications and the smooth running of the UK's critical national infrastructure (CNI). Yet it's also invisible to almost all users, even though cryptography underpins every online service, and every aspect of the UK's infrastructure.

Quantum computers of the future, with their potential to offer capability unachievable by any conventional computers, pose a threat to much of the cryptography that underpins the security of our digital infrastructure. Although such computers are some years away, governments of all major nations are investing heavily in the development of quantum computing.

Migration to **post-quantum cryptography** (PQC) – cryptography that is resistant to attack by quantum computers – is the primary mitigation to this threat. There will be a global migration of IT and operational technology systems to use PQC. Major technology firms are already integrating PQC into some of their core products.

Our priority at the NCSC is to ensure that the UK's migration to PQC is smooth and does not raise wider cyber risks to our central government systems and our CNI. However, as the national technical authority for cyber security, we also need to help system and risk owners across all sectors of the UK plan their PQC migrations. We can't solve all the challenges in migration for every organisation; the scale is far too large. So, our focus is on how we raise understanding, set examples of best practice and identify interventions the NCSC can make that have the most scalable impact. These are outlined below.

Providing access to cryptographic expertise

Addressing the quantum computing threat has, for many years, been a problem for mathematicians and cryptographers, and this summer, three post-quantum algorithm standards were finalised. However, migration to PQC is a much broader cyber security effort that needs expertise from cryptographers alongside systems integrators and engineers.

A challenge for migration to PQC is that preparatory effort in **cryptographic discovery** (the process of identifying sensitive data, and where the cryptography that protects it lives within a system) is not a simple activity. However, the UK has some world-leading specialist cryptography companies, who have a focus on PQC. The NCSC is currently building a pilot scheme to accredit some of these companies, and to help them find markets in the UK. This will also help some of our critical sectors access the expertise required to help them prepare for their migration

As these initiatives encourage new companies in this sector to grow, they will need to be able to hire skilled talent from UK universities, and develop applied cryptographers, fusing expertise from a wide range of scientific disciplines, who understand how to build cryptographic systems in the real world. To enable this growth, we would be keen to see groups with deep expertise in the implementation of cryptography flourish within UK academia, so that all sectors of the economy will benefit.

Maintaining confidence in PQC

Migration to PQC, for many organisations, will take more than a decade and cover multiple investment cycles and changes of leadership. This means we need to understand the incentives that will encourage organisations to invest now; if everything is left until several years' time, migration will be poorly planned, rushed, more expensive, and likely introduce the sort of easy-to-exploit vulnerabilities we are too used to seeing.

The NCSC's work on market incentives (see page 54) will play a part in this. We know that our regulators understand their sectors better than we do, so our focus is to equip those regulators with the knowledge and advice that will enable them to set the right direction.

As well as building this initial momentum, we need to ensure that we help maintain confidence throughout migration. We are now in a period where mature implementations of the algorithms, built into modern protocols, are still evolving. In this early phase where organisations are planning their migration (rather than deploying PQC widely), we might expect to see some vulnerabilities; not in the underlying cryptography but in the implementation of the technology. There is a role for many groups, in the media, in academia, and in government, to discuss these cases maturely. The NCSC's role, as the authority within government on cryptography, will be to help our key partners navigate these discussions, and signal to the rest of the UK our confidence in PQC.

Learning from the early adopters

There are some sectors – finance is a good example – where working within international regulations (and keeping pace with competitors) means that planning is already well underway in many larger organisations. There are other sectors that are less well-resourced with significant legacy technology, for which direct upgrades to PQC will not be possible.

The NCSC's approach is to identify good practice and lessons learned in the faster-moving sectors. Since the differences between sectors are vast, we're not planning to set universal target dates for migration. Instead, we'll work with regulators to help them set suitable targets for each sector individually.

However, we do believe that planning for all sectors should get underway as soon as possible, using what we learn from early adopters to develop case studies and guidance for some of the harder migration problems. Where we identify aspects of migration within government (and within unregulated areas that are not fully understood), we will support pilot projects that help us provide the guidance that people need.

The benefits of secure migration

We intend to have accredited a small group of PQC consultancies by the end of March 2025. Alongside this, we will be running test projects within government focussing on the discovery activities that the NCSC recommends all organisations undertake; understanding where and how cryptography is used in all systems - theirs and their suppliers, the technologies that rely on it, and the data it protects whether in transit or storage. We will also be refining our broader offer to UK industry and provide tailored advice to sectors of national importance to support transition to PQC.

Migration to PQC is a national technology change programme. It comes with significant potential cyber risk, and we have a strong responsibility to manage that. But it also promises major opportunities. All organisations should be focussing on activities that underpin PQC migration; clear system auditing, rationalising services, putting a greater focus on building systems that can be easily updated in future and growing new technical skills. These are all important for broader secure design and management, so if the migration is done well, we will all benefit, far beyond the cryptographic changes.

Designed and created by Treble and M&C Saatchi

Follow us

@NCSC

@cyberhq

National Cyber Security Centre

National Cyber Security Centre
a part of GCHQ