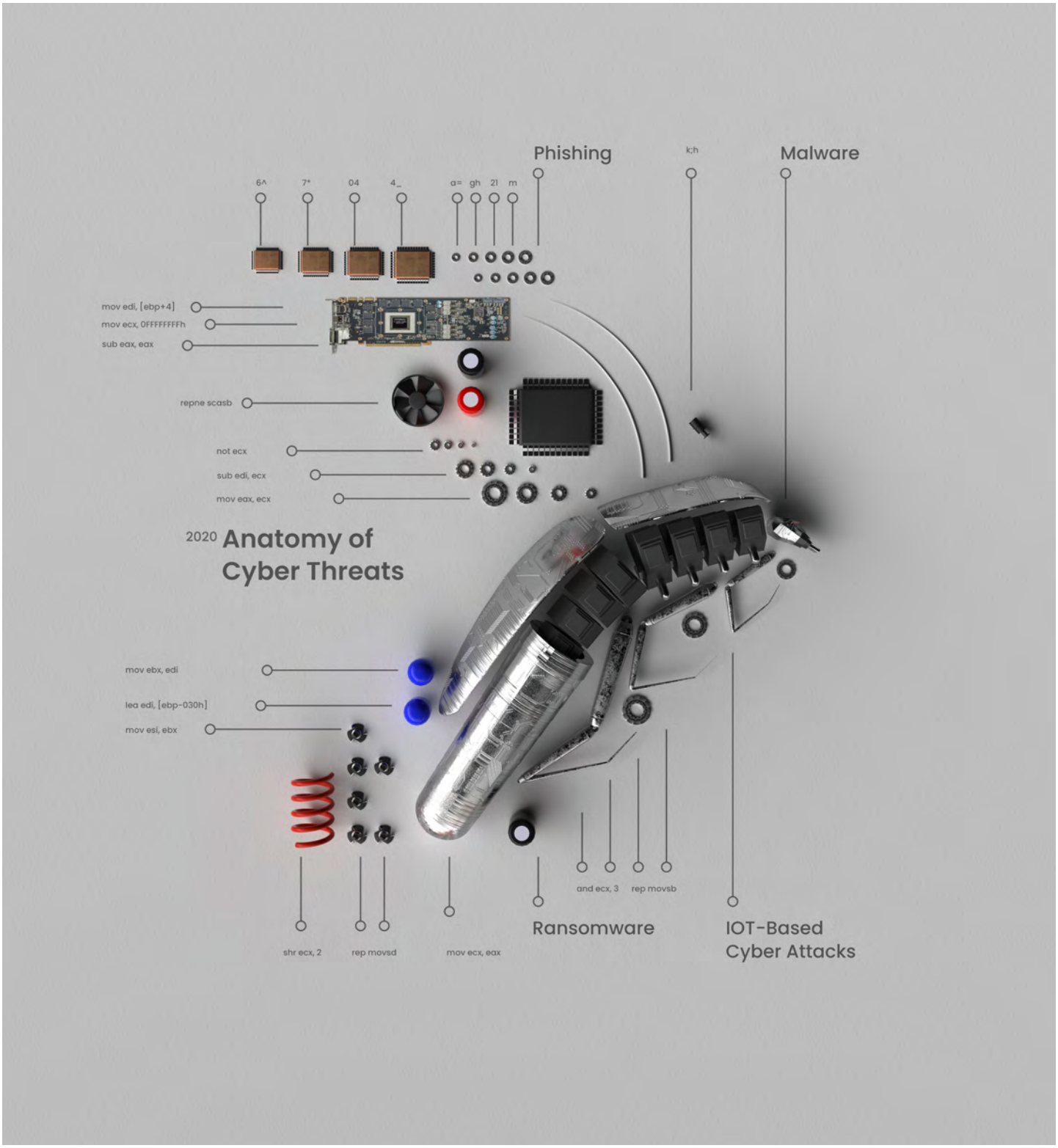
National Cyber Security Centre
a part of GCHQ

Annual Review 2020

Making the UK the safest place to live and work online



The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber threats.

Since the NCSC was created in 2016 as part of the Government's five-year National Cyber Security Strategy, it has worked to make the UK the safest place to live and work online.

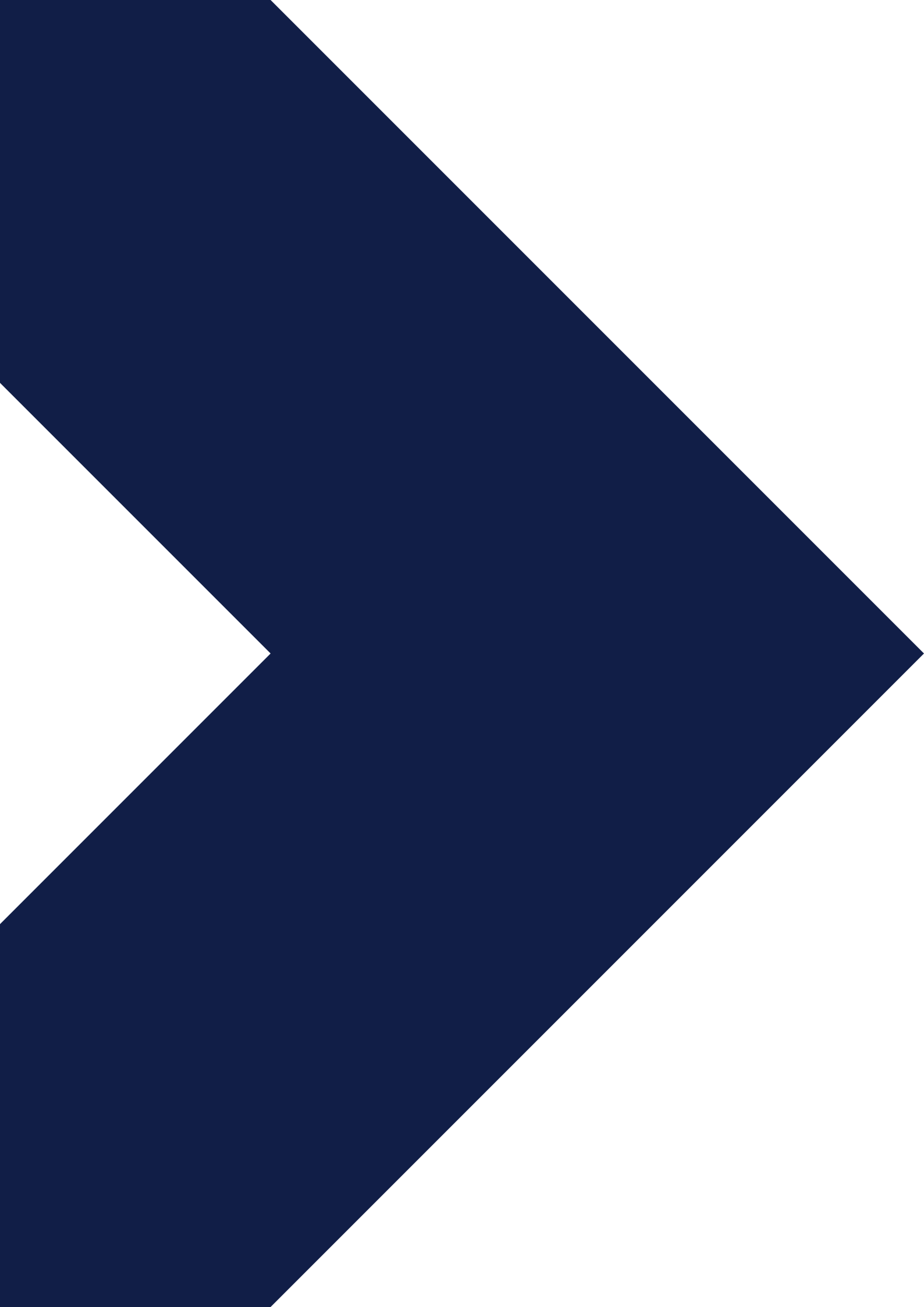
This Annual Review of its fourth year looks back at some of the key developments and highlights from the NCSC's work between 1 September 2019 and 31 August 2020. As part of a national security organisation not all its work can be disclosed publicly but the review seeks to describe the year with insights and facts from colleagues and teams inside and out of the organisation.

The NCSC has also produced a digital report where you can see this year's events come to life at:

ncsc.gov.uk/annual-review-2020

National Cyber Security Centre
a part of GCHQ

GCHQ



Contents

17 **1** Coronavirus – Responding to the pandemic

33 **2** Defending democracy

45 **3** Building a resilient nation

63 **4** Proactive engagement

81 5 Defending the digital homeland 24/7

107 6 Driving cyber skills and innovation

117 7 International influence

Ministerial foreword

The Rt Hon Penny Mordaunt MP,
Paymaster General

For the NCSC, as for the UK as a whole, this year has been dominated by the unprecedented challenge of the coronavirus pandemic.

The organisation is dedicated to making the United Kingdom the safest place in the world to live and work online. During the pandemic it has tackled more cyber threats than ever before.

This Annual Review shows how the NCSC took decisive action against malicious actors in the UK and abroad who saw the UK's digital lifelines as vectors for espionage, fraud and ransomware attacks.

The NCSC helped to protect NHS Trusts, the Nightingale hospitals and vital NHS systems, ensuring they were able to function remotely in spite of coronavirus.

In this year of complex challenges, the NCSC continues to react to swiftly evolving cyber threats. The organisation's nationwide guidance to individuals and businesses on protecting their security proved invaluable. Its new service aimed at rooting out online scams saw the public respond with reports of over two million suspicious emails.

This Review demonstrates two important messages about the NCSC's work. First: we are all the targets of cyber criminals. While preventing crime is the NCSC's priority, working in close partnership with law enforcement, it has also supported nearly 1,200 victims of 723 attacks this year that proved impossible to deflect. Second: cyber security is a team sport.



Government, industry and the public have an important role in building UK resilience to a spectrum of risks – hostile activity from state and non-state actors, terrorism and serious organised crime. At this pivotal time for the cyber sector, I want to welcome the NCSC's new Chief Executive Officer, Lindy Cameron, and pass on my gratitude to her predecessor, Ciaran Martin.

From the NCSC's inception, Ciaran was instrumental in developing the UK's National Cyber Security Strategy, striking the balance between economic opportunity and security. Lindy, with over two decades' experience of national government security policy, is well placed to steer the NCSC from strength to strength.

The pandemic continues to affect how we live and work. It is vital that cyber security remains a priority. It will help us to stay ahead of changing technologies, seize the opportunities for the UK as an independent country outside the European Union, and harness cyber's full potential to help drive economic recovery.

Introduction

by Lindy Cameron, CEO of the National Cyber Security Centre

It is a great privilege to present the fourth Annual Review of the National Cyber Security Centre, a part of GCHQ. I am honoured to have been appointed as the NCSC's second Chief Executive Officer, taking over from Ciaran Martin who was so pivotal in the development of this world-leading organisation.

This Review outlines another impressive year of delivery for the NCSC from September 1 2019 to August 31 2020, largely against the backdrop of the shared global crisis of coronavirus. As you would expect, the pandemic features heavily in this Review. I am proud to lead an organisation of staff that both helped with the UK's response to coronavirus and also sustained delivery of a nationally important brief, despite the challenges felt by us all this year.

Expertise from across the NCSC has been surged to assist the UK's response to the pandemic. More than 200 of the 723 incidents the NCSC handled this year related to coronavirus and we have deployed experts to support the health sector, including NHS Trusts, through cyber incidents they have faced.

We scanned more than one million NHS IP addresses for vulnerabilities and our cyber expertise underpinned the creation of the UK's coronavirus tracing app. An innovative approach to removing online threats was created through the 'Suspicious Email Reporting Service' – leading to more than 2.3 million reports of malicious emails being flagged by the British public. Many of the 22,000 malicious URLs taken down as a result related to coronavirus scams, such as pretending to sell PPE equipment to hide a cyber attack.

The NCSC has often been described as world-leading, and that has been evident over the last 12 months. Our innovative 'Exercise in a Box' tool, which supports businesses and individuals to test their cyber defences against realistic scenarios, was used in 125 countries in the last year. Recognising the change in working cultures due to the pandemic, our team even devised a specific exercise on remote working, which has helped organisations to understand where current working practices may be presenting alternative cyber risks.

Proving that cyber really is a team sport, none of this would be possible without strong partnerships internationally and domestically. We worked closely with law enforcement – particularly the National Crime Agency – and across government, industry, academia and, of course, the UK public.

The NCSC is also looking firmly ahead to the future of cyber security, as our teams work to understand both the risks and opportunities to the UK presented by emerging technologies. A prominent area of work this year was the NCSC's reviews of high-risk vendors such as Huawei – and in particular the swift and thorough review of US sanctions against Huawei. The NCSC gave advice on the impact these changes would have in the UK, publishing a summary of the advice given to government as well as timely guidance for operators and the public.

And on the future, this report shows our commitment to creating an environment in which cyber security can thrive. There is a lot to do but the NCSC is committed to playing a leading role across the cyber

security community. A record number of young people have been introduced to cyber through a portfolio of skills programmes, including one which saw a 60% rise in girls applying for the summer courses, which were all delivered remotely. It is a top priority that the UK's future cyber security workforce better represents the UK public, which is why the NCSC's partnership with KPMG on the 'Decrypting Diversity' report into diversity and inclusion in the UK cyber security industry is so important.

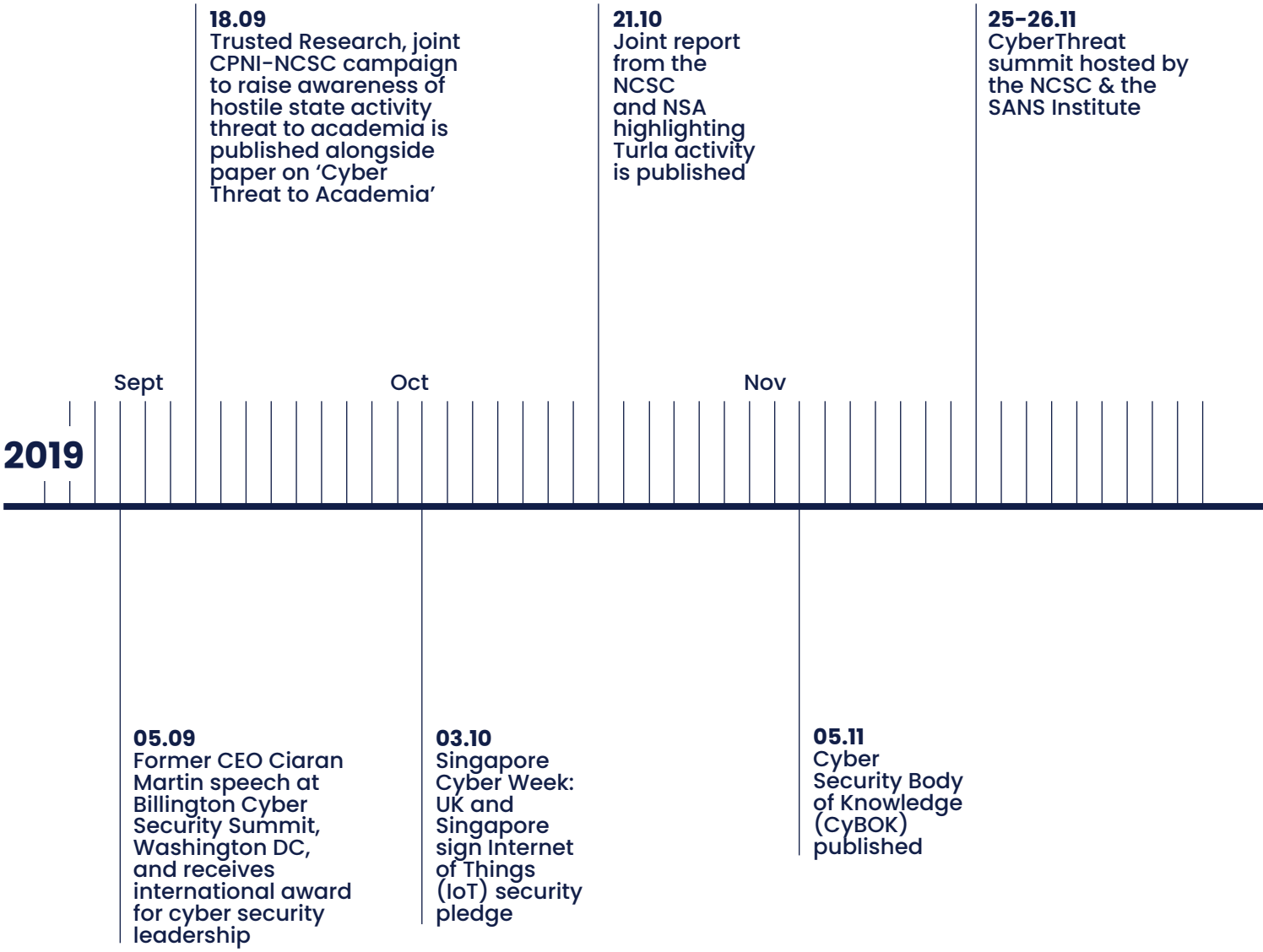
This Annual Review and the record of delivery within it is testament to the innovation, expertise, hard work and dedication of the NCSC's workforce, especially in this year's extraordinary circumstances. My thanks go to them all and I hope they take great pride in their achievements.

I am hugely excited to lead this team and take the NCSC on the next stage of its journey. Throughout this Review, the real-world impact being driven by our expertise to the benefit of the UK is evident. As NCSC has done since its inception, we will continue to adapt and innovate to drive the UK's cyber resilience, not only in the coming year but for the rest of this decade and beyond.



Lindy Cameron became the NCSC's second Chief Executive Officer in October 2020 replacing Ciaran Martin. Ciaran helped to set up the NCSC and acted as CEO from its inception in 2016, after having previously acted as the GCHQ Board Member responsible for cyber security since 2013. On leaving the NCSC, Ciaran has taken up an appointment as a Professor of Practice in Public Management, based at the Blavatnik School of Government at Oxford University. Lindy joins the NCSC with over two decades of experience in national security policy and crisis management, serving the Government at home and overseas, most recently as Director-General at the Northern Ireland Office.

12 month timeline



September 2019 – August 2020

29.11
NCSC Guidance: Downloadable copies of cyber security information cards for schools

12.12
UK General Election – the NCSC works to safeguard the election and protect the Register to Vote site

22.01
NCSC Guidance: Mobile Devices – advice for organisations in procurement and employee use of mobile devices

10.02
The NCSC welcomes opening of the Northern Ireland Cyber Security Centre

Dec

Jan

2020

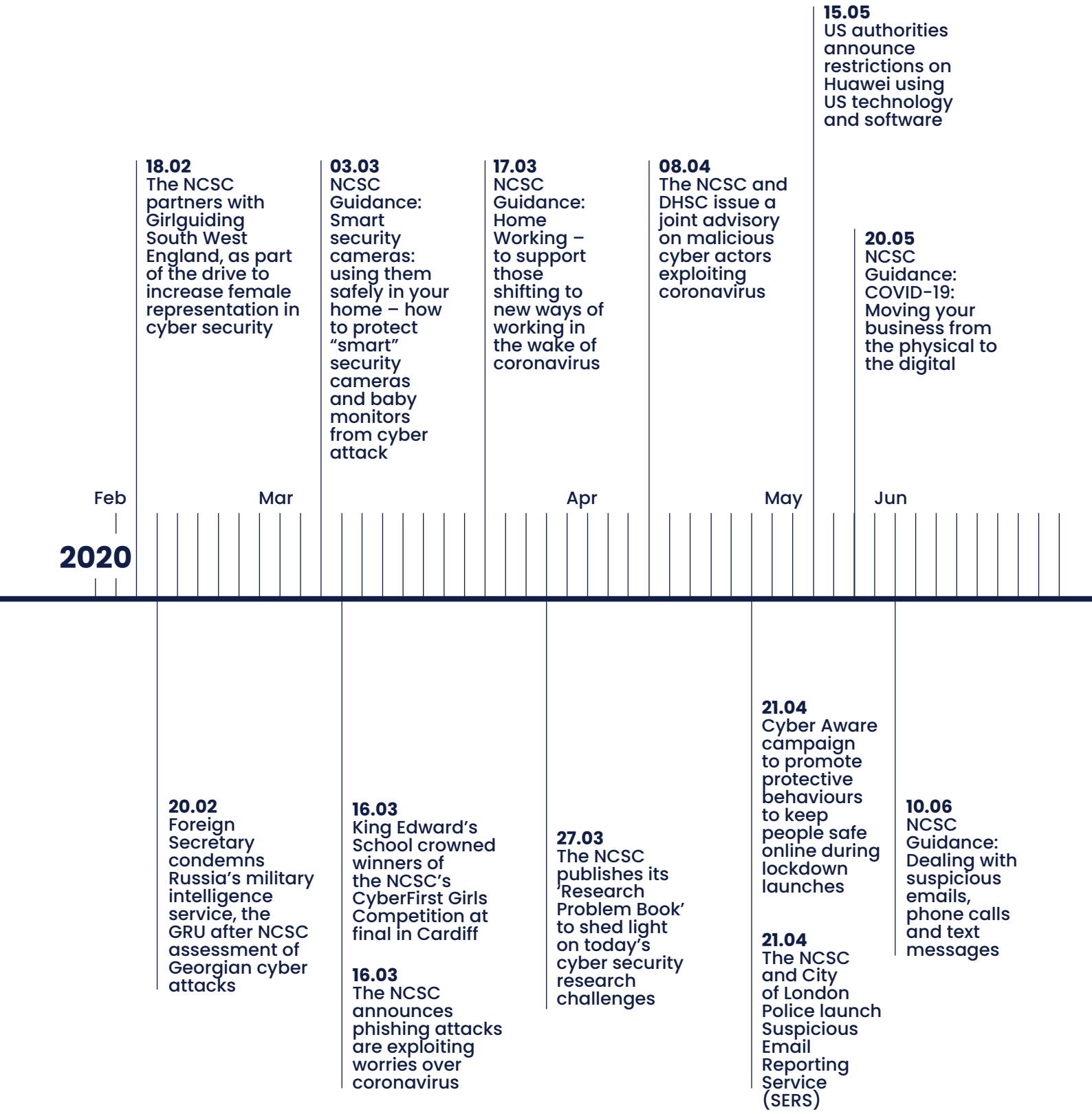
Feb

03-04.12
NATO Heads of State and Government meeting, London – former NCSC CEO Ciaran Martin takes part in NATO Engages event

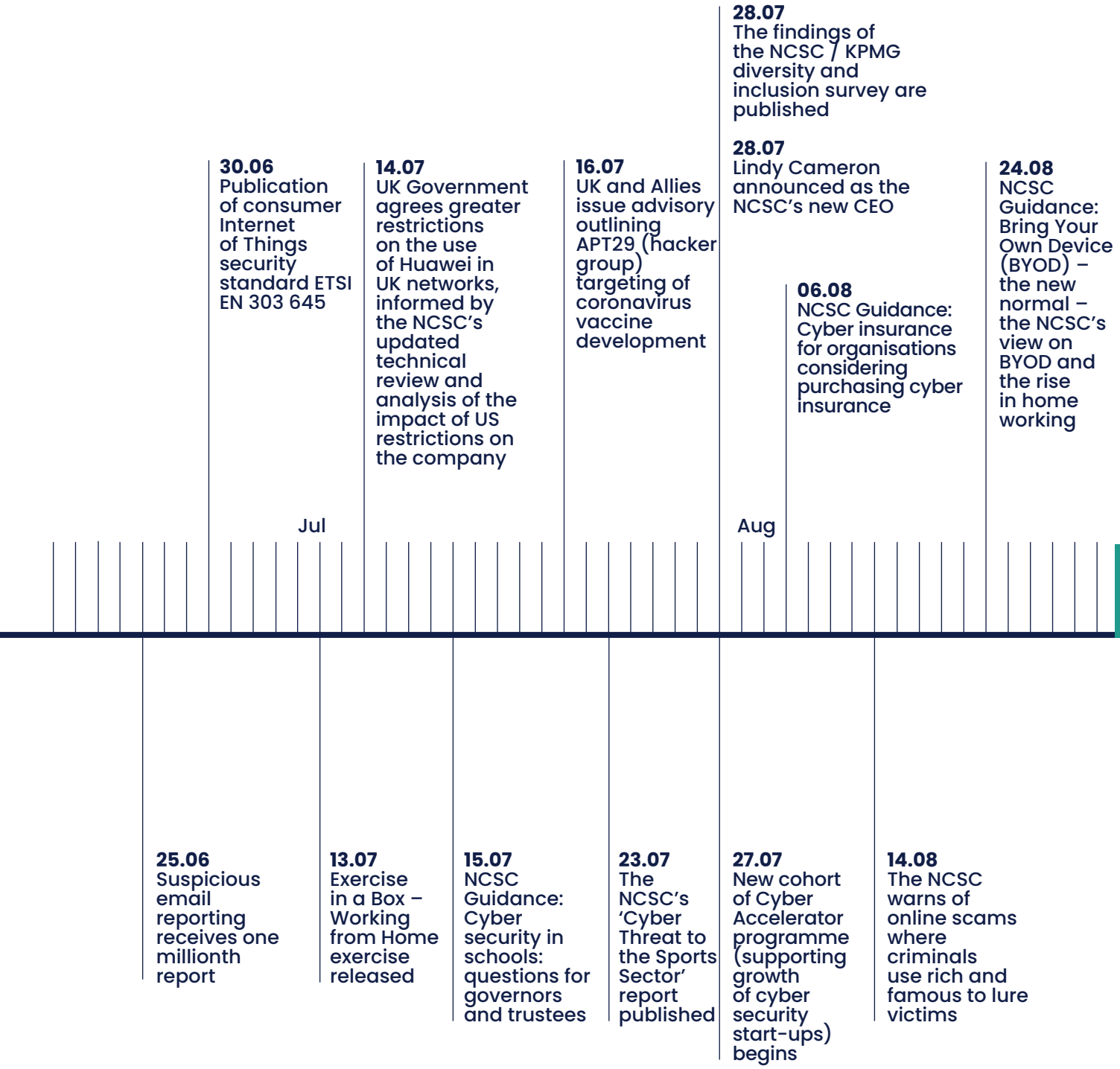
13.12
Cyber security advice for Members of Parliament and their staff published

28.01
UK Government announces plans to exclude high risk vendors from "core" parts of 5G and full-fibre networks

12 month timeline



September 2019 – August 2020



NCSC year four highlights



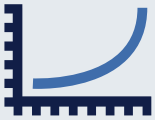
Handled **723** cyber security incidents



2.3 million suspicious emails forwarded to new SERS



Provided support to almost **1,200** victims



2.7 million visitors to the NCSC's website



Discovered and took down **166,710** phishing URLs, **65.3%** of which were removed within **24 hours**



Produced **30** pieces of guidance and **60** blogs



Produced **414** threat assessments



Awarded **17,100** Cyber Essentials Certificates

Produced **101,747** physical items for **140** customers through the UK Key Production Authority (UKKPA)

Visited and welcomed visiting delegations from over **20** countries

Engaged with **1,770** young people in the **2020** CyberFirst summer courses

Added almost **2,953** new members onto the NCSC's Cyber Security Information Sharing Partnership (CiSP)

Delivered more than **100** workshops, podcasts and webinars all over the UK for the voluntary sector

Hosted **101** events, with more than **4,602** attendees



Jeremy Fleming, Director GCHQ

"The world changed in 2020 and so did the balance of threats we are seeing. As this Review shows, the expertise of the NCSC, as part of GCHQ, has been invaluable in keeping the country safe: enabling us to defend our democracy, counter high levels of malicious state and criminal activity, and protect against those who have tried to exploit the pandemic. The years ahead are likely to be just as challenging, but I am confident that in the NCSC we have developed the capabilities, relationships and approaches to keep the UK at the forefront of global cyber security."


BUG NO3

1

Coronavirus – Responding to the pandemic

Much of the NCSC's work this year revolved around the coronavirus outbreak, which required a government-wide response. The NCSC's multi-faceted role included giving advice to an increasingly digitally active and dependent public, fixing vulnerabilities and responding to threats emanating from the pandemic.

The NCSC's proactive measures to defend the UK from coronavirus-related threats fell into five strands of work:

1. **Building NHS Resilience**
2. **Protecting vaccine and medicine research**
3. **Supporting remote working and tackling cyber crime**
4. **Securing the NHS Covid-19 app and large-scale data**
5. **Supporting Essential Service Providers**

Responding to the pandemic: the facts

7
Worked closely with the Centre for Protection of National Infrastructure (CPNI) on the secure build of seven Nightingale hospitals

160+
More than 160 instances of high-risk and critical vulnerabilities shared with NHS Trusts

200+
More than 200 incidents the NCSC responded to this year related to the UK's coronavirus response

230
Victims supported by the NCSC who faced incidents that were related to coronavirus

235
Rolled out Active Cyber Defence (ACD) services, including Web Check, Mail Check and protective DNS, to 235 front-line health bodies across the UK, including NHS Trusts

1,283
Engaged with over 1,200 ESPs across the UK to outline available NCSC guidance and support

51,000
Total number of Indicators of Compromise (IoCs) shared with the NHS

1 million
Scanned more than one million NHS IP addresses to detect security weaknesses

1.4 million
Performed threat hunting on 1.4 million NHS endpoints to detect suspicious activity

260
Blocked 260 SMS Sender IDs which were likely to or have been used in malicious SMS campaigns with coronavirus as their theme, such as spoofing legitimate government or healthcare IDs

15,000
More than 15,000 coronavirus-related malicious campaigns taken down by the NCSC and its commercial partner, Netcraft

Building NHS resilience

During the pandemic, protecting healthcare was the NCSC's top priority, and the organisation worked ceaselessly to support the NHS. The national objective was clear: to keep the system and its staff secure and resilient to cyber threats.

To achieve this, the NCSC introduced measures including the design of a new back-up service, pioneering discovery tradecraft and deploying analysts to look at NHS threat data. This was facilitated by the Department of Health and Social Care (DHSC) signing a "Direction" giving the NCSC consent to check the security of NHS IT systems.

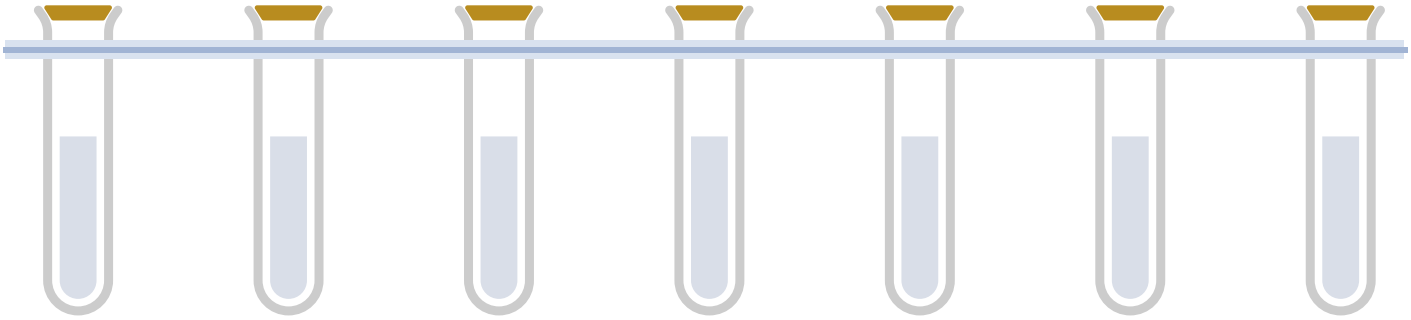
As a result, more than one million NHS IP addresses were supported, over 160 high-risk and critical vulnerabilities were identified and shared, and threat hunting performed on 1.4 million endpoints. The NCSC supported the health sector through cyber security incidents, and ACD services were put in place to protect more than 235 NHS units, including Trusts.



Protecting vaccine and medicine research

Support to vaccines and therapeutic medicines was a clear priority for the summer. The NCSC supported the Government's Vaccine Taskforce, which controlled decision-making on research funding and purchasing through to manufacturing and distribution, universities and pharmaceutical companies.

Work on vaccines and therapeutic medicines was an important supply chain component – particularly when it came to manufacture and distribution – and this work will continue as an integral part of the NCSC's mission.



Russian espionage

In July, the NCSC revealed Russian cyber actors, known as APT29, had been targeting organisations involved in coronavirus vaccine development. The NCSC assessed that APT29, also named "The Dukes" or "Cozy Bear", almost certainly operated as part of Russian intelligence services.

An advisory published by the NCSC outlined a variety of tools and techniques, including spear-phishing and custom malware known as "WellMess" and "WellMail" were being used to steal valuable intellectual property. This not only exposed the hostile action directly but also demonstrated to a wide range of pharmaceutical companies that they needed to understand more about protecting themselves.

The assessment, which received global interest, was supported by partners at the US Department for Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) and National Security Agency (NSA), and the Canadian Communication Security Establishment (CSE).

Rt Hon Dominic Raab, MP, First Secretary of State and Secretary of State for Foreign, Commonwealth and Development Affairs

"It is completely unacceptable that the Russian Intelligence Services are targeting those working to combat the coronavirus pandemic.

"While others pursue their selfish interests with reckless behaviour, the UK and its allies are getting on with the hard work of finding a vaccine and protecting global health.

"The UK will continue to counter those conducting such cyber attacks, and work with our allies to hold perpetrators to account."

Paul Chichester, NCSC Director of operations

"We condemn these despicable attacks against those doing vital work to combat the coronavirus pandemic.

"Working with our allies, the NCSC is committed to protecting our most critical assets and our top priority at this time is to protect the health sector.

"We would urge organisations to familiarise themselves with the advice we have published to help defend their networks."

Sharing threat information with the NHS

Indicators of Compromise are pieces of data which identify potentially malicious activity on a system or network. These help detect and mitigate threat activity. Before the NCSC created the IoC Machine last year, it took several hours for officials to share information relating to threats in the UK. The IoC machine made it possible to identify what can be shared in a matter of seconds – meaning the NCSC can share more threat information in real time.

With the improved ability to share IoCs and the need to protect the health and associated sectors during the pandemic, the NCSC exponentially increased the number of potential compromises tips to the NHS – with 51,910 shared by the end of August.

The shared IoCs were collated from the NCSC's own declassified sources and from its Industry 100 (i100) secondees from threat intelligence organisations. These i100 contributions were significant and valuable, complementing the NCSC's own collections and providing additional mitigation effects for the health sector. Secondees have worked alongside NCSC analysts to triage and investigate all IoCs before release, to ensure accuracy, validity and quality.

Since March, the NCSC has shared more than 200,000 IoCs with the Protective Domain Name Service (PDNS) and other domestic and international partners. Enhancements to the IoC Machine since its launch have enabled wider sharing of IoCs. A feature called 'Connected Communities' empowers partners directly connected to the IoC Machine to share IoCs within in their community or sector – subject to established information sharing protocols within the Critical National Infrastructure (CNI). In this way, the NCSC is realising the vision of the Cyber Defence Ecosystem, to get the right information to the right place and at the right time.

Supporting remote working and tackling cyber crime

When many organisations moved to remote working because of coronavirus, the NCSC responded with new guidance on how to help employees work and communicate securely from home, including those who needed to use their personal IT for work.

The NCSC published advice for organisations moving their business online at pace. Advisories were issued about how cyber criminals were seeking to exploit the pandemic for profit, and guidance was updated on how to spot and deal with suspicious emails, calls and texts (including coronavirus-based scams).

The pandemic led to a huge increase in employees working from home, with many making rapid adjustments to their new "office" and learning new skills, such as coping with intermittent Wi-Fi, or handling the etiquette of virtual meetings on Zoom, Microsoft Teams or Skype. With more people using personal devices for work purposes came an increased vulnerability to cyber fraud, as criminals sought to exploit the changing circumstances. Some scams, frequently using phishing emails, claimed to have a "cure" for coronavirus, or sought donations to bogus medical charities. Many users found that clicking a bad link led to malware infection, loss of data and passwords.

The NCSC published advice for UK organisations on how to reduce the risk of attack on devices, and how to deal with suspicious emails, texts or phone calls. The guidance recommended steps in such areas as setting up new accounts for employees, controlling access to corporate systems, and helping staff to ensure their equipment was cyber secure.

The NCSC also assisted the Government Security Group (GSG) and the Government Digital Service (GDS) in providing advice to allow civil servants to access official IT when working remotely, and issued guidance for best practice in BYOD. This involved working with GSG, GDS, Microsoft and Google to help organisations configure access to Office 365 and G Suite from personal devices.



Disrupting cyber crime

Cyber criminals look to exploit any vulnerability to generate income and coronavirus was no exception. The NCSC led the way throughout the pandemic to expose attack methods of those exploiting the situation online and to advise on ways to defend against them.

This year a significant proportion of attempted compromises was related to coronavirus – whether it was linking to bogus products or targeting people using their devices in a different way due to the pandemic.

The NCSC disrupted thousands of attempts to trick people, from fake lures of personal protective equipment (PPE), testing kits and cures and even sham key worker badges to activate supermarket discounts.



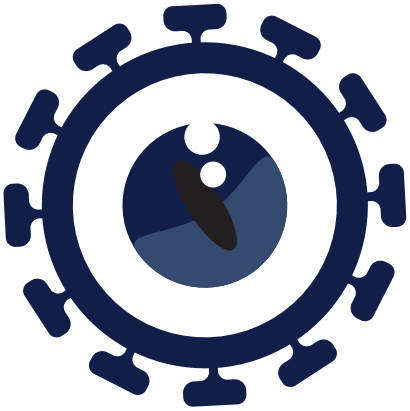
Nicky Hudson, NCSC Director of Policy & Communications

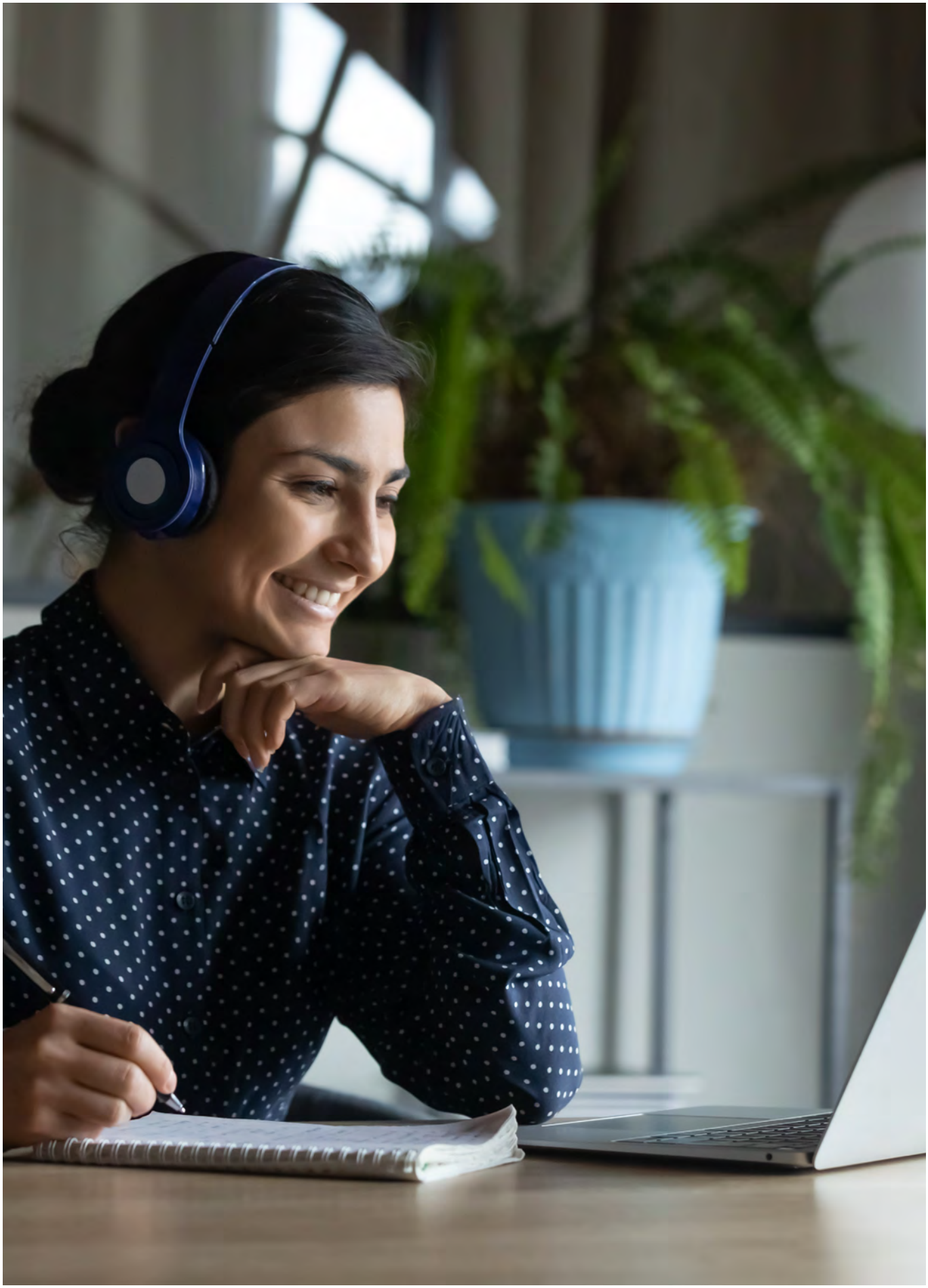
"We know that cyber criminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the coronavirus outbreak.

"Our advice to the public is to follow our guidance, which includes everything from password advice to spotting suspect emails.

"In the event that someone does fall victim to a phishing attempt, they should look to report this to Action Fraud as soon as possible."







Timeline of NCSC coronavirus-related interventions to support people and businesses

March

16.03
The NCSC reveals criminals carrying out phishing attacks using coronavirus-related products as a lure

17.03
New guidance published as home working increases

April

01.04
Organisations identified as ESPs sent bespoke communications on advice, support and preventative measures to help them with cyber security

08.04
Joint coronavirus threat advisory published with CISA (US) for individuals and organisations

21.04
'Cyber Aware' campaign launches to help protect citizens online during lockdown

May

Release of the SERS to combat fraudulent emails

04.05
The NCSC to supports DHSC on creation of NHS COVID-19 app

05.05
Joint UK and US advisory on APT groups targeting healthcare services

June

25.06
One millionth public report received into the SERS

July

13.07
'Home and remote working' scenario added to Exercise in a Box toolkit

16.07
UK and allies expose Russian attacks on coronavirus vaccine development

August



Securing the NHS Covid-19 app and large-scale data

The NCSC supported the NHS Test and Trace programme, the work of the Joint Biosecurity Centre (JBC) and the development of the NHS COVID-19 app to help curb the spread of the coronavirus.

The NCSC's role

- Ensuring NHS teams had the information they needed to make decisions affecting users' privacy and data security, including integrating a senior security architect to be the app's Chief Information Security Officer
- Advising on cyber security best practice and how to implement it, helping the NHS teams to use the NCSC's cyber security design principles as a guide
- Maintaining transparency and openness with the public about the privacy and security decisions made by the NHS, by posting blogs on the NCSC website during development and to accompany trial and national launches
- Soliciting feedback from the cyber security community on the app, using the NCSC's existing HackerOne Vulnerability Disclosure Programme (VDP) to gather input from outside experts
- Testing the efficacy of contact tracing using Bluetooth in lab and real-world scenarios

Threat modelling

A key area of the NCSC's support was supporting the threat modelling used by developers, helping them to understand the risk to the app from external threats, and the potential implications of their security and privacy decisions. The NCSC ran multiple threat modelling workshops and supported the use of a consistent approach across the project, using the STRIDE model (Spoofing, Tampering, Repudiation, Informal disclosure, Denial of service, Elevation of privilege). This model helped the NHS team implement more security measures in the app to support users' privacy, data security, and resilience against misuse / abuse.



Matthew Gould, Chief Executive Officer, NHSX

"The NCSC's support during a time of unprecedented pressure on the NHS has been invaluable. The close working between NHSX, NHS Digital and the NCSC has let us have the maximum impact improving the NHS's cyber resilience with minimum burden on the NHS frontline."

The balance of privacy and utility

The NCSC also supported the NHS to find the right balance between user privacy and utility. For example, the NCSC advised on the optimum level of analytical data collected so as not to de-anonymise users, but granular enough to provide meaningful insights into whether the app worked. Based on these discussions, the app team selected a minimum set of metrics which were chosen to fulfil the requirements – including postal district, isolation status and number of location check-ins. Where even these metrics could identify users, for example, postal districts with small populations, the analytics are aggregated into larger sets to reduce the risk of users becoming identifiable from the information they provide.

Privacy-preserving system architecture

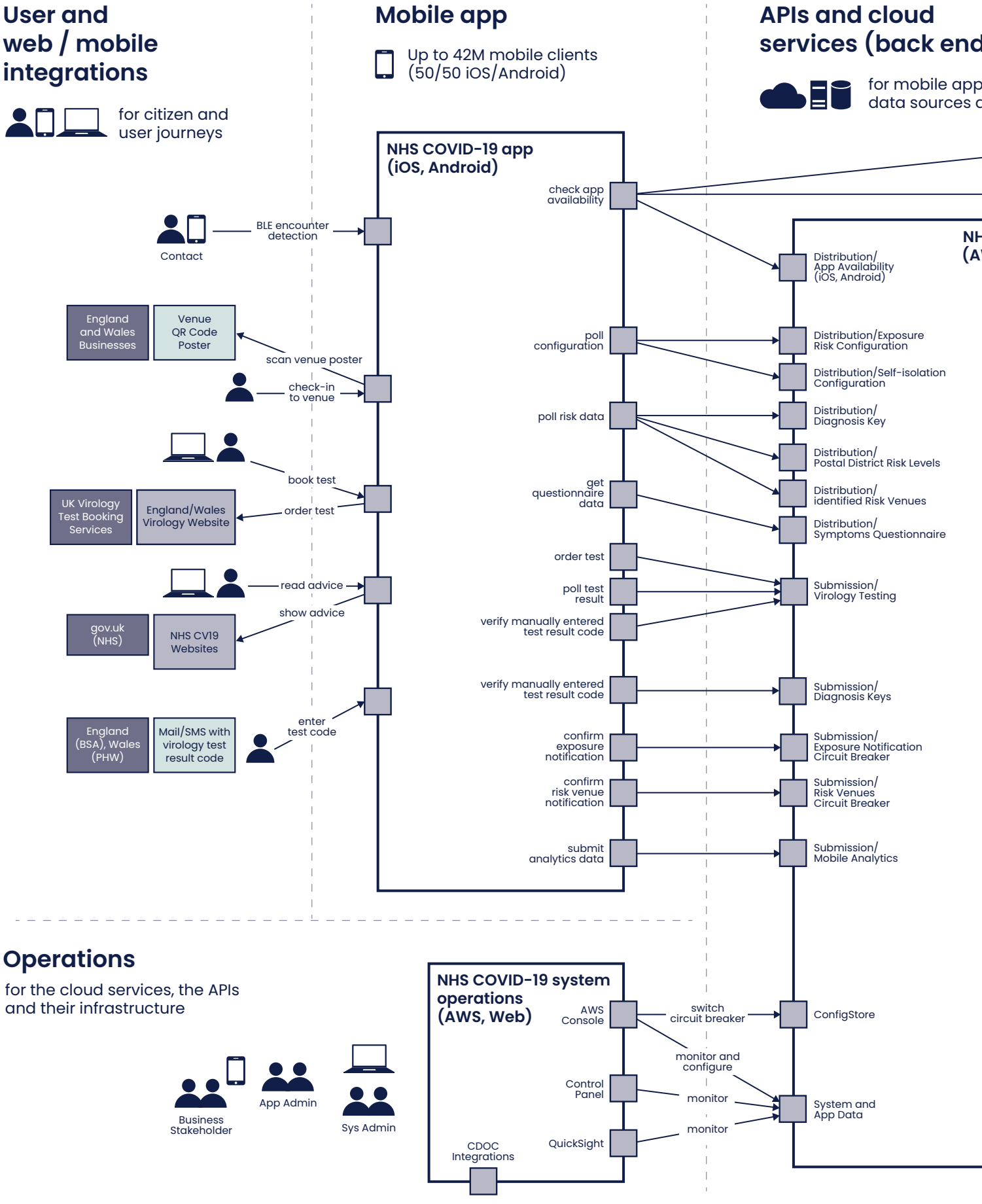
The app architecture, detailed in the graphic below, was designed to be privacy-preserving – no user state or identifiers are stored in the cloud.



Dr Ian Levy, NCSC Technical Director

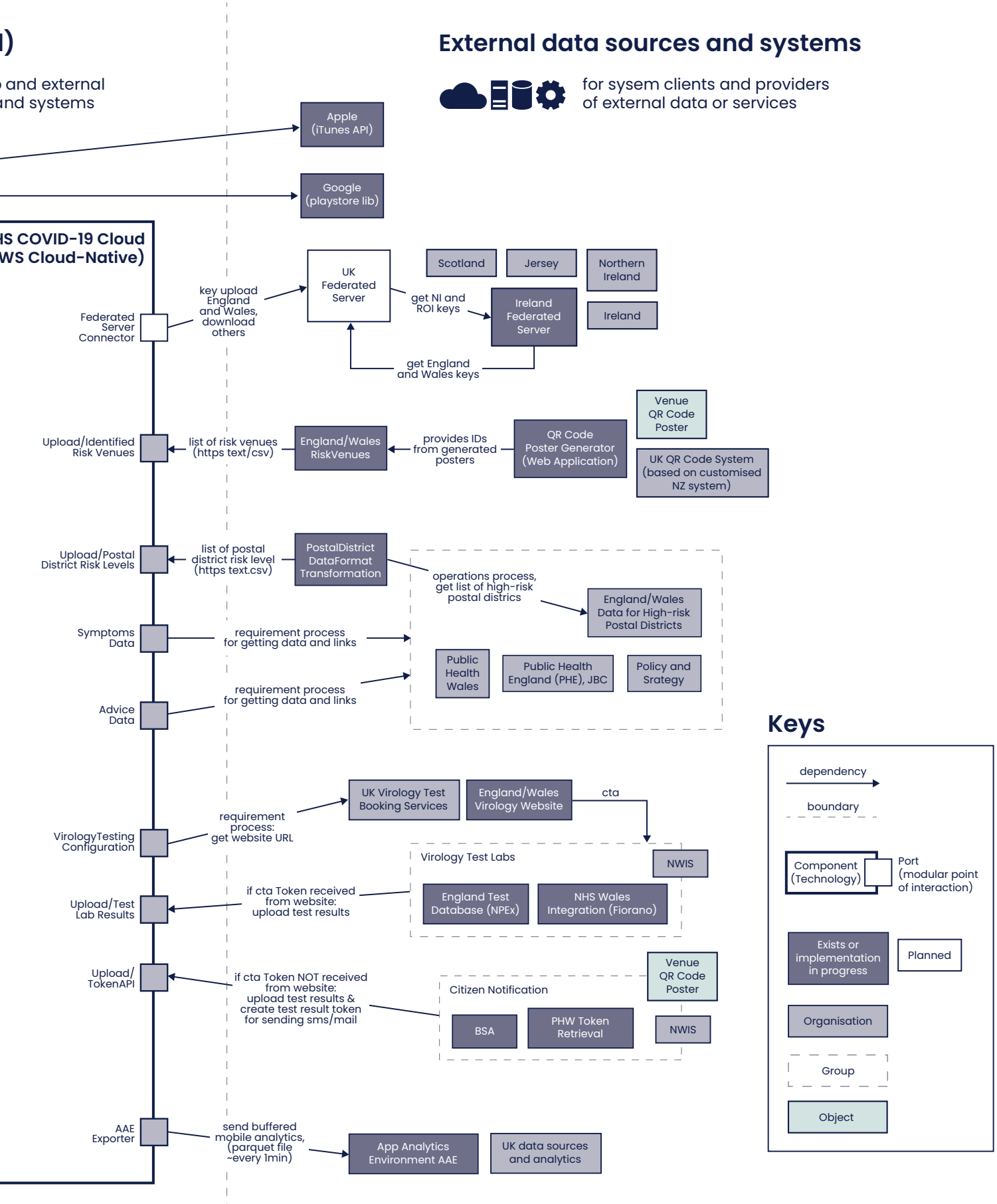
"This is an example of how we deploy our high-end security architects to key projects in government to ensure that security is at the heart of its systems."

As well as supporting the UK Government and agencies in England, the NCSC also worked with the Devolved Administrations and some Crown dependencies. This included providing technical advice to the Northern Irish and Scottish contact-tracing apps and advising on secure interoperability between the England and Wales app.


User and web / mobile integrations
for citizen and user journeys
Mobile app
Up to 42M mobile clients (50/50 iOS/Android)
APIs and cloud services (back end
for mobile app data sources
NHS COVID-19 app (iOS, Android)
check app availability
Contact
BLE encounter detection
England and Wales Businesses
Venue QR Code Poster
scan venue poster
check-in to venue
book test
UK Virology Test Booking Services
England/Wales Virology Website
order test
read advice
show advice
gov.uk (NHS)
NHS CV19 Websites
England (BSA), Wales (PHW)
Mail/SMS with virology test result code
enter test code
poll configuration
poll risk data
get questionnaire data
order test
poll test result
verify manually entered test result code
verify manually entered test result code
confirm exposure notification
confirm risk venue notification
submit analytics data
Distribution/ App Availability (iOS, Android)
Distribution/Exposure Risk Configuration
Distribution/Self-isolation Configuration
Distribution/ Diagnosis Key
Distribution/ Postal District Risk Levels
Distribution/ identified Risk Venues
Distribution/ Symptoms Questionnaire
Submission/ Virology Testing
Submission/ Diagnosis Keys
Submission/ Exposure Notification Circuit Breaker
Submission/ Risk Venues Circuit Breaker
Submission/ Mobile Analytics
Operations
for the cloud services, the APIs and their infrastructure
NHS COVID-19 system operations (AWS, Web)
AWS Console
switch circuit breaker
ConfigStore
monitor and configure
Control Panel
monitor
System and App Data
QuickSight
monitor
CDOC Integrations
Business Stakeholder
App Admin
Sys Admin

External data sources and systems

for sysem clients and providers of external data or services

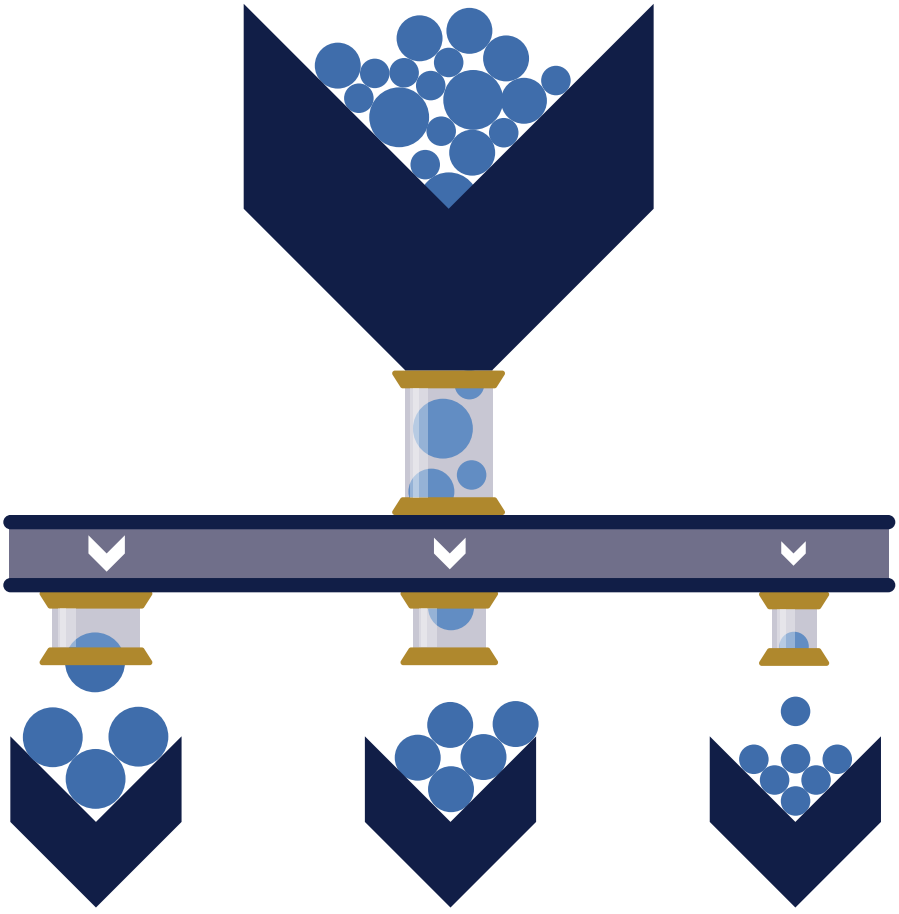


Support for the coronavirus large-scale data processing environments

To support the NHS and the Government's virus mitigation needs, there were considerable efforts from departments to rapidly process data from multiple sources, and the NCSC helped to ensure data processing environments were secure.

These environments included systems used by health and social care facilities to help predict demand on services in geographic areas, and the JBC to join data together from multiple open and commercially available data sources.

The NCSC's security experts advised on how to ensure processes were properly protected and able to produce the reliable data needed to inform key policy and operational decisions.



Supporting Essential Service Providers

What are ESPs?

- ESPs are public, private and third sector organisations essential to the UK's response to the coronavirus crisis
- They cover a wide range of areas including online supermarkets, haulage companies, ventilator manufacturers, healthcare suppliers, supply chain companies and charities
- They also include existing CNI partners such as communications, energy and financial organisations

How were they identified by the NCSC?

- At the start of the coronavirus outbreak the NCSC worked with government departments to identify and map ESPs
- Those already engaged with the NCSC were contacted, then the team worked with central government, trade associations and other organisations to bring together a portfolio of contacts
- The NCSC repurposed its CNI Knowledge Base, which maps the UK's national infrastructure, to help government understand the interdependencies and connections between ESPs in certain sectors

What support were they given?

- 17 new items of guidance and a range of additional engagement material were produced to advise on the actions needed to reduce the risks of cyber attacks
- The NCSC liaised with 1,283 ESPs – enabling them to reach out to hundreds of additional supplier companies
- Incidents and cyber enquiries were managed and findings fed back into the NCSC's products
- This work resulted in products being created to help the change in operating and working environment such as the 'moving your business from physical to digital' publication
- Bespoke offers of support were provided, such as the Cyber Essentials offer to small and medium sized businesses supporting healthcare



2

Defending democracy

This year the NCSC played a bigger role than ever in defending the UK's democratic processes and institutions.

While defending democracy from cyber threats has always been a key priority, the unique challenges produced by a general election and the introduction of a "virtual Parliament" meant cyber security was never more important in UK politics.

Virtual Parliament

The coronavirus pandemic changed the way millions of people worked, including Parliamentarians. The solution to enable MPs and peers to carry out their functions came through technology, and the NCSC and the Parliamentary Digital Service were central to delivering what was arguably the biggest ever change to how Parliament operates.

The challenge

Democracy relies on elected representatives meeting to debate, scrutinise and vote but restrictions on movement and contact meant MPs and peers were unable to do so in Parliament. Solutions had to be rapidly implemented to ensure Parliamentarians returning after Easter recess could conduct their business at a time when crucial decisions were being taken in Westminster.

Virtual debates

Technology was rapidly developed to allow Parliamentarians to debate from remote locations in a secure setting. This meant in addition to the 50 MPs allowed into the Commons, a further 120 were able to participate online.

To counter the risk that hackers and online intruders could disrupt proceedings, the NCSC worked with Parliamentarians to upgrade awareness and training in cyber security. It provided advice to ensure the new system had the right balance of security controls to mitigate the threat posed by cyber criminals, while safeguarding important conventions and privileges.

Remote divisions

For centuries, voting in Parliament has been done in a very specific way: through the provision of physically entering one of the two lobbies on either side of the chamber to cast their vote.

With most MPs not in the chamber, a digital solution was required to allow votes to be cast remotely. A new system was built with multiple checks, to ensure a high level of confidence in the votes being cast.

Working together

The NCSC was just one part of a broader team that worked together to deliver virtual Parliamentary proceedings.

Broadcasters, Parliamentary digital staff and staff across both Houses at Westminster collaborated to ensure appropriate cyber security controls were in place.

Virtual Parliament in session



Stephen Timms, Labour MP for East Ham

"The Work and Pensions Select Committee, which I chair, was able to continue its work without interruption, during lockdown with members and witnesses participating mainly remotely.

"We have been able to question Ministers and officials virtually, holding them to account for their actions during the pandemic. I greatly appreciate the work of the NCSC in making this possible."

John Nicolson, SNP MP for Ochil and South Perthshire

"I have been impressed with the speed and efficiency with which remote Parliamentary working was arranged. I've found that contributing by Zoom has worked well, and remote voting was quick and effective."

Sir Lindsay Hoyle, Speaker of the House of Commons

"The House of Commons has been operating in more or less the same way for more than 700 years – so it was quite incredible that we were able to change our modus operandi within a few weeks.

"With great ingenuity, the in-house Broadcasting Unit and Parliamentary Digital Service, aided by security advice from the NCSC, introduced hybrid proceedings, which allowed many MPs to join by video link, with only 50 allowed in the chamber under social distancing rules. Remote voting – which helped the House through the height of the crisis – was superseded by pass-reader voting. While no one could have anticipated the changes that have had to be made to see the House through this pandemic, the one positive that can be taken away is that the organisation is better prepared for an emergency of this type than ever before."

Dame Cheryl Gillan, Conservative MP for Chesham and Amersham

"Asking questions on the floor of the House, participating in the Public Accounts Committee, Chairing the All Party Parliamentary Group on Autism, holding remote surgeries with constituents, holding team meetings with my staff and Chairing the Political Affairs and Democracy Committee of the Council of Europe have all worked perfectly using Microsoft Teams, Zoom and Kudo (internationally).

"The technical work, carried out at pace, that has permitted this remote connectivity has preserved our democracy at this crucial time and the Parliamentary Digital Service and the NCSC have ensured that vital continuity and security of the "Mother of Parliaments" by enabling its ongoing scrutiny of the Executive."

The 2019 General Election

Protecting the UK's electoral processes is one of the most important objectives of the NCSC. Supporting this aim sees the organisation working all year round – offering expert cyber security guidance and advice – to support political parties and parliamentarians. As part of the NCSC's preparation the organisation monitored developments in the lead up to the vote and worked with international partners to learn from their experiences in mitigating the risk of cyber attacks against national ballots. During the election, the NCSC responded to a wide range of incidents, working behind the scenes to triage threats, investigate leads and providing advice and assistance where required.

Protecting the Register to Vote website, the NCSC supported the resilience and security of the online platform to allow citizens to access or update their details on the electoral register. The NCSC's experts worked closely with the Register to Vote team at the Cabinet Office to review the site's ability to withstand peaks in traffic.

On average, the Register to Vote website receives around 25,000 daily online submissions, but on 25 November, there was an unexpected spike in interest and the site received 366,000 applications.

Thanks to the groundwork done to ensure resilience, the service remained stable, despite the considerable increase in load, ensuring record levels of registrations.

Distributed denial of service (DDoS) attacks

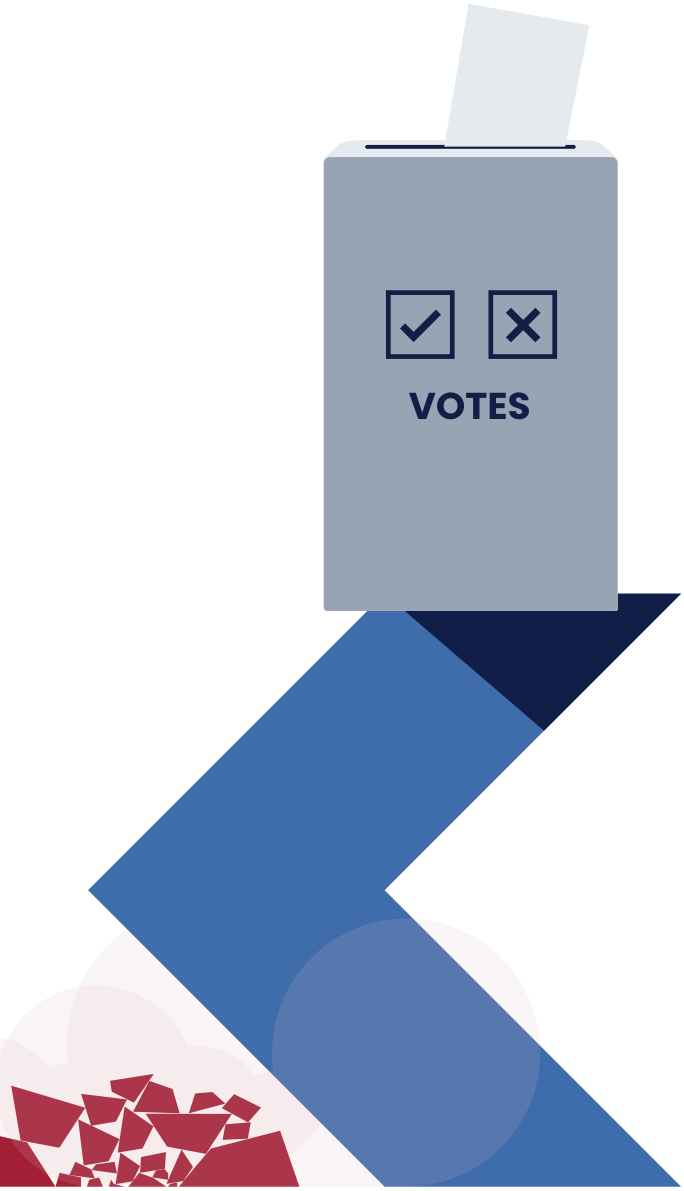
Prior to the dissolution of Parliament, the NCSC hosted a seminar with the UK's Parliamentary parties to brief them on the cyber security threat and the steps they could take to protect themselves.

Early in the campaign, a series of Distributed Denial of Service (DDoS) attacks against political party websites became a major story. Whilst these were relatively low-capability attacks, the timing was concerning.

The fact that these attacks were largely unsuccessful was a testament to the preparation done by the parties affected to defend themselves. The NCSC published relevant advice on its website and shared this guidance with the Parliamentary parties' IT teams.

Support to new MPs

After the election, the NCSC provided guidance on best practice for all new MPs to ensure they and their staff were cyber security aware. Specific guidance on how to respond to targeted phishing attacks was given by the NCSC's Incident Management (IM) team to more than 200 prominent figures – including government ministers.



Foreign interference

The UK Government is clear that any foreign interference in the UK's democratic process is completely unacceptable, but certain states seek to exploit elections through cyber attacks, disinformation and other methods.

The NCSC is working with the Government in taking forward a programme to ensure there are robust safeguards against hostile state activity, foreign lobbying activity and third parties seeking to interfere in democratic processes. The UK will continue to identify and respond to malign activity alongside NATO and international partners.

In a Written Ministerial Statement on 16 July 2020, the Foreign Secretary said that the Government was almost certain that Russian actors sought to interfere in the 2019 General Election.

Rt Hon Dominic Raab MP, First Secretary of State and Secretary of State for Foreign, Commonwealth and Development Affairs

"On the basis of extensive analysis, the Government has concluded that it is almost certain that Russian actors sought to interfere in the 2019 General Election through the online amplification of illicitly acquired and leaked government documents.

"Sensitive government documents relating to the UK-US Free Trade Agreement were illicitly acquired before the 2019 General Election and disseminated online via the social media platform Reddit. When these gained no traction, further attempts were made to promote the illicitly acquired material online in the run-up to the General Election.

"Whilst there is no evidence of a broad-spectrum Russian campaign against the General Election, any attempt to interfere in our democratic processes is completely unacceptable. It is, and will always be, an absolute priority to protect our democracy and elections."



Leaving the European Union

The NCSC's Digital Government team provided a wide range of information assurance services in support of the Government's European Union (EU) Exit plans.

This included providing advice on and reviewing multiple departmental cyber security health checks and penetration-testing reports to assess the potential vulnerability of these systems across the Government estate, reassuring the Cabinet Committee that risks were being managed.

The NCSC also played a key role in briefing government trade negotiation teams on their communications security, and potential threats from the UK and overseas. With coronavirus forcing some of this online, in collaboration with GSG and GDS, the NCSC provided guidance on the safe use of video conferencing systems and carried out reviews to provide assurance to delegations before their engagements.

The NCSC briefed the UK representation in Brussels on cyber risks and security advice in an increased threat profile around EU Exit negotiations.

The NCSC supported the Cabinet Office and HMRC in building security into new systems designed to monitor the near real-time flow of goods across the UK border after EU Exit. This contributed to the decision to proceed with proof of concept trials.

Offering dynamic cyber solutions to government

Through guidance and training, the NCSC helps improve the level of cyber resilience in national and local government, ensuring that the public sector can rely on secure access to essential services, networks and data.

This year the NCSC:

- Provided advice as part of the 'One Government Cloud Strategy', which will allow for unprecedented cross-organisational collaboration
- Designed a new protocol which uses novel cryptography to allow public services to query sensitive databases on the cloud
- Supported HMRC with the introduction of coronavirus-related services including Job Retention, Self-Employment Income Support and the Statutory Sick Pay Rebate Scheme
- Oversaw the secure delivery of data from departments as part of support to the Office of National Statistics in preparation for next year's Census
- Provided guidance on how to risk manage employees using IT devices while working from home and mitigated cyber security vulnerabilities in government departments' systems

The Cyber Centre of Excellence is a government security initiative to help improve cyber security advice across departments. The Centre has played a vital role in helping departments to implement the NCSC's ACD capabilities, conducting risk analysis to address vulnerabilities and to improve cyber resilience across government.

Advanced Mobile Solutions

With government needing its personnel to be able to work remotely and securely on mobile devices, the NCSC's Advanced Mobile Solutions (AMS) has given authorised users protected access to the most sensitive networks.

This year to ensure the safe connection between less secure remote devices to secret networks, AMS created new classes of "cross domain" technology, using highly innovative infrastructure security. The new approach has enabled methods of secure communication between individuals and groups, such as video conferencing, whether they are in protected facilities or working remotely. This provides a significant improvement in protection compared to standard security technology such as Web Application Firewalls.

Dr Ian Levy, NCSC Technical Director

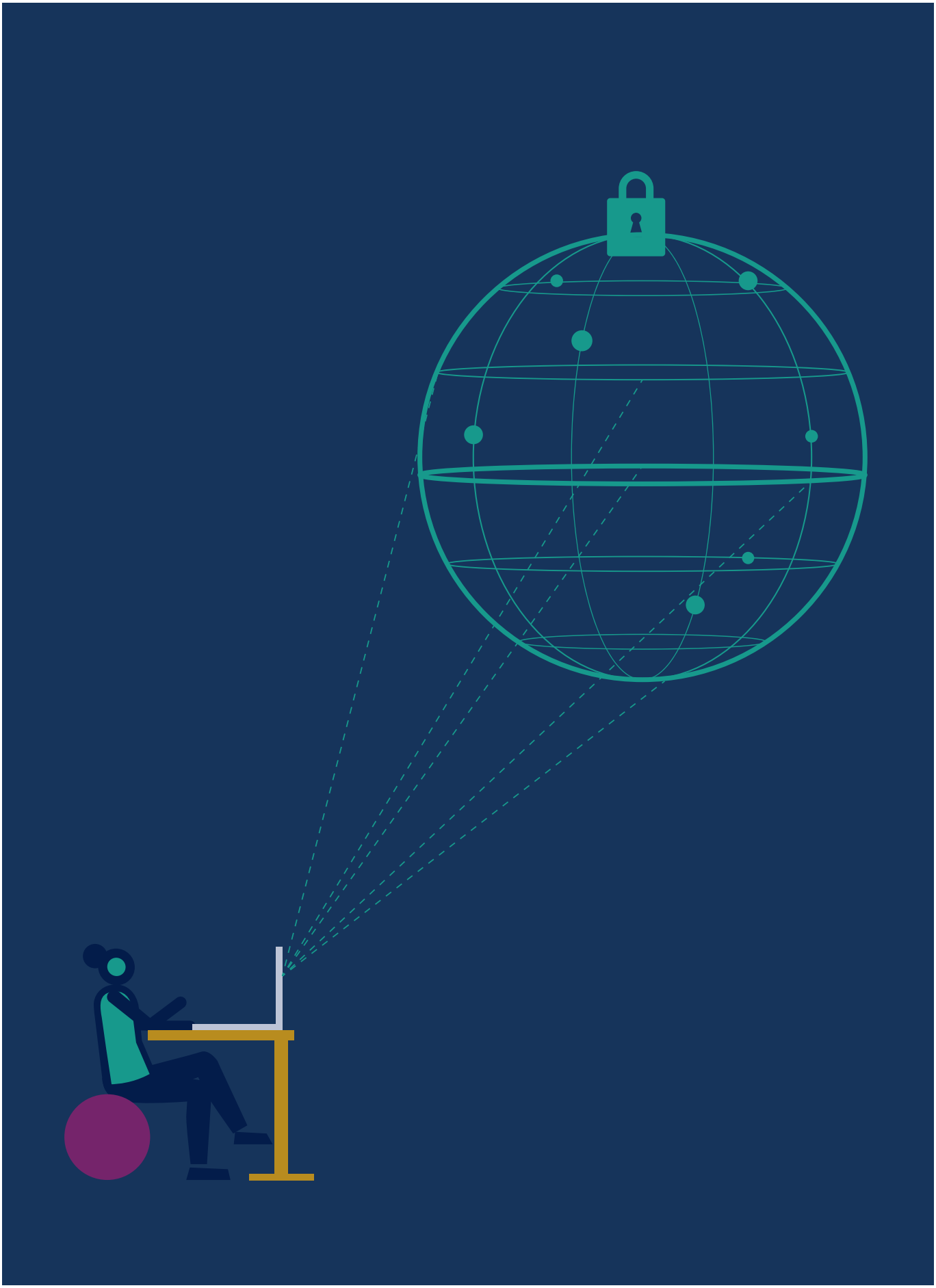
"Capabilities like AMS highlight both the very latest developments in cyber security and also the ability of highly sensitive departments to work in a modern way. The advances are the result of the NCSC's diligent research collaborations with our academic and industry partners."

Stephen Thomas, Head of Rosa GOST Team, Cabinet Office

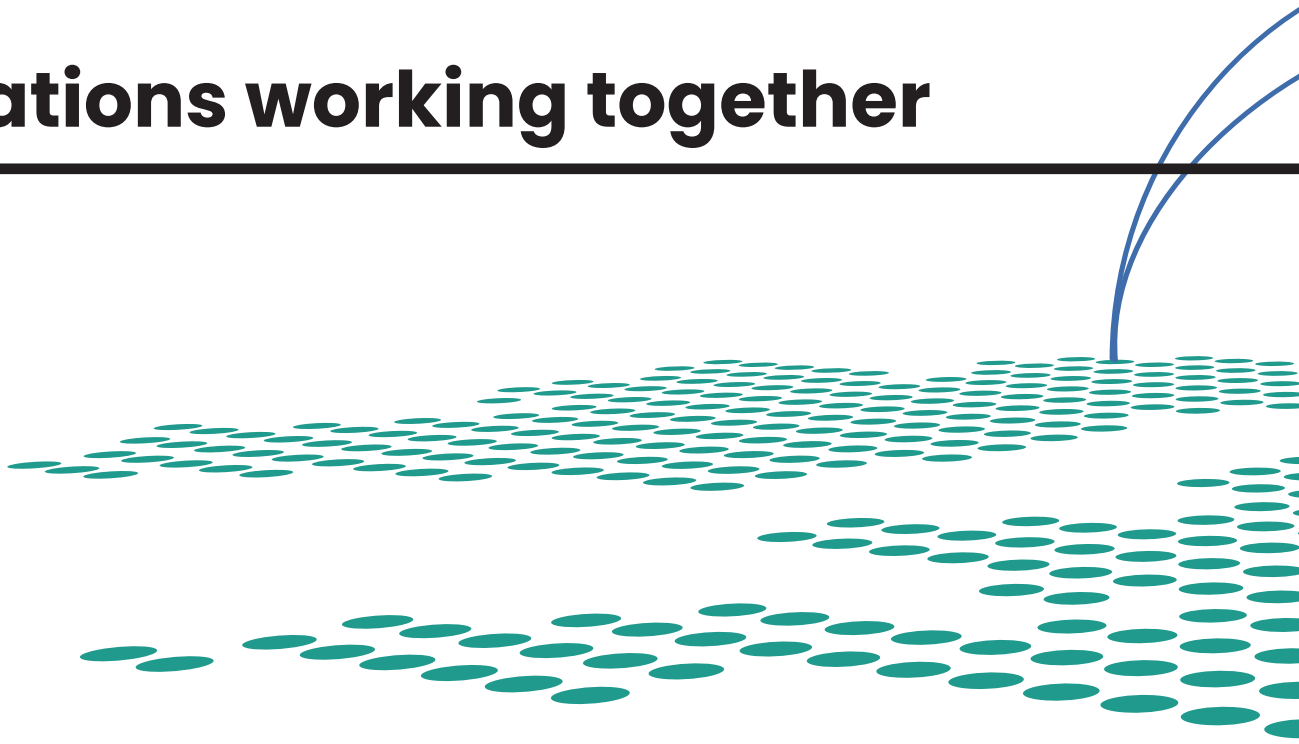
"The NCSC's Advanced Mobile Solutions, sponsored by Initiate, underpins the Cabinet Office's Rosa service and is transforming how HMG works.

"Through Rosa, several government departments and industry suppliers are now mobile working at above OFFICIAL – something we only expect to increase as the UK moves towards more distributed working."

- AMS and derived technologies are currently deployed to over 500 devices across multiple organisations
- The NCSC anticipates a significant increase in these numbers as a new managed service (initially scaled to 2,000 devices) comes online at the end of 2020 and new secure remote working systems, currently being built, come online in early to mid 2021



UK nations working together



Ignatius O'Doherty, Director of Digital Shared Services, Northern Ireland Department of Finance

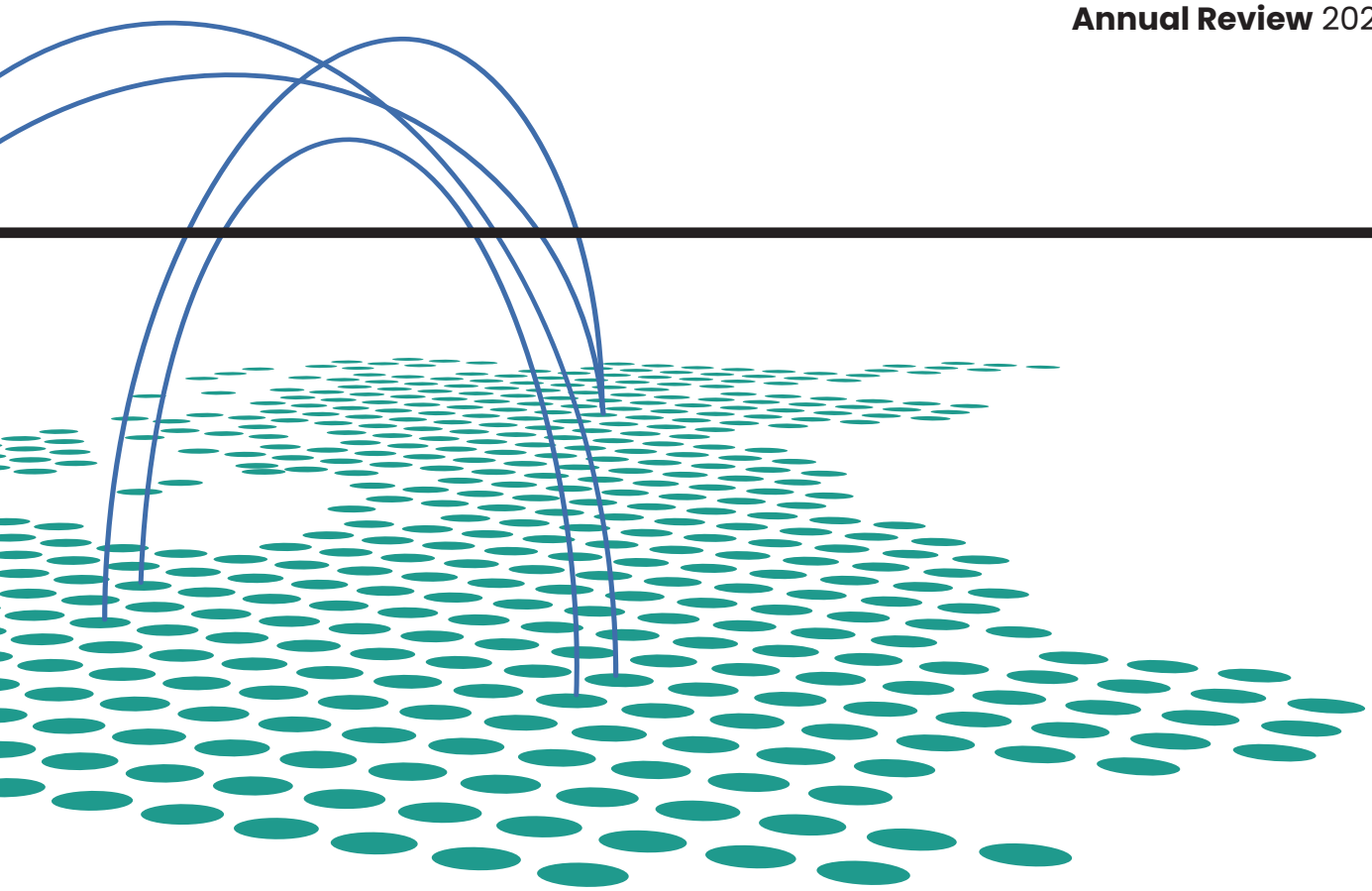
"The presence of the NCSC on Devolved Administration working groups has added real value to our work programmes by providing strategic direction and insight into key cyber interventions.

"The NCSC continues to deliver regular and timely threat assessment significantly enhancing our ability to identify and manage cyber risk.

"The NCSC's technical expertise regularly supports the analysis of security vulnerabilities and has provided specialised advice on technical aspects of a major procurement aimed at strengthening our cyber defences."

Clare El Azebbi, Head of Cyber Resilience Unit, Scottish Government

"The National Cyber Security Centre has provided excellent expertise, advice and support to the Scottish Government as we work towards making Scotland a world-leading nation in cyber resilience. We enjoy the positive and productive partnership we have with all parts of the NCSC and look forward to continuing this as we face the shared challenges ahead."



Welsh Government spokesperson

"(The NCSC's cyber skills initiatives for young people) have enhanced the awareness of cyber resilience and security with education stakeholders in Wales and through Hwb, the Welsh Government's information sharing platform for education. The Welsh Government looks forward to continuing to work with the NCSC to promote cyber opportunities that contribute to our ambition of developing digital resilience within our learners.

"We welcome the support given by the NCSC as we continue to boost cyber resilience in Wales, from increasing uptake of Active Cyber Defence across Wales to issuing grant awards to local authorities and the wider public sector in Wales for cyber security training for IT managers, plus funding to for councils to enhance cyber resilience in light of coronavirus."



3

Building a resilient nation

In response to the fast pace and ever-changing national and international security threats, the NCSC works through established partnerships to help make the UK as resilient as possible – from defending citizens, businesses and charitable institutions, to safeguarding Critical National Infrastructure , defence and security assets and operations.

Defence, security and resilience

The NCSC works closely with the Ministry of Defence (MOD) to ensure UK Armed Forces can operate with confidence based on reliable information shared safely with UK and international partners.

The UK's most sensitive information and most important capabilities are protected using the NCSC's Crypt-Key (an encryption management system), which is underpinned by the technical expertise the NCSC holds as the UK's technical authority on cyber security. The NCSC is committed to ensuring the MOD has the capability in this space it needs now and in the future.

Over the past year, the NCSC has worked with the MOD, NATO and other partners on the transformation that is required throughout the UK National Crypt-Key Enterprise and this vital collaboration will continue.



Jacqui Chard, NCSC Deputy Director, Defence and National Security

"At the NCSC, we are proud that our technical expertise helps to keep our armed forces safe and operating with confidence all around the world."

UK Key Production Authority

At the heart of the NCSC's security work is the expertise needed to create highly secure, encrypted communications for the government, military, industry and Allies. Its research on improving these systems has led to significant new developments in Crypt-Key, transforming old, paper-based practices into modern, digital ones.

This year, the UK Key Production Authority (UKKPA) - a part of NCSC - replaced the long-standing method of producing cryptographic keys on punched paper tape with a more efficient capability for producing and distributing keys in an electronic, highly secure format, meeting the advanced requirements of national and international defence partners.



Eight-hole punched paper tape example

Defence of the realm

The NCSC worked to protect military personnel and the nation's most important ground, naval and air assets, providing support with incident and threat reporting, and training for staff.

As part of this role, the NCSC provided advice on cyber security risks and policy to the Continuous At Sea Deterrent (CASD), including the mitigation of any potential supply chain vulnerabilities. Ongoing support is given to the Successor programme, which will deliver the replacement to the current Vanguard-class Trident Submarine.

The NCSC continued to support the UK's thought leadership in NATO, and technical expertise on cyber security and cryptography to help the organisation protect its communications and information infrastructure.

The NCSC led the development of NATO's action plan to protect its secure communications against the threat from future quantum computing and is providing ongoing assistance to the organisation's implementation of its plan.

HMS Vengeance, Vanguard-class submarine



Dr Ian Levy, the NCSC's Technical Director

"Protecting our most sensitive data and capabilities is something the NCSC is designed to do, using our world-leading cryptographic expertise and understanding of the threats from our adversaries."

General Sir Patrick Sanders, Commander of Strategic Command

"UK Strategic Command and the NCSC frequently work hand-in-hand to enhance Defence's security posture and in the fight to protect our networks and critical national information against constant attack.

"Cyberspace is the most active domain, and the NCSC delivers critical support to us in threat and incident management, high grade cryptography and in providing specialist support such as preparing for CSG21 (UK Carrier Strike Group 21) and the ongoing support to the strategic deterrent."

Poseidon Maritime Patrol Aircraft

The NCSC worked with the MOD on all cyber security aspects of the Boeing Poseidon P-8A Maritime Patrol Aircraft, which will offer a high level of sea defence to the UK due to its unique submarine-hunting capabilities.

Operating from RAF Lossiemouth, the aircraft successfully achieved its initial operating capability in April, contributing to maritime counter-terrorism, and will be able to support search and rescue operations worldwide.

Joint Strike Fighter

Defence's fleet of new F-35B combat aircraft was supported by the NCSC as it extends its operational ability with deployment into international areas of conflict. The NCSC provided TEMPEST testing, ensuring the highest level of secure communications, and was involved in the development of Lightning Shield to maintain operational security. The latter ensured the F-35B's Freedom of Action and is in operational use by the UK Lightning Force and Royal Australian Air force.

The NCSC continues to review the cyber security of the aircraft's international maintenance support and the rapid provision of the necessary key material to support carrier landings. It provides guidance to secure the international ground systems for the F-35B and provided technical expertise to mitigate the threat to the supply chain that supports the aircraft.

Rear Admiral Matt Briers, Director Carrier Strike, Ministry of Defence

"The work the NCSC does to battle-harden our fifth generation F-35B Lightning jets from cyber security threats is vital and means the UK can deploy and support this capability at a time and place of our choosing."

Dr Ian Levy, the NCSC's Technical Director

"Protecting our most sensitive data and capabilities is something the NCSC is designed to do, using our world-leading cryptographic expertise and understanding of the threats from our adversaries."



F-35B Lightning combat aircraft

Supporting the citizen

While the NCSC works to protect the UK's national security and strategic interests around the world, closer to home it works to safeguard everyday citizens and communities from cyber crime and threats.

Suspicious Email Reporting Service

Every day billions of emails are sent globally, helping businesses to function efficiently and keeping people connected. While the vast majority are harmless, the small proportion that are malicious still account for millions of daily cyber threats.

"Phishing" attacks see criminals sending untargeted, mass emails asking for sensitive information (such as bank details) or encouraging recipients to visit a fake website. Such emails can be highly effective at mimicking an established organisation, and even highly skilled cyber experts can be fooled into clicking a link.

The NCSC has long been committed to making emails safe. While ACD measures make it harder to commit these attacks – and minimise the harm they cause – successful attempts still land in people's inboxes.

That's why this April the NCSC, in partnership with the City of London Police, launched the SERS, and encouraged people to forward emails they thought could be malicious. The response was immediate – with more than 5,000 reports within 24 hours. Four months after launching, the service had received 2.3 million reports – an average of 133,000 per week.

Martin Lewis, founder of MoneySavingExpert.com

"There's been an explosion of scam adverts in the UK. We've been fighting them on all fronts. I've even sued, but the toughest nut to crack is scam emails, because emails come from everywhere.

"That's why the NCSC's new report-and-remove function is so vital... at last, we can forward scams to report@phishing.gov.uk and know that someone will take action.

"Yet we need what I call "social policing" too – everyone that can spot a scam must take up arms and report it to protect those who can't. It's why I've shouted it from the rooftops on my show, MSE and social media, and we've seen the rate of reports quadruple, which is proof people are ready to do their bit."

SERS: How it works

Members of the public are encouraged to forward suspicious emails to report@phishing.gov.uk to enable action to help protect other people from falling victim to crime.

Emails are analysed and if malicious content is found, a takedown notice is issued to the hosting provider requesting it removes the content.

In parallel, the malicious URLs are added to a block list which is provided to browser, anti-virus and firewall vendors.

The SERS is a good example of the NCSC working for and with the citizen to make the UK the safest place to live and work online.

SERS fact box

Between April and August 2020:

- Received 2,330,231 reports from members of the public
- 22,237 malicious URLs taken down/ blocked
- 9,315 scams taken down/removed

Clinton Blackburn, Commander, City of London Police

"Phishing is often the first step in a lot of fraud cases we see. It provides a gateway for criminals to steal your personal and financial details, sometimes without you even realising it, which they can then use to take your money.

"Unquestionably, a vast number of frauds will have been prevented, thanks to the public reporting all these phishing attempts. Not only that, but it has allowed for vital intelligence to be collected by police and demonstrates the power of working together when it comes to stopping fraudsters in their tracks."



Celebrity scams

This year there has been a growing trend of fake celebrity-endorsed investment scams.

The scams saw spoofed news articles featuring public figures such as Sir Richard Branson, Ed Sheeran and Martin Lewis promoting fake "get rich quick" schemes. The reader was encouraged to click a link to invest, but in reality the money went to cyber criminals.
The NCSC's Takedown team proactively searched for these scams and took definitive action to take down 300,000 malicious URLs created to trick people into losing money.

Speaking in August then NCSC Chief Executive Officer Ciaran Martin said:

"These investment scams are a striking example of the kind of methods cyber criminals are now deploying to try to con people.

"We are exposing them today not only to raise public awareness but to show the criminals behind them that we know what they're up to and are taking action to stop it."

Sir Richard Branson, Virgin Group Founder

"We have dealt with hundreds of instances of fake sites and fraudsters impersonating me or my team online.

"We are working in partnership with organisations such as the NCSC to report these sites and do all we can to get them taken down as quickly as possible.

"Sadly, the scams are not going to disappear overnight, and I would urge everyone to be vigilant and always check for official website addresses and verified social media accounts."

English Songwriter, Singer & Actor, Ed Sheeran Explains Why He Decided to Invest £1,000,000 in Bitcoin and Reveals A Secret Money-Making Loophole to His Fans!

Sir Richard Branson Brings Financial Freedom for ALL - Here's How He's Doing It.

Student Reveals How He Earns More Than £35,000 Every Month Working From Home

Securing smart cameras

In March, the NCSC issued advice on the safe use of smart security cameras and baby monitors. This followed research by organisations like Which?, revealing that live feeds or images from smart cameras can in some cases be accessed by unauthorised users, putting the public's privacy and security at risk.

Smart cameras are often configured so people can remotely access them and some are shipped with default (highly hackable) passwords set by the manufacturer. The NCSC's advice included some simple steps for citizens to protect themselves and their families from this threat.

The NCSC alert was accompanied by media briefings to ensure citizens had the necessary information to protect themselves, resulting in prominent press coverage and strong support from Which? and other influential commentators and individuals.

To counter the threats from vulnerable devices, the NCSC supported the Department of Culture, Media & Sport (DCMS) in its development of legislation requiring manufacturers of connected consumer devices sold in the UK to:

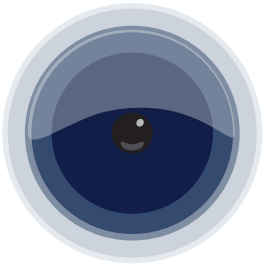
- Not include universal default passwords in their products
- Have a vulnerability disclosure policy
- Provide clarity to the consumer around how long a device will receive security updates for

This year, DCMS ran a "Call for Views" on its proposal to bring forward legislation for connected consumer devices. This provided industry, organisations, and individuals with an opportunity to comment on the UK's approach. This legislation would give consumers more confidence in the devices they buy by placing government security guidance into law.

The NCSC worked alongside DCMS to support the development of a new international standard (EN 303 645) which captures what the NCSC expects to see in connected consumer devices sold in the UK. As a result, manufacturers will have clarity over what they need to do to ensure their devices meet an agreed baseline of security. This world-leading international standard will increase the security of devices globally and is already included in proposals for legislation in the UK, Finland, and Singapore.

Key steps to stay safe:

- Change any default passwords to one using three random words instead
- Regularly update your camera (preferably auto-update), to keep it secure
- Turn off remote viewing feature if you don't need it



Securing financial institutions

Being part of the UK's CNI it is a vital responsibility of the NCSC to help secure the financial and banking sector in its substantial online dealings.

Financial Sector Cyber Collaboration Centre (FSCCC)

Working alongside the UK Government, NCA, financial regulators and institutions, the NCSC has been a leading player in a groundbreaking initiative to improve the resilience of the UK's financial sector. This year, the NCSC supported the creation of the FSCCC, and hosted the new initiative.

What is the FSCCC?

The FSCCC is a partnership which identifies, investigates and coordinates the response to incidents that have potential consequences for the finance sector, by combining, analysing and distributing information from across the sector to produce timely outputs for the financial industry.

Who is involved in the FSCCC?

The FSCCC currently includes around 40 firms but will continue to grow with the ambition of supporting other sectors in future. FSCCC activities are coordinated by the Fusion Cell, which the NCSC hosts and enables through its i100 scheme.

The Fusion Cell works with partners from finance sector firms and other organisations, such as the Cyber Defence Alliance (CDA) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), analysing threats and corroborating intelligence from a range of sources.

What has it done so far?

Since October 2019, the FSCCC briefed the sector on latest developments on cyber attacks, such as DDoS extortion activity, and raised awareness of emerging threats enabling firms to refine defences. The Centre has convened incident management calls to share time-critical information on topics including heightened geopolitical tensions, expiring browser certifications and attacks on the finance sector supply chain.

It continues to develop with the support of financial organisations and regulators, the NCSC and wider government to build greater cyber resilience in the UK finance sector.

Dr Deborah Petterson, NCSC Deputy Director, Private Sector Critical National Infrastructure

"The NCSC, alongside the entire UK Government, is working closely with the most critical UK businesses of today and tomorrow to increase their resilience to cyber threats.

"This is exemplified in the joint work between industry and the NCSC in developing the FSCCC to defend UK interests against cyber threats.

"Working with trusted international partners helps multiply our impact globally and ensures our work remains at the cutting edge of what is possible."

Exercise in a Box

The 10 scenarios you can test in Exercise in a Box are:

- **Supply chain risks**
- **Home and remote working**
- **Threatened leak of sensitive data**
- **Mobile phone theft and response**
- **Third party software compromise**
- **Attack from an unknown Wi-Fi network**
- **Insider threat resulting in a data breach**
- **BYOD policy implications**
- **Phishing attack leading to ransomware infection**
- **Cyber threat simulation exercise: responding to a mock threat**

Exercise in a Box

Last year, the NCSC launched the online tool 'Exercise in a Box', which enables businesses to test how resilient they are to cyber attacks. The toolkit offers a range of realistic scenarios organisations could face, allowing them to carry out drills in preparation for real-life events.

Due to the shift in the number of staff working remotely, in July a 'Home and Remote Working' exercise was released. It focused on three key areas of distributed working; how staff members can safely access networks, what services might be needed for secure employee collaboration, and what processes are in place to manage a cyber incident while working remotely.

As part of the exercises, staff members were given prompts for discussion about the processes and technical knowledge needed to enhance their cyber security practices. At the end, an evaluative summary was created, outlining next steps and pointing to the NCSC guidance.

Sarah Lyons, NCSC Deputy Director for Economy and Society Engagement

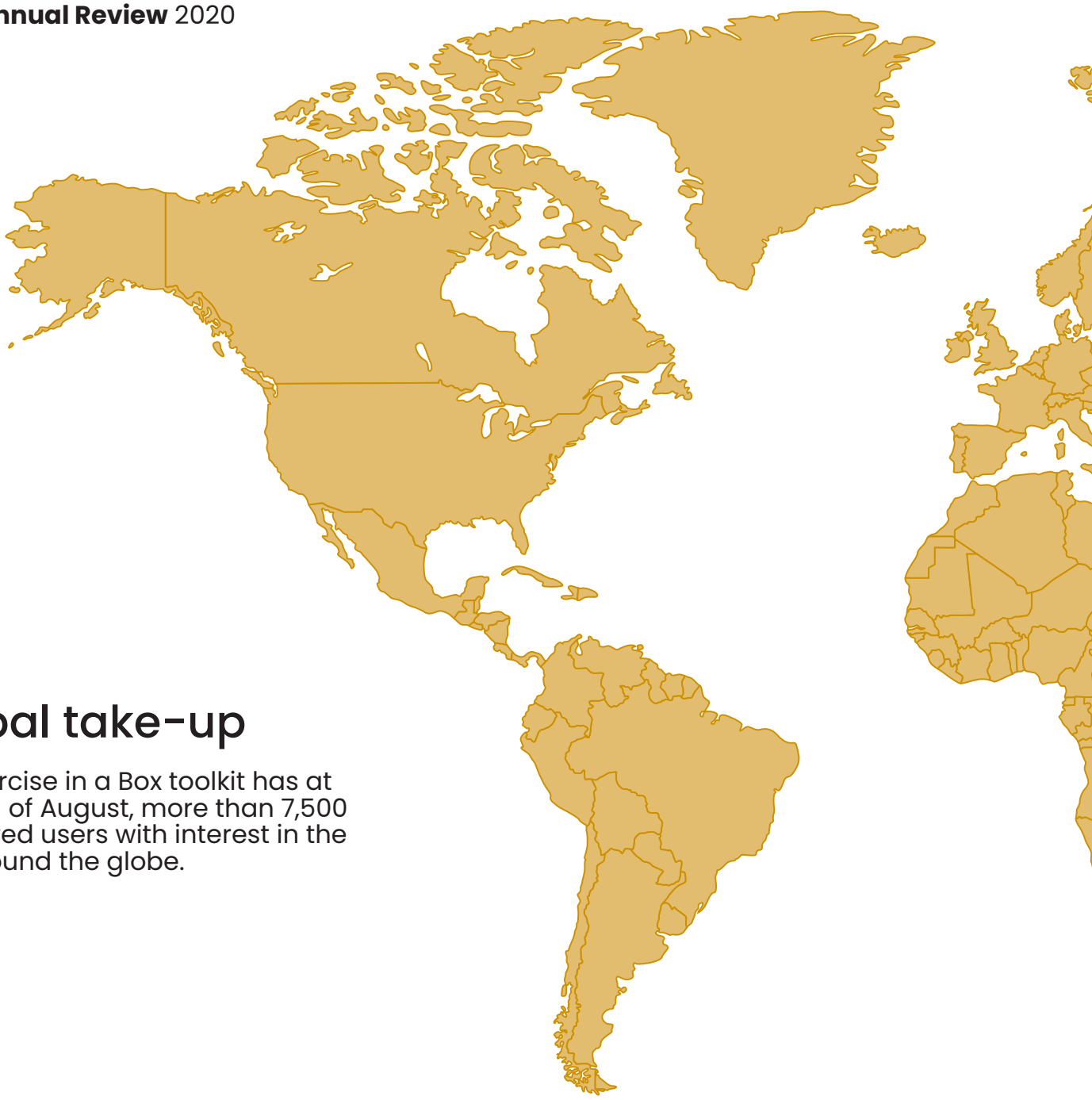
"Businesses wanted to do all they could to keep themselves and their staff safe while home working continues, and using Exercise in a Box is an excellent way to do that.

"While cyber security can feel daunting, it doesn't have to be, and the feedback we have had from our exercises is that they're fun as well as informative.

"We urge business leaders to treat Exercise in a Box in the same way they do their regular fire drills – doing so will help reduce the chances of falling victim to future cyber attacks."

Eventura spokesperson

"Exercise in a Box is a fantastic tool that's free, well thought-out, easy-to-use and can help improve an organisation's security posture – what's not to love in that?"

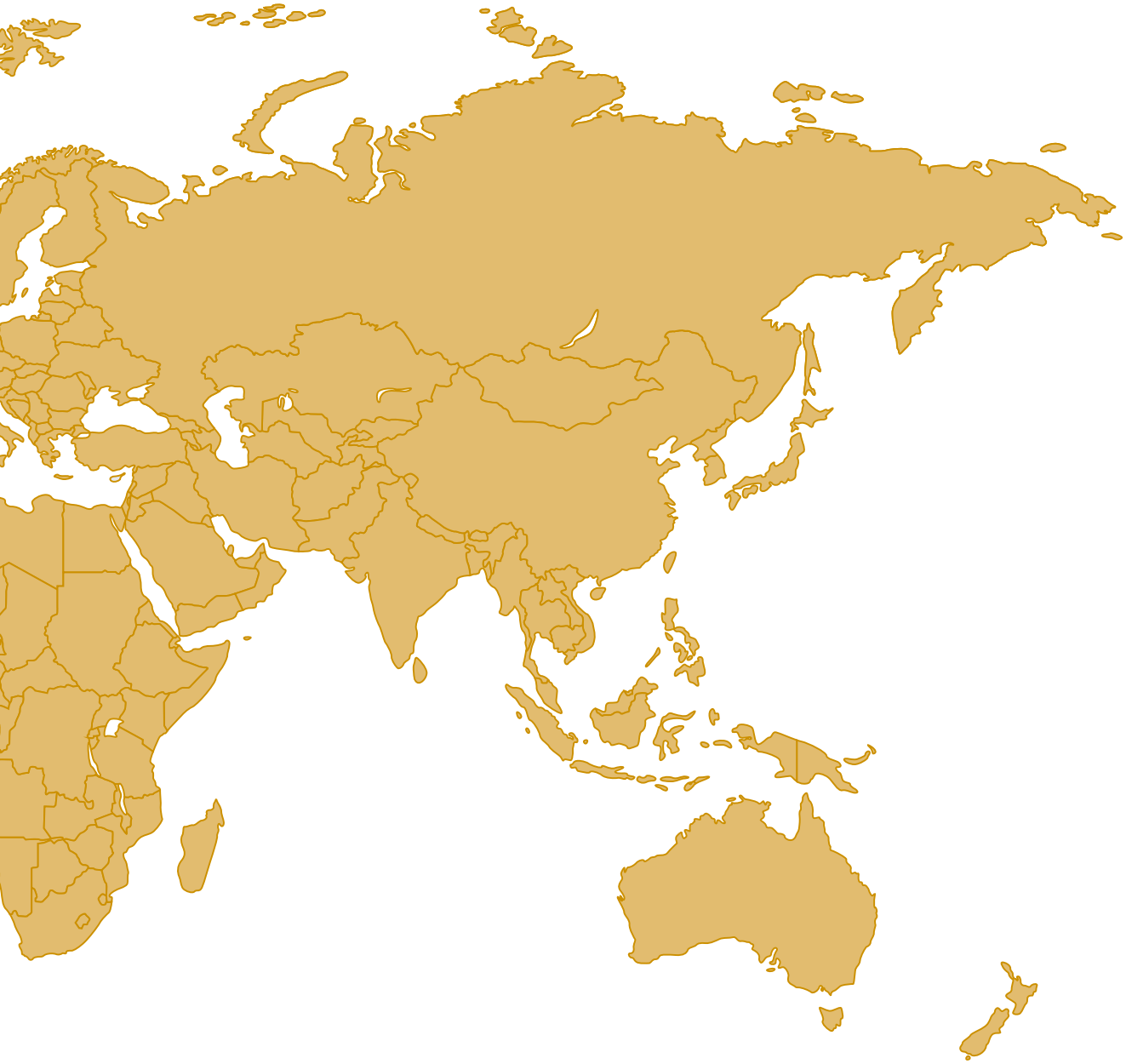


Global take-up

The Exercise in a Box toolkit has at the end of August, more than 7,500 registered users with interest in the tool around the globe.

The top 10 countries by use with Exercise in a Box:

1. **United Kingdom**
2. **United States**
3. **Ireland**
4. **India**
5. **Spain**
6. **Finland**
7. **Pakistan**
8. **Germany**
9. **Netherlands**
10. **Canada**



Steve, the NCSC Exercise in a Box team

"In many cases the effects of cyber attacks could be mitigated by putting good cyber hygiene principles into practice, or by planning and implementing an incident response capability.

"Exercise in a Box is designed for the non-cyber expert with everything the facilitator needs to set up, plan, and deliver the exercise. Among the topics covered are phishing attack leading to ransomware infection, the threatened leak of sensitive data, and mobile phone theft and response.

"On completion there is an end report with links to NCSC advice and guidance. In addition, we've just added micro exercises on single topics designed to provide the basics over 15-20 minutes."

New 'Single Source of Truth' for the UK's Critical National Infrastructure

The NCSC's Knowledge Base is the 'Single Source of Truth' that allows the government and CNI sector to better understand and manage the UK's CNI, its supply chains, and the interdependencies between them all.

The Knowledge Base is a mapping tool (IT system) which helps analysts view the CNI data on a map or as a network diagram with each interdependency mapped across it. It was used to support the response to the coronavirus pandemic, and next year, the user base will be extended to help foster collaboration and discussion more widely across UK Government.

Both the criticalities approach (an assessment based on the importance of an organisation, supply chain or sub-sector) and the CNI Knowledge Base were developed and implemented by the NCSC on behalf of Cabinet Office (Civil Contingencies Secretariat) as part of the National Cyber Security Programme.

Andrew Bell, Critical National Infrastructure Programme Manager, Department for Transport

"The new functionality delivered by the CNI Knowledge Base will be a game changer for the UK Government. For the first time, we will have the tools needed to identify the functional, organisational and geographic dependencies within and across CNI sectors, informing meaningful collaboration with stakeholders and helping us make the UK safe, secure and resilient."

Civil Contingencies Secretariat, Cabinet Office

"The NCSC Knowledge Base will enable a step-change in the way the Government anticipates, prevents and responds to cascading risks that could impact our most essential services. A flagship project under the 2016 National Cyber Security Programme, it provides a world-leading capability in CNI risk management."





4

Proactive engagement

Cyber security is a team sport, and while the NCSC is a key player, it can't make the UK the safest place to live and work online alone. Over the last 12 months government, industry and the general public came together to enhance their shared cyber security.

This chapter sets out how the NCSC developed existing and new partnerships with individuals, communities and institutions to create new ideas and solutions to give the UK a winning edge.

Cyber Aware

Most of the cyber threats to the public are high-volume, low-sophistication attacks which can be prevented with just a few actions. However, a considerable proportion of the public are not taking the simple steps to protect themselves. In 2019, it was reported that 23.2 million hacking victims had "123456" as their password, meaning that without actively encouraging the adoption of protective behaviours, the UK would remain an attractive target for cyber criminals. The cross-governmental 'Cyber Aware' campaign relaunched in April to better equip the public against the increased cyber security threats related to the coronavirus outbreak. The campaign communicated actionable guidance for staying secure online and advice on how to report a suspicious email.

During the campaign period, paid digital advertising exceeded government benchmarks for website click-through rates and, after six weeks of activity, the SERS received 672,810 reports. This resulted in the successful removal of 5,085 malicious URLs and 1,801 previously unknown scams, significantly reducing the number of people who could fall victim to cyber crime.

With individuals spending more time online, and businesses moving increasingly from physical to digital practices, the Cyber Aware campaign will relaunch in November 2020 to encourage citizens and micro businesses to adopt the six behaviours that will help protect them from the most common attacks.

The campaign is designed to help the public and micro businesses understand the best ways to stay secure online and take necessary protective actions. It supports the NCSC's wider efforts to combat the threat "at source", working behind the scenes to stop the threat reaching the public. The NCSC also works with key industry partners to make their systems more secure by default and to make it easier for the public to adopt more secure online behaviours on their platforms. This critical programme of work ensures that the Cyber Aware behaviours are as implementable as possible by the public across the wide range of online services and devices that they use.





Cyber Aware

Six top tips:

- **Create a separate password for your email**
- **Create a strong password using three random words**
- **Save your passwords in your browser**
- **Turn on two-factor authentication**
- **Update your devices**
- **Turn on back up**

Find out more at www.cyberaware.gov.uk

Partnership snapshot

The NCSC is committed to raising cyber security and resilience across every part of national life. This includes supporting and empowering UK businesses, academia and the charity sector.

A snapshot of our partnership over the past 12 months:

Academia:	**Businesses:**	**Charity / voluntary sector:**
Cyber security information cards for schools	**Entry level advice for NatWest business customers**	**Guidance on cyber security**
The NCSC worked with the National Education Network to distribute 33,000 cyber security information cards to help those working in UK schools to better understand cyber threats. The cards were also presented to Ofsted inspectors at their November conference.	The NCSC's Small Business Guide was used in innovative ways to reach NatWest business customers. It was included in a blog posted to its Bankline platform, and references and links to the Guide were included in NatWest's 'Security tip toasters' and FAQ content on its public-facing platforms – these were live for two weeks, receiving 40,000 unique views. 9,000 bespoke versions of the guide were created and distributed to NatWest's business customers.	To help the NCSC reach small charities in their local communities, the NCSC worked in partnership with the National Association for Community and Voluntary Action and the Foundation for Social Improvement, to upskill over 40 local delivery partners and deliver awareness raising sessions using the NCSC's Small Charity Guide. To date, over 5,000 small charities have been trained in cyber security. In addition, this year the NCSC delivered more than 100 workshops, podcasts and webinars all over the UK for the voluntary sector.

Rail safety

As the UK's transport infrastructure becomes more digitally connected, there remains a critical need to maintain the highest standards in health and safety. The work the NCSC has done this year with the independent regulator, the Office of Rail and Road (ORR), exemplifies its support to the physical safety of citizens through cyber security.

The NCSC assisted the ORR with software risks, a developing area of focus for the sector, so it can better ensure safety in the UK rail industry. This was welcomed as a positive step towards greater understanding of the importance of good cyber security in safety critical systems within the rail industry.

Paul Appleton, Deputy Director of Railway Safety at the ORR

"We have been working in collaboration with the NCSC and the Department for Transport in looking at rail software risks so that we're prepared to manage any future risks to support the railway industry. We know that cyber security is vital to ensure systems are kept running and this work is a positive step for managing safety critical systems well to ensure the high levels of health and safety that the UK expects."

Fair play for sport

The NCSC published its first analysis of the sports industry in July, which revealed that 70% of sports institutions had suffered a cyber incident in the past year – double the average for UK businesses.

The 'Cyber Threat to Sports Organisations' report outlined measures recommended to prevent criminals cashing in on the industry.

Case studies in the report included:

- A member of staff at a racecourse losing £15,000 in a scam involving the spoofing of eBay
- A Premier League club's Managing Director being hacked before a transfer negotiation – meaning the £1 million fee almost fell into the hands of cyber criminals
- An employee at an organisation holding athletes' performance data having their email address compromised, allowing the hackers access to sensitive information over several month
- An English Football League club suffering a ransomware attack which crippled its corporate and security systems. As a result of the attack the CCTV and turnstiles at the ground were unable to operate, almost leading to a game's cancellation

Tony Sutton, Chief Operating Officer at Rugby Football League

"The issue of cyber security is one all sports, including Rugby League, take seriously. As we grow our digital capabilities and online platforms, protecting the governing body, our members, customers and stakeholders is paramount.

"We welcome the NCSC report and the guidance it offers the sports sector."

Sir Hugh Robertson, Chair of the British Olympic Association

"Improving cyber security across the sports sector is critical. The British Olympic Association sees this report as a crucial first step, helping sports organisations to better understand the threat and highlighting practical steps that organisations should take to improve cyber security practices."

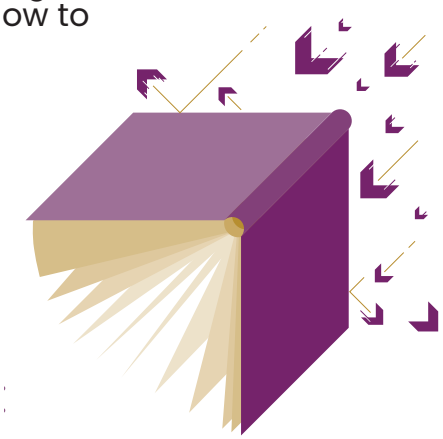
Protecting academia

The NCSC continued its support for the academic sector this year as it saw a spate of ransomware attacks against UK schools, colleges and universities.

Through engagement with key institutions such as the Department for Education (DfE) and Jisc (a not-for-profit organisation providing digital and IT services to education and research institutions), rapid and tailored guidance was offered to the sector on how to improve cyber security.

A new alert, 'Targeted ransomware attacks on the UK education sector by cyber criminals', supplemented existing NCSC advice for academic institutions across the UK.

The NCSC also presented on the topic at a webinar set up for the Association of Colleges, issued a press release and provided a ministerial briefing.



David Corke, Director of Education and Skills Policy at the Association of Colleges

"It has never been more important for colleges to have the right digital infrastructure in order to be able to protect their systems and keep learning happening, whatever the circumstance.

"This needs a whole college approach and for a focus wider than just systems, it needs to include supporting leaders, teachers and students to recognise threats, mitigate against them, and act decisively when something goes wrong.

"The NCSC's guidance will prove incredibly useful for colleges to ensure that they can do just that."

Steve Kennett, Executive Director of e-infrastructure at Jisc

"Jisc welcomes the NCSC's support in dealing with the current spate of ransomware impacting the UK Education and Research community.

"We encourage everyone to review the latest guidance from the NCSC and take the time to assess the risks to their organisation."



Trusted Research

The UK has a thriving research and innovation sector that attracts investment from across the world – but the open nature of research collaboration also entails certain risks. 'Trusted Research' is the NCSC and Centre for the Protection of National Infrastructure's (CPNI) latest advisory paper for UK universities and research institutions, which aims to help them make informed decisions about international collaboration and protect their own researchers and academic values.

The NCSC and CPNI have worked closely with the academic sector and partners, such as Universities UK, to develop the guidance which breaks the threat down into two basic types: criminals and nation states.

In the first instance, universities are targeted by cyber criminals just as any other organisation might be. Criminals seek to access personal information, convince users to install malware and lock or damage data, all with a view to financial gain.

In the second case, nation states are interested in the valuable research and intellectual property generated by universities.

The NCSC's 'Cyber Threats to Universities' report was launched at Birmingham University on the same day that 'Trusted Research' was published.

Industry 100 – The private sector secondee initiative

The NCSC's i100 scheme continues to expand, delivering results across all areas of the organisation.

The initiative sees a variety of companies with unique insights and capability in cyber defence loan staff to the NCSC on a part-time basis to collaborate in defending the UK. The secondees are given a security clearance and sign an agreement that enables them to work alongside the NCSC's staff, including on sensitive projects and investigations.

A virtual team of i100 analysts from threat intel, telecoms, software and security firms working in the NCSC's operations team made an indispensable contribution to the organisation's efforts to understand cyber threats and respond to incidents.

During the coronavirus pandemic, they were at the forefront of identifying malicious infrastructure targeting the public, industry and government, as well as flagging incidents to the NCSC and drawing on skills and expertise to understand and mitigate threats.

Cyber Security Toolkit

The NCSC's Business Engagement team worked with over 80 new and established partners across the private sector, for example within construction, civil engineering, architecture and farming.

More than 150 legal firms were hosted by the NCSC in February for an event which articulated the threat to the legal sector and helped companies understand what mitigations they can put in place.

Working with the British Retail Consortium, the NCSC helped revise its 'Cyber Security Toolkit' for retailers. And in June an NCSC workshop on credential stuffing (a form of cyber attack involving stolen log-in details) was delivered to retailers to help this important sector better understand the risks and how to mitigate against them. The workshop received very positive feedback from attendees who welcomed the NCSC's support.

Matt Warman, MP Parliamentary Under-Secretary of State for Digital Infrastructure, DCMS

"It is vital businesses take action to protect themselves and their customers from security risks and cyber insurance can play an important part in robust risk management strategies.

"I encourage firms to consider this guidance and use programmes such as Cyber Essentials to make sure they have fundamental cyber security defences in place."

Cyber insurance

In consultation with major stakeholders and industry partners, the NCSC produced its first ever guidance on cyber insurance after calls for expert technical advice on the growing cyber insurance market.

The guidance highlighted the seven cyber security questions organisations should be asking if they are considering purchasing cyber insurance. These questions ranged from the levels of defence that are already in place, to whether the insurance covers the aftermath of an incident.



The seven questions the guidance recommends senior leaders ask about cyber insurance are:

1. What existing cyber security defences do you already have in place?
2. How do you bring expertise together to assess a policy?
3. Do you fully understand the potential impacts of a cyber incident?
4. What does the cyber insurance policy cover (or not cover)?
5. What cyber security services are included in the policy, and do you need them?
6. Does the policy include support during (or after) a cyber security incident?
7. What must be in place to claim against (or renew) your cyber insurance policy?

British Insurance Brokers' Association

"The British Insurance Brokers' Association welcomes this guidance for businesses. This guide clearly explains how good cyber security and suitable insurance go hand in hand.

"Insurance brokers can provide support and advice to firms looking for cover and in turn businesses benefit from reducing the impact of disruption caused by a cyber attack."

The Association of British Insurers (ABI)

"Being a victim of cyber crime can have a devastating impact on any business, whatever its size, with SMEs especially vulnerable. Nearly half of UK firms reported a cyber attack over the last year, but despite this, take-up of cyber insurance by businesses remains low.

"This NCSC guide reinforces just how wide-ranging and serious the impact of a cyber attack can be, and why it is important to manage your cyber risk and put cyber security measures in place."

Cyber Essentials

Cyber Essentials is a government-backed, industry-supported certification programme to help organisations protect themselves against common online threats. They can apply for two levels of certification:

1. Cyber Essentials – a self-assessment that gives an organisation protection against a wide variety of cyber attacks
2. Cyber Essentials Plus – a hands-on technical verification is carried out to assess an organisation's cyber security

With many organisations adjusting to new ways of working due to social distancing measures, the number of certifications has risen this year and was up by 20% compared to last year. Cyber Essentials is also part of the Government's support to organisations during the pandemic specifically, with key invited organisations being offered the initiative to help them manage their cyber risk.

In April, IASME Consortium Ltd became the NCSC's sole delivery partner for Cyber Essentials. To ensure a smooth transition, it issued regular briefings for certification bodies, and will work alongside the NCSC over the next year to keep pace with the changing landscape and consider additional Cyber Essentials levels.

CYBER ESSENTIALS

Dr Emma Philpott MBE, CEO, the IASME Consortium Ltd

"We were absolutely delighted to step into the role of Cyber Essentials Partner.

"We see the Cyber Essentials scheme already having such a positive effect on the security of UK business and the strong partnership with the NCSC allows us now to enhance the scheme to be even more effective."

Anonymous recipient of Cyber Essentials coronavirus response offer

"As a key supplier of medicines to the NHS, pharmacies and supermarkets, we were offered funding for a Cyber Essentials check on our IT systems and help to improve our security.

"The assigned Partner has been great to work with and has really helped our business identify areas of improvement. We highly recommend this scheme if you have the option."

Cyber regulation

The UK's National Cyber Security Strategy 2016-2021 highlights the importance of effective regulation in driving improvements to CNI cyber security. The past year saw a significant expansion of the NCSC's support to UK regulators, and a major review of the Network and Information Systems (NIS) regulations upon which much CNI cyber security regulation is based.

NIS Post-Implementation Review

The DCMS NIS Post-Implementation Review, drawing on input from the NCSC amongst others, was published in May. It described the positive impact the new regulations are having. For example, a majority of the Operators of Essential Services (OES) taking part in the Review reported increased board-level attention to cyber security, raised investment in protecting critical networks and improvements to their capability to respond to cyber incidents.

Cyber Assessment Framework (CAF)

The NCSC provided a framework for regulators and OES to use to assess levels of security. The majority of UK cyber regulators have now adopted the CAF, which the NCSC continues to update and improve. The latest version, specifically designed to meet a wider range of regulatory requirements, better supports regulation of the cyber aspects of safety which is important to regulators, such as the Health & Safety Executive.

This year, the NCSC's technical work expanded regulators' ability to use the CAF to set a range of target levels of cyber security in their sectors depending on the threat faced. These targets are aligned to levels of risk, based on sector cyber risk scenarios derived from real-life cyber incidents. Recently the Civil Aviation Authority became the first regulator to make use of this new capability with the publication of its tiered approach to cyber regulation.

Cyber Regulators Forum

The new NCSC Cyber Regulators Forum provided a unique opportunity for cyber regulators of all UK CNI sectors to engage with each other and with the NCSC, by taking part in discussions about the technical, practical and cultural aspects of regulating cyber security.

Regulation is making a difference: insights from the energy sector

In the energy sector, the regulator Ofgem conducted analysis of its OES with 90% reporting they have improved their cyber security since the introduction of NIS regulations.

Supply chain management has also seen improvements, with a doubling in the number of OES achieving the outcomes set out in the CAF since 2019. This type of CAF-based evidence shows that the NIS regulations are now resulting in improvements being made. The NCSC looks forward to continuing to work with Ofgem and other regulators as they drive changes to the security and resilience of CNI across multiple sectors.



Cyber Accelerator

The NCSC's acclaimed Cyber Accelerator programme works with dynamic start-ups to encourage new products, skills, jobs and growth. It is a collaboration between the NCSC, DCMS, and Wayra, Telefónica's open innovation arm.

Based in Cheltenham, it offers mentorship to tech businesses that are creating solutions for the security industry and spurs innovation and competition to boost the country's economic growth.

Since it began, 36 companies have been successfully supported by the initiative. The amount of external investment raised by alumni after their time on the Accelerator exceeds £90 million and they have created more than 75 jobs.

The companies chosen for this year's programme were given rare opportunities, meeting key cyber security professionals and pitching their products to potential investors. In February, seven companies took part in the RSA conference on cyber security in Silicon Valley and were invited to a private coaching session at the home of Steve Blank, the originator of the Lean Start-Up movement.





Case study 1: Simple Cyber Life

In his previous life as a professional rugby player, Jonny Pelter was used to tackling problems as a team. After retiring from the game, he found he was spending an increasing amount of time helping his friends and family with domestic cyber security issues, such as removing computer viruses or dealing with online bullying.

"I could see that families were often becoming paralysed by the complexity of online safety and they were suffering from "security fatigue". There are so many products and choices to be made that parents don't know where to start and end up being unable to implement any protection at all," says Jonny.

"The "safety tech" market is focused on producing more products such as parental control apps, but providing the technology is not the problem. The issue is overcoming security fatigue for families."

So, he decided to take the plunge and start his own company, Simple Cyber Life, marketing it as an online platform that helps parents get personalised protection in place quickly and easily.

"We help parents understand what protection they need and use automation to get that protection on their devices. We then provide an online community of experts and like-minded parents to support them so they stay safe over time.

"The NCSC was seeking start-ups that could have wider societal benefits and we were looking for a prestigious platform from which we could get expert advice and accelerate our development.

"We felt incredibly privileged to be chosen for the programme, from which we've learned how to structure our investment strategies, how to position the company for corporate deals, and how to get our marketing in shape for acceleration.

"We've gained a great deal from the expertise and new connections, and have now started the transition from a part-time outfit of contractors to a full-time growing team."

Case study: Trust Stamp

Another success story of the Accelerator programme is Trust Stamp, which uses artificial intelligence and biometrics to create unique digital identities, bypassing the need for usernames and passwords. The four-year-old company is expanding and has attracted investment from Mastercard.

An application developed by Trust Stamp records facial biometrics, irreversibly converts them into a "hash" and matches them with multiple sources, such as public records or social media to verify a person's identity. Data can be connected to the hash to facilitate transactions, whether by commercial or government agencies.

The company's co-founder and CEO, Gareth Genner, says:

"Our application allows a mixture of biometrics to be used but protects against the common vulnerabilities of fake identities, phishing and online security breaches by storing a non-PII hash that is matched using artificial intelligence.

"Our work with Mastercard has been on enhancing data security in environments with low connectivity, such as in parts of Africa, where we can create protected legal identities that can help communities when they want to register for, say vaccination programmes. Our ethos is to create a world where secure, trusted identity is a universal human right, empowering opportunity and access for all."

Gareth adds that the company's participation in the Accelerator programme brought access to invaluable expertise and connections:

"Through our links with the NCSC we now have 11 staff gaining from that expertise in Cheltenham, and we are planning to create 20 new jobs in the area."

Andrew Mason, co-founder of RapidSpike, a Leeds-based Cyber Accelerator start-up

"The Accelerator programme has been an exceptional learning experience for RapidSpike. We have honed our messaging, validated our marketing and technical approach and met some brilliant people through the NCSC and Wayra.

"I would fully recommend any business with cyber growth ambitions to apply now, get involved and immerse themselves into it fully. You won't be disappointed."

Supporting local government

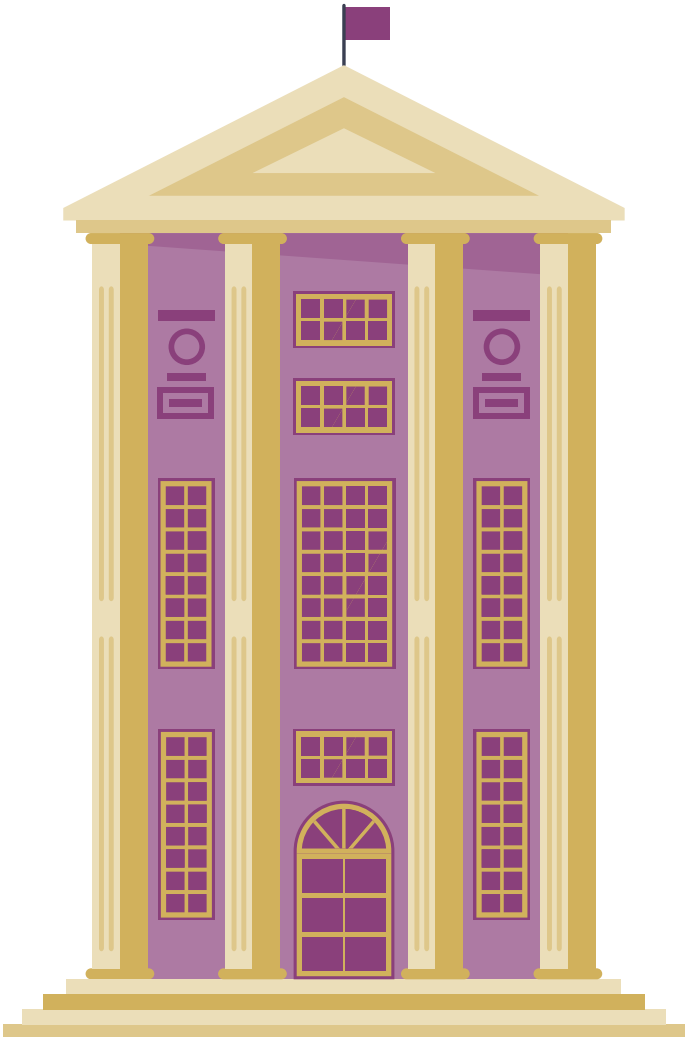
As the concept of "smart cities" – using advanced technology to pair devices and data with a city's physical infrastructure – continues to develop, so too does the demand for cyber security around these networks.

Local government has been expanding the development of this technology to enable communities to tackle such issues as the control of traffic congestion, and improving refuse control and air quality, with the overall aim of improving the efficiency of the UK's wider economy.

The increased interconnectivity and the development of the IoT creates vulnerabilities, so the NCSC has increased its engagement with local authorities to provide advice to securely develop new systems.

Graham Farrant, Chief Executive Officer, Bournemouth, Christchurch & Poole Council

"We are actively pursuing our Smart Place ambitions, using the latest digital technologies to improve the lives of our residents, the vibrancy of our communities and the prospects of our local businesses. A critical aspect of our Smart Place programme is maintaining trust with local residents, businesses and stakeholders as well as maintaining the reputation of the Council, so working alongside the NCSC is critical in establishing confidence."



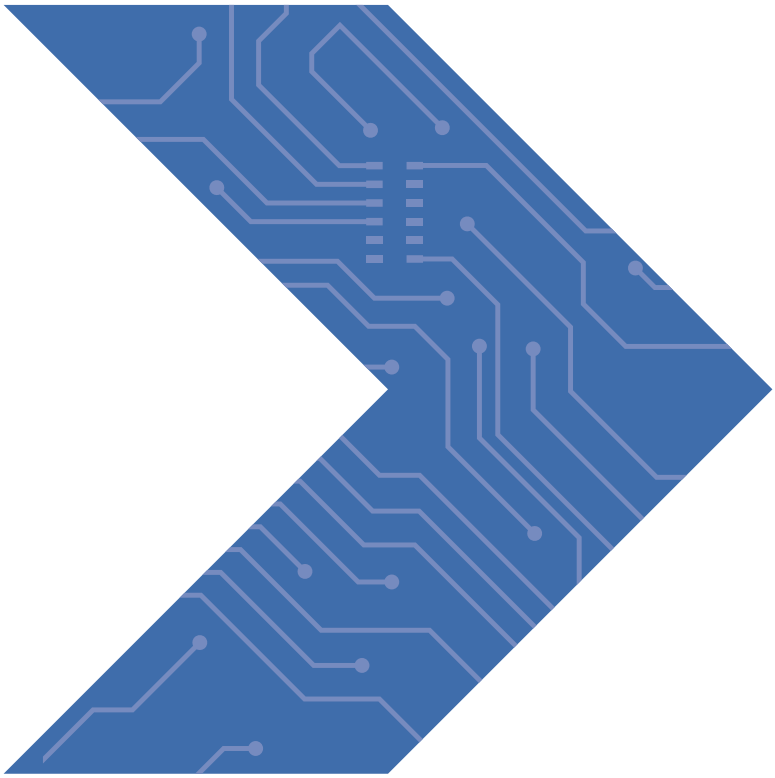
Fostering a dynamic sector

To enhance the cyber security of the nation and drive digital growth, the UK needs a vibrant cyber security sector made up of high quality, trustworthy companies that can support all sectors of the economy and all sizes of organisation. The current landscape is complex, with a huge range of products and services of varying quality, and it can be hard for organisations to know who they can trust with their cyber security needs.

The NCSC will extend its reach and build on its brand and expertise to raise the bar in UK cyber security, by creating a curated marketplace of NCSC-assured industry products and services to help guide businesses to suitable vendors.

The organisation is building a 'National Catalogue of Assured Industry Products & Services' that will help buyers identify sellers they can trust. Using wider levers of government, the NCSC will encourage and promote this in a way that adds value to the UK economy and opens up opportunities for trusted vendors to sell their services in both the domestic and foreign markets.

This is a challenging ambition, but one which the NCSC believes is not only achievable through collaboration with industry, but is essential to secure its vision to make the UK the safest place to live and work online.



Events

CYBERUK is usually a highlight in the NCSC calendar, bringing together both leaders and technical experts with an interest in cyber security from across the UK and abroad. CYBERUK 2020 was due to take place in Newport in May, but sadly had to be cancelled due to coronavirus.

The NCSC adapted to the challenges of the pandemic, switching from the physical to the virtual. It has set up a programme of work to build its capacity to continue to deliver bigger and better virtual offerings in the future. This will include a meeting of CYBERUK Leaders early in 2021.

The NCSC delivered a wide and varied events programme this year, delivered both at its national HQ in London and around the UK.

From September to mid-March, NCSC HQ hosted 101 events with more than 4,500 attendees from across industry, academia and the public sector including law enforcement, health, local and central government.

Other events taking place over the last year include the Cyber Threat summit which took place over two days in November 2019, co-hosted by the NCSC and the SANS Institute. Cyber Threat brought together more than 350 cyber security practitioners from across the UK and Europe for a deep dive into some of the thorniest and most technical challenges facing cyber security professionals today.

Jeremy Fleming, Director GCHQ, speaking at CyberUK 2019





5

Defending the digital homeland 24/7

The core aim of the NCSC is to make the UK the safest place to live and work online. The NCSC loves technology and seeks to help the UK enjoy the benefits of the digital age in a safe and secure way.

To do this, measures are put in place to remove vulnerabilities and prevent as many attacks in the first place. Where attacks do get through the NCSC is there: to respond to incidents, to help support victims and to continually refine the best defences.

Cyber attack trends

While the NCSC works 24/7 with its partners to prevent cyber attacks, some will inevitably get through. In the last year the NCSC dealt with 723 cyber security incidents involving almost 1200 victims. These are the highest annual totals since the NCSC was formed.
This year's total means that since the NCSC commenced operations in 2016, the organisation has coordinated the UK's defence against a total of 2,528 incidents (annual totals of 590, 557, 658 and 723).

Several incidents came onto the NCSC's radar proactively, through the expert work of its threat operations and assessments teams. Many others were raised by victims of malicious cyber activity and cyber attacks.

According to the DCMS 'Cyber Security Breaches Survey 2020', almost half of businesses (46%) and a quarter of charities (26%) reported having cyber security breaches or attacks over a 12-month period. Of the 46% of businesses that identified breaches or attacks, more were experiencing these issues at least once a week in 2020 (32%, vs. 22% in 2017).

The nature of cyber attacks has also changed since 2017. Over this period there has been, among those identifying breaches or attacks, a rise in businesses experiencing phishing attacks (from 72% to 86%), and a fall in attacks involving viruses or other malware (from 33% to 16%).

Paul Chichester, NCSC Director of Operations

"At the NCSC, we get ahead of the cyber threats and defend critical sectors before damage is done.

"Thanks to our access to key intelligence, our ability to predict trends and the agility of response, we refocused many of our capabilities to focus on coronavirus-related sectors this year.

"It's vital that we stay ahead of threats and are able to quickly react to the threat landscape."



Trends

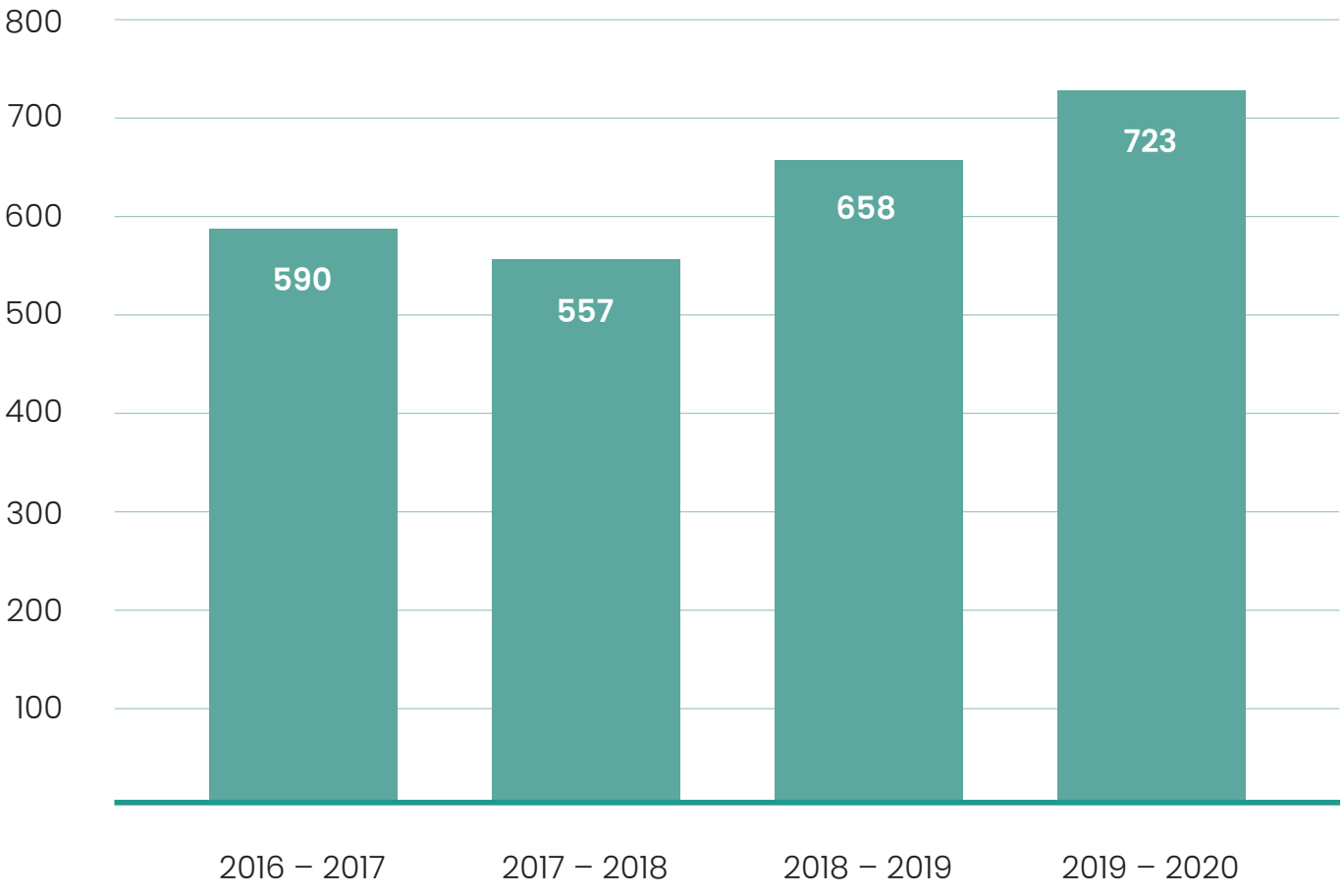
- Around a quarter of the incidents the NCSC responded to this year related to coronavirus
- 10% rise in the number of incidents (723 v 658), and 33% increase in the number of victims (<1200 v c900) this year compared to last
- The NCSC also handled more than three times as many ransomware incidents than last year



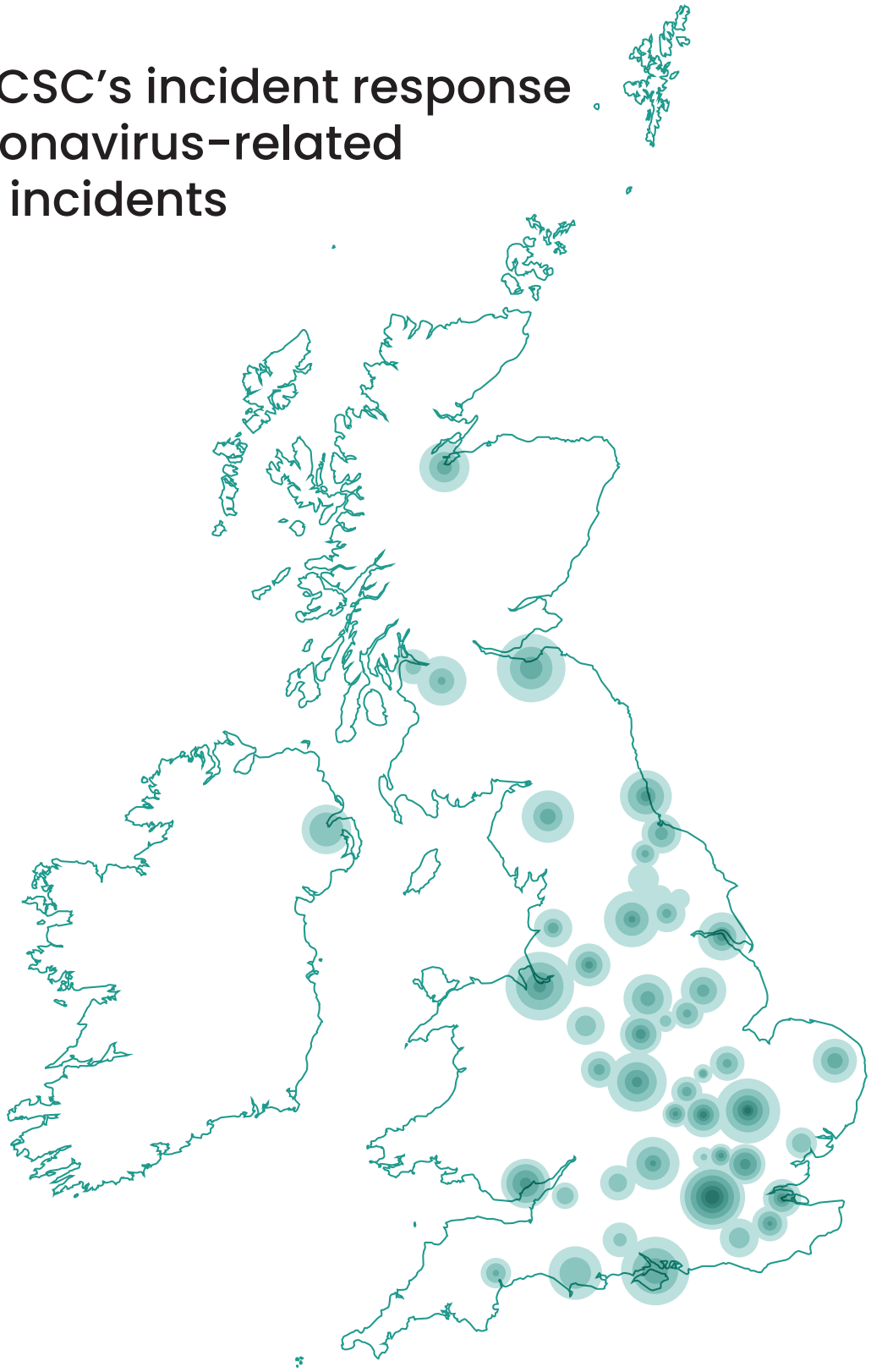
Eleanor Fairford, NCSC Deputy Director, Incident Management

"We actively redirected our efforts to defend the health sector and because it was such a priority, it rose to our second most supported sector this year."

Incidents supported each year



The NCSC's incident response to coronavirus-related cyber incidents



This map illustrates the broad geographic spread across the UK of all the cyber incidents the NCSC managed that may have had some bearing on the national response to the pandemic between February and July.

The location is indicative rather than a precise pinpoint of each incident. These incidents varied in terms of their severity and type.

Ransomware

Over the past year, the NCSC saw a significant rise in ransomware attacks on the UK, including an attack against Redcar and Cleveland Council which caused considerable damage and disruption.

There has also been a significant change in the way ransomware attacks are carried out. Rather than simply preventing access to data, criminals are stealing it and threatening to leak the most sensitive parts publicly.
There are obvious business sensitivities to ransomware attacks, and there have long been fears the crime is underreported. The NCSC, in collaboration with the NCA, is committed to helping victims and tackling the wider issue, working as part of a team with law enforcement colleagues.

While the NCSC tracks trends and attempts to disrupt operations, it works closely with the NCA, which coordinates and leads the national law enforcement response to ransomware incidents. This includes supporting victims, successfully resolving incidents through a range of outcomes and pursuing criminal proceedings against those responsible.



Redcar and Cleveland Borough Council spokesperson

"We worked closely with the NCSC following the cyber attack and its expertise and guidance enabled us to recover our systems effectively and plan additional security measures above industry-approved standards."

So, what is ransomware, why are criminals using it and how can you avoid being a victim?

What is ransomware?

Ransomware is a type of malicious software (malware) that prevents victims from accessing their device, or the data that is stored on it.

Once the malicious software is on a network, the criminals can encrypt data that would have an impact on the organisation's services and then withhold it until a payment is made.

The system itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network – such as the WannaCry malware that impacted the NHS in May 2017 – meaning it is untargeted and potentially viral.

The criminal ransomware model

Traditionally, the victim is told that they have been denied access to their own data which will not be restored until they make a payment in cryptocurrency, such as Bitcoin. Once this payment is made, the criminal will unlock their computer or allow access to the data.

The NCSC has seen an increase in the scale and impact of ransomware attacks and a new and growing trend to be more targeted and more aggressive than ever before.

Lynne Owens, Director General of the National Crime Agency

"The NCSC is a key partner for the NCA's National Cyber Crime Unit, helping us achieve our mission to reduce the threat to the UK from cyber crime, through investigations and disruptions delivered in partnership with Team Cyber UK.

"We work closely at both a strategic and tactical level. From shaping the whole system response to assisting industry with advice on protecting their systems and preventing malicious activity.

"We jointly deploy to crime scenes, allowing the NCA to obtain evidence, whilst managing crimes in action, leading to the identification of suspects, arrests and prosecutions.

"Nowhere is this more important than in the response to ransomware – where our partnership assists the victim with restoration of their systems whilst enabling us to pursue the suspects in the UK and overseas, using a range of measures including arrest, prosecution and international sanctions."

What is the new trend?

Criminals are increasingly found lurking on a network, searching before ransomware is even deployed, looking for specific sensitive data that the victim would not want to be made public – such as a secret patent, or information about staff salaries.

Rather than simply seeking to withhold data, criminals are increasingly threatening to leak the most valuable information publicly unless the victim pays the ransom. This new trend to extort means that victims are at risk even if they have backed up their data, as they would not want the information published externally.

The data available suggests that the UK is not the most heavily targeted country, predominantly because British victims are traditionally less likely to pay the ransom than those from other parts of the world. However, the trends suggest that unless defences are improved, ransomware will increase globally and in the UK, with criminals developing new techniques to circumvent cyber defences.

NCA
National Crime Agency

What happens after a victim pays the ransom?

Even if the ransom is paid, there is no guarantee that victims will get access to their computer or files – or that the criminal won't just charge again under threat of leaking the same information. It will also likely result in repeat incidents as criminals become emboldened in holding people to ransom.

Depending on the comprehensiveness of disaster recovery and business continuity plans in place, normal service can take weeks, if not months, to resume.

How to avoid being a victim

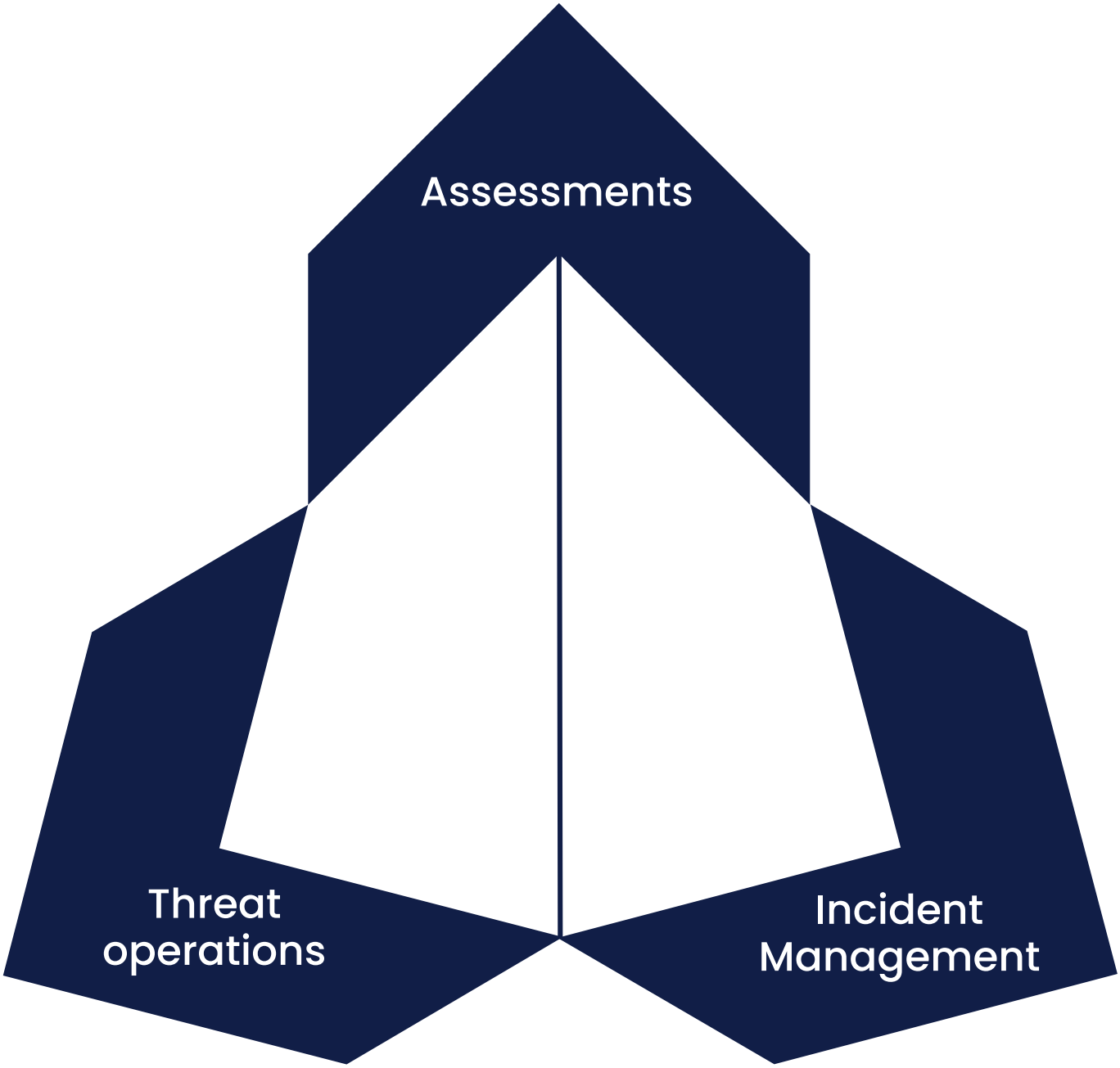
The NCSC has updated its 'Mitigating Ransomware and Malware Attacks' guidance, recommending that organisations deploy a "defence in depth" strategy. By implementing a technical architecture with multiple defensive layers, if one mechanism fails another is there to thwart an attack.

Organisations should also have an incident response plan, which includes a scenario for a ransomware attack, and this should be exercised.

More generally, a good first step to avoid being a victim is making offline backups of data. The criminal will hold less power over an organisation or individual if they already have copies of the thing they are trying to withhold.

Inside the nerve centre

The NCSC's operations and incident response team is comprised of highly skilled experts based across the UK. The team discovers new cyber threats, responds in support of victims, assesses the trends in cyberspace, shares information with partners and industry and leads on counter campaigns to deter threat actors. In doing so, the team uses a wide range of data sources, including from industry partners. It works closely with law enforcement and leads the intelligence community in defending the UK 24/7.



Threat operations

- Predict adversaries' future behaviour and mitigate damage
- Consider both secret intelligence and open-source trends to assess cyber threats
- Share classified assessments wherever possible to UK defenders, on the NCSC website and threat sharing platform CiSP

Assessments

- Generating technical knowledge on the cyber threats facing the UK
- Discover and detect attacks proactively, through the NCSC's unique intelligence and trusted partnerships
- Develop and deploy counter cyber campaigns that deter threat actors and make it harder for them to attack the UK

Incident Management

- Support for UK organisations that are the victims of the most damaging cyber attacks
- The IM team works closely with law enforcement, the UK intelligence community and the private sector
- Lessons learned from incidents are used to inform future assessments and public guidance to the sector

"Support, reassurance and effective team working" - victim testimonial

One of the near 1,200 UK-based victims of a cyber attack supported by the NCSC this year recalls their experience. Anybody who alerts IM is treated in confidence, and the below has been offered in anonymity from a representative of the victim, which was a large international organisation.

Under attack

"In response to a significant and sustained cyber attack, our company approached the NCSC to request support with the management of the investigation.

"The initial engagement consisted of information-sharing, triaging and establishing a cadence for future meetings. This quickly evolved into a strong and beneficial partnership, based on mutual trust, transparency and a spirit of collective responsibility."

Strengthening the defence

"After appointing Cyber Incident Response (CIR)-accredited suppliers and having further discussions with the NCSC's Incident Management team, an introduction was made to law enforcement partners.

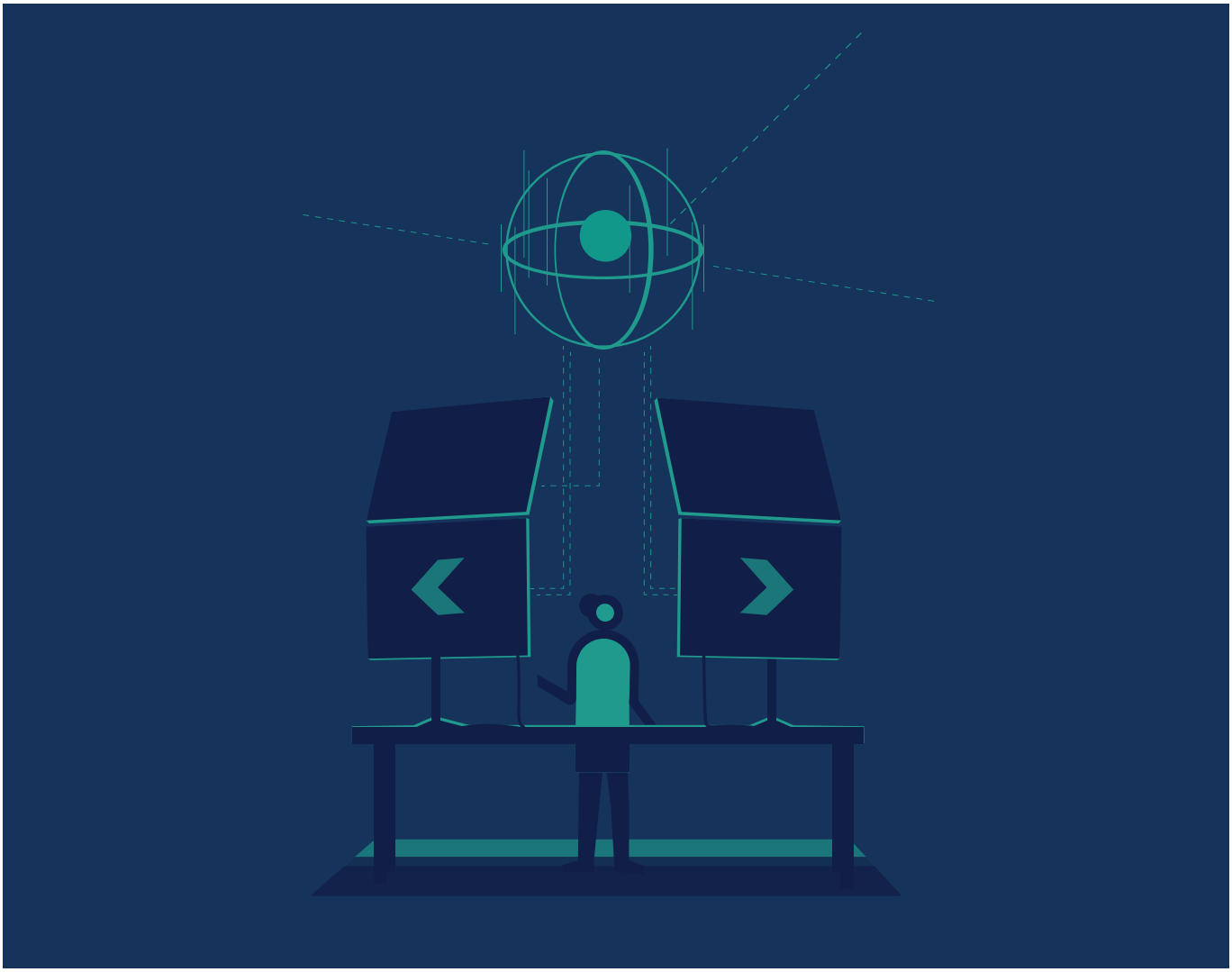
"This invoked a stream of investigative activity which not only served to stabilise a volatile and uncertain situation but materially improved our understanding of the threat actor's motives and intent.

"As a result, the company's Executive team was able to take appropriate risk-based decisions from a highly informed perspective, thereby minimising the impact of the attacker's presence on the company's operations."

The NCSC's role

"From a technical perspective, the NCSC's incident response team provided significant support throughout the full investigative lifecycle.

"Operating as a central coordination unit, the team offered ongoing recommendations and guidance, ensuring that our continuity arrangements, eradication approach, evidence gathering, and cyber uplift activities were harmonised, prioritised and correctly orchestrated."



Communicating with the public

"A highly effective relationship was also built between the NCSC and NCA Press Officers and our Corporate Affairs team. This served to ensure that consistent messaging was agreed and published in response to media speculation and enquiries from interested third parties.

"It also strengthened the assurances provided to our existing client base and perception of the partnership between the NCSC and the company to fully respond to the cyber attack."

"We owe a debt of gratitude"

"The overriding theme of the engagement was one of support, reassurance and effective team working.

"The professionalism, commitment and knowledge of the NCSC as well as the NCA was exemplary throughout the incident.

"We owe a debt of gratitude to all those involved who helped the company ensure critical operations continued to be provided to our customers during the incident and wider coronavirus pandemic."

5G in the UK

The NCSC has regularly provided essential telecommunications advice to DCMS, Ministers and the wider public that has directly influenced UK policy. A prominent example this year has been the advice related to facilitating the country's move from 4G to a more advanced 5G network.

In January, the UK Government announced plans to put in place additional safeguards and exclude high-risk vendors, such as Huawei, from "core" parts of 5G and full-fibre networks. This decision, taken by the Prime Minister-chaired National Security Council (NSC) was informed by detailed technical evidence from the NCSC as determined by the threat landscape at the time.

In a global first, detailed advice on this high-risk vendor decision was published to operators and the public, alongside a 30-page summary of the UK Government's multi-year analysis into the risks to telecoms networks. This oversight has included the Huawei Cyber Security Evaluation Centre (HCSEC), which has been running for nine years.

However, the NCSC must continually monitor global situations and update advice when appropriate. In May, the US Government placed far stricter sanctions on Huawei which the NCSC immediately understood were highly significant for the UK telecommunications sector and its security. An additional detailed analysis into the impact of the US sanctions was swiftly and thoroughly conducted by the NCSC and new advice was given to the Government.

Based on this advice, the NSC agreed that there should be greater restrictions on the use of Huawei in UK networks to ensure the security of those networks. In response, the DCMS Secretary of State announced that UK operators should stop buying Huawei equipment after 31 December 2020 and remove Huawei from the UK's 5G network by the end of 2027. Based on the NSC's decision, the NCSC published updated advice for operators and the public, and a summary of its analysis, again demonstrating its commitment to offering public transparency.

This year has demonstrated that supplier diversity is fundamental to the long-term security and resilience of the sector, alongside broader security standards. Going into 2021, the NCSC is actively supporting DCMS's diversification strategy, seeking to fix the market failings that limit vendor choice and do not value vendor security.

While supplier diversity is necessary, it is not sufficient to secure the telecoms sector. The NCSC's ground-breaking analysis into telecoms security risk identified the most critical security improvements for the sector. In close partnership with DCMS, the NCSC is using this world-leading analysis to inform the drafting of legislation, specifically the forthcoming Telecommunications (Security) Bill. Through this Bill, DCMS plans to implement one of the toughest oversight regimes in the world for telecoms security. At the same time, the NCSC is supporting operators as they seek to meet the new standard and the regulator Ofcom as it prepares to support the implementation of the standard and enforce it.



The Rt Hon Oliver Dowden CBE MP, Secretary of State for Digital, Culture, Media and Sport

"5G will be transformative for our country, but only if we have confidence in the security and resilience of the infrastructure it is built upon.

"Following US sanctions against Huawei and updated technical advice from our cyber experts, the Government has decided it is necessary to ban Huawei from our 5G networks."

Kathryn Roe, Deputy Director, Telecoms Security & Resilience, Digital Culture, Media and Sport

"The technical advice and expertise of the NCSC has been at the heart of our approach towards the telecoms supply chain review, high-risk vendors, and the development of the UK's diversification strategy.

"We are making strong progress to drive up telecoms security standards and this is testament to the excellent and seamless partnership working across DCMS and the NCSC."

Active Cyber Defence

The ACD programme seeks to stop a range of different attacks ever reaching UK citizens, institutions or businesses. Working in a relatively automated and scalable way, it removes the burden of action from the user and enables attacks to be taken down at scale.

There are six key programmes within ACD that have been rolled out:

Web Check



Helps owners of public sector websites to identify and fix common security issues – making sites in the UK a less attractive target to attackers

Protective DNS



Prevents access to known malicious domains and puts restrictions on malware communications on compromised networks

Takedown Service



Locates malicious sites and alerts hosts and owners, requesting them to remove them from the internet

Mail Check



Helps public sector email administrators improve and maintain the security of their email domains by preventing spoof emails

Vulnerability Disclosure Platform



Identifying, reporting and remediating vulnerabilities in government and other key services

Host Based Capability



Advanced NCSC threat detection capability that can be deployed to detect threats on an organisation's network

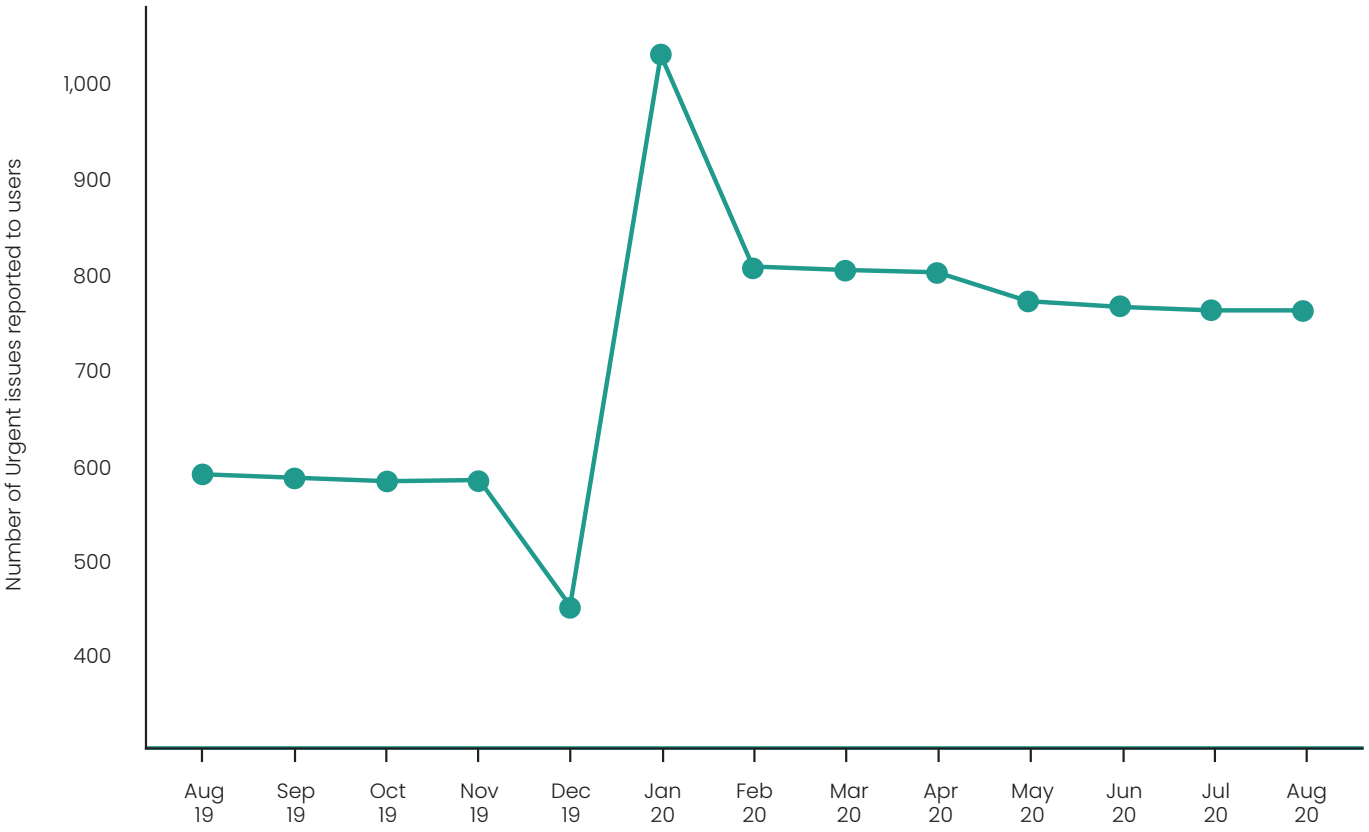
This year has seen the NCSC build on previous successes with established tools. It has enhanced functionality of its Web Check and Mail Check services, which help owners of public sector websites to identify and fix common security issues. These have since been rolled out across the public sector and beyond.

Web Check

There are now circa **3,000** service users representing over **1,000** customer organisations.

The security issues reported to them are categorised Urgent, Advisory and Informational.

Urgent issues reported to users by month



Protective DNS

2.8 million

public sector internet users protected by PDNS (estimated)

290 more

organisations using PDNS compared to one year ago, including many NHS and critical sector organisations onboarded in March, pre-pandemic peak

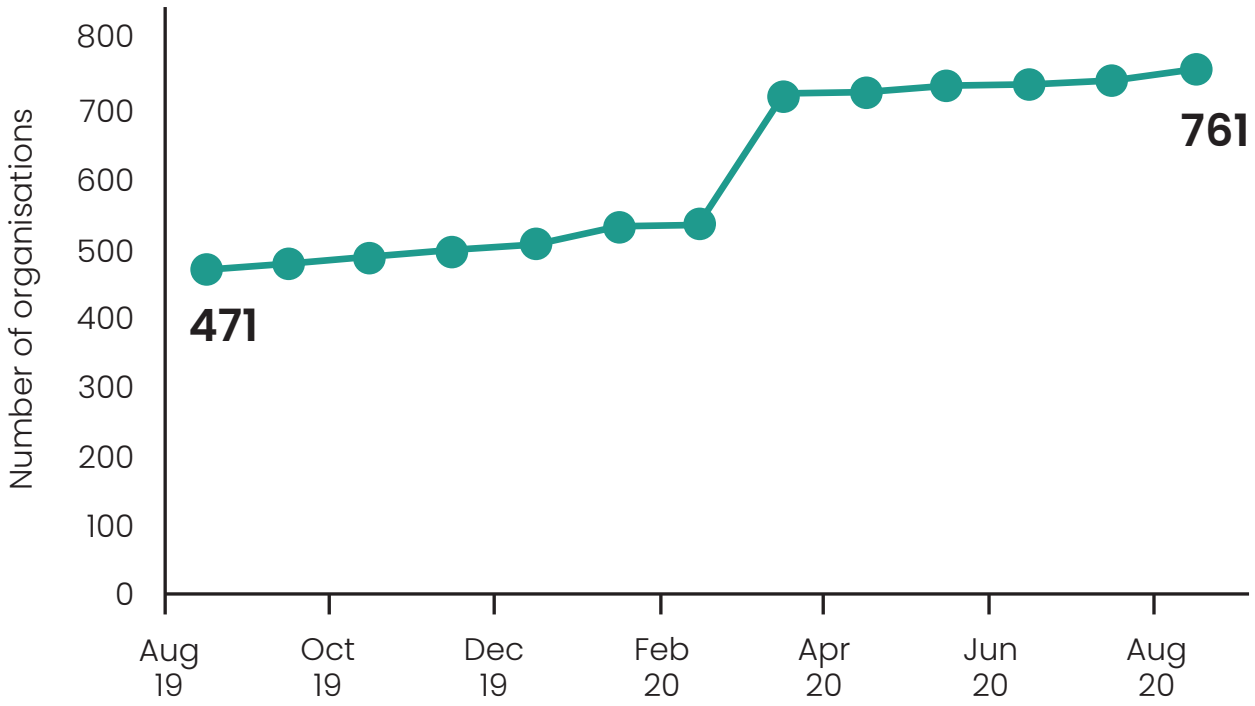
201 billion

successfully resolved PDNS queries between 1 September 2019 and 31 August 2020

760+ organisations

are using the service and it blocks around 18,000 unique domains at a rate of 7.2 million times per month

Organisations using PDNS



Takedown Service

The takedown service finds malicious content hosted on the internet and seeks to have it removed, the goal being to reduce the harm that common cyber security threats cause.

99.6% of phishing URLs discovered were successfully taken down

This totalled **166,710** phishing URLs across all campaigns

65.3% of these were removed within 24 hours of being determined malicious

42,576 URLs were associated with UK Government-themed phishing attacks, hosted globally

UK share of visible global phishing attacks further reduced to **1.27 %** (from **2.1%** last year)

Coronavirus themed takedowns

Since March, the NCSC has taken down 15,354 campaigns which used coronavirus themes in the "lure". These were hosted globally

251 phishing campaigns

8,800 were Advance Fee Fraud (419 scams)

2,984 mail servers distributing malware

1,156 were associated with fake shops selling bogus PPE, coronavirus products, test kits (and even vaccines)

Ecommerce

The NCSC started work against bogus online shopping sites (fake shops) and has taken down **113,000 URLs**.

With these sites, victims post their credit card details and will either get fake goods in return or no goods at all.

The NCSC found **1,318 sites** that had been compromised with credit card skimming malware.

The Takedown Service automatically notified the site owner and the skimming code was subsequently removed.

Mail Check

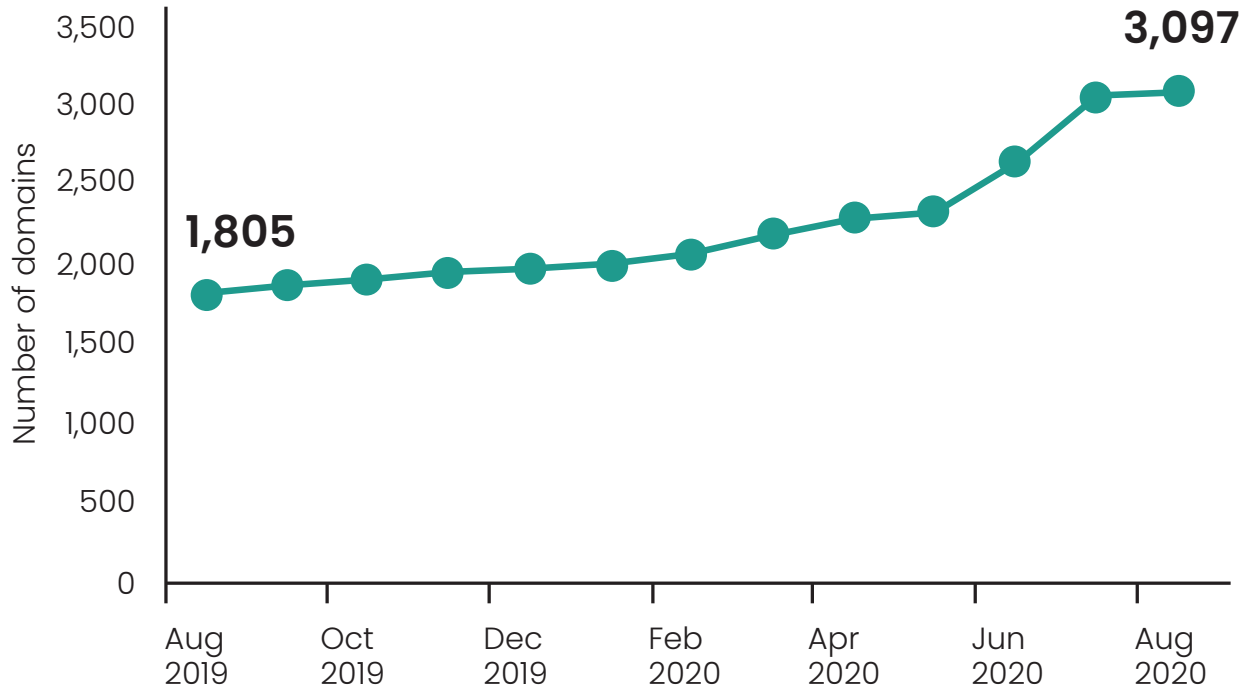
Mail Check monitors **11,417** domains classed as public sector

The number of public sector domains using DMARC nearly doubled
from 1,805
at the end of Aug 2019
to 3,097
at the end of Aug 2020

The number of public sector domains protected by a DMARC policy that blocks suspicious emails (quarantine or reject) more than doubled

from 899
at the end of Aug 2019
to 2,253
at the end of Aug 2020

Domains with DMARC



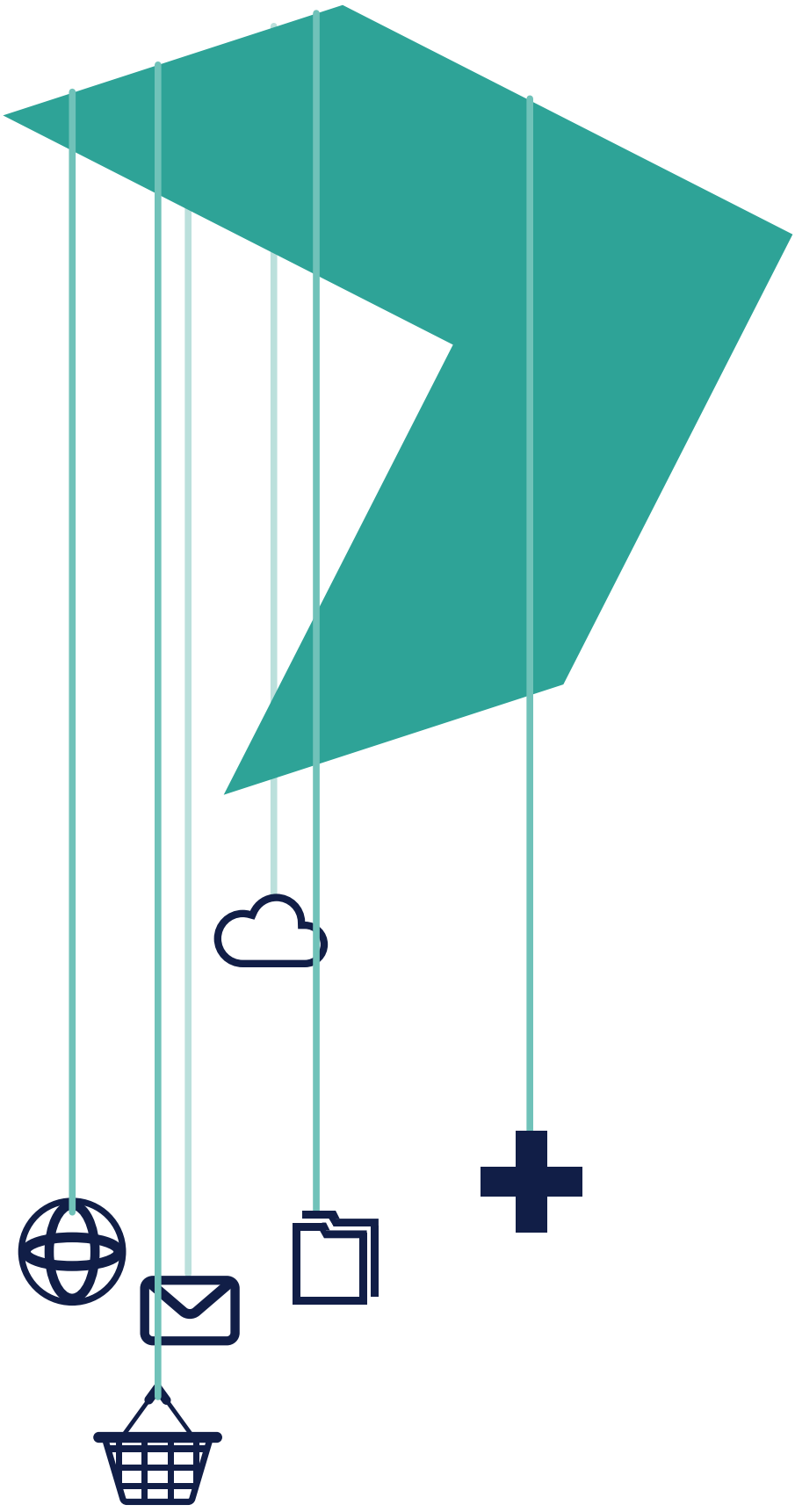
Vulnerability Disclosure: Supporting organisations and finders

Security vulnerabilities are discovered all the time and people want to be able to report them directly to the organisation responsible. The NCSC has worked with organisations and those who find security vulnerabilities to make it easier to report and therefore quicker for the system owner to remediate the issue. The NCSC runs three initiatives:

- Vulnerability Reporting Service allows vulnerabilities in UK Government services to be reported to the NCSC, if the system owner cannot be contacted. The NCSC will work to get the vulnerability information to the owner so the issue can be remediated. This year the NCSC has worked with over 150 UK Government organisations to remediate a range of security vulnerabilities
- The Vulnerability Disclosure Pilot aims to improve the UK Government's ability to adopt vulnerability disclosure best practices. Departments signed up to the pilot gain access to a dedicated platform and a technical triage service. This year seven have launched their own vulnerability disclosure processes through the pilot
- The Vulnerability Disclosure Toolkit is designed for organisations of all sizes who want to learn more about implementing a vulnerability disclosure process. It contains the essential components they need to set up their own process

Host Based Capability

The service has grown over the past year to provide coverage for 130,000 government devices (up from 35,000 last year). The NCSC continues to provide a three-part service offering (Detect, Threat Surface, and Forewarn). In addition to detecting malicious and suspicious cyber activity within government, the NCSC has cumulatively provided over 170 'Threat Surface' reports to its partners.



Detecting and mitigating vulnerabilities

The Domain Name System (DNS) is one of the core technologies used on the internet, essentially acting as a phonebook or contact list to translate between human-readable domain names and machine-readable addresses.

Like all contact lists, errors can easily be introduced from causes such as human error or information simply becoming stale and inaccurate over time. In the context of DNS, this can lead to domain names pointing to resources that are unregistered.

The NCSC refers to these as "dangling DNS records". Sometimes it's possible for an attacker to register the resource that such a record points to, therefore giving them control over what is returned to anyone who visits the domain name. This attack, known as "subdomain takeover", can have serious consequences and can result in victims being tricked into interacting with malicious websites, despite the domain name displayed in their web browser looking completely legitimate.

The NCSC's research into this issue revealed that many dangling DNS resources were associated with a small number of popular service providers. In some cases, the dangling resource could be easily registered to safeguard it from an attacker doing so for malicious purposes.

It was clear this was a systemic issue, affecting all sectors of the UK (and beyond), and the NCSC is developing a prototype platform to reduce the UK impact by performing detection and automatic mitigation at scale, starting with the public sector. The prototype identifies and protects assets provided by the four most commonly vulnerable cloud resources, as assessed by the NCSC's research.

The system analyses billions of fully qualified domain names every week and has discovered more than 62,000 vulnerable DNS records globally. This included nearly 35 vulnerable NHS domains and several others within the UK public sector. As part of the work to protect the NHS throughout the pandemic, the NCSC conducted its first automatic defensive registration of a vulnerable NHS domain in August.

Managing legacy systems

One of the most common security flaws is the use of legacy IT: software, hardware and systems that are no longer supported or able to be patched, making them vulnerable to commodity attacks. Due to budget constraints, organisations may not be able to afford to upgrade. Whilst there is no absolute solution, the NCSC is helping to make those organisations as safe as possible, by developing a legacy guidance tool which will be available in 2021 through the ACD programme.

If a user can describe their IT infrastructure, the tool will provide an indication of where weaknesses lie and point at guidance to mitigate risks.





Privileged Access Management (PAM)

Working with varied organisations allows the NCSC to identify common areas of security weakness and channel its efforts where it can have the biggest impact. One of the identified issues concerns how people manage access to system administration interfaces.

Attackers may target the credentials used to log into these interfaces and the devices that the administrators use to access them. Gaining access will reward the attacker with a high level of system privileges in the targeted environment. Similarly, system administrators could themselves also abuse their accesses – the insider threat. The NCSC has worked with a small software company to develop a solution called Big Chief, which reduces the risks and impact of this attack.

At its core, Big Chief is a web-based application that implements concepts referred to as Privileged Access Management. A minimum viable product neared completion this year, and the next stage will be user trials, after which the NCSC will explore ways – including the potential for open sourcing – to get the capability to potential users.





6

Driving cyber skills

A critical element of the UK's cyber security future is growing the skills and capabilities that will help safeguard the services and institutions the country depends on, as well as creating the opportunities and advantages that will benefit the UK and its citizens for generations to come.

The NCSC has an important part to play in fulfilling this strategic objective, and creating the next generation of cyber security experts and specialists, as well as developing today's practitioners is a key priority for the organisation.

Developing the cyber profession

The NCSC has continued to grow its own internal specialists and talent pipeline, as well as supporting the Government Security Profession and wider government cyber security community. For the latter, the NCSC shared its Technical Reconnect programme with specialists from across government. The course teaches the latest NCSC guidance to ensure delegates are familiar with cyber security best practice and can recognise the drivers behind it. Delegates learn through highly practical hands-on opportunities to build, attack and repair the various technologies that are encountered in modern security environments.

The training is delivered periodically over six months, and instructor-led training, practical lab activities, group exercises and regular consolidation exercises. Together with the NCSC's other cyber security training and development offerings, this offering quickly pivoted to online delivery as coronavirus took hold.

All 118 apprentices on the NCSC's Cyber Security Degree Apprenticeship Scheme continued their studies uninterrupted during the coronavirus pandemic.

The organisation's diverse pool of apprentices developed technical skills needed to keep the country safe and this year they have been directly contributing towards shaping the NCSC's future. The Year 1 apprentices undertook their first work-based placements this summer and helped to develop innovative projects that will directly support recovery from coronavirus. Their projects include work on distributed learning, multi-agency asynchronous working and novel learning techniques.

This year has seen the advent of a new Cyber Security Development Framework (CSDF) to support the professionalisation of cyber risk consultants and security architects. It includes a single packaged resource to enable the NCSC's staff to develop their capabilities, covering a broad range of technical and engagement-specific skills. It helps professionals understand the pathways available to them, the capabilities required for these roles, how they are recognised and how to build a plan to

CyberFirst apprentice on a Year 3 placement at the NCSC

"Working for the public-facing side of the business allows an insight you wouldn't normally see anywhere else in the building. The limits for customer engagement are endless, and the work produced always has a real influence.

"I enjoy that you can see the impact you have on customers. On top of this, the atmosphere in teams is always so friendly and encouraging, so overall the NCSC is a great organisation to work for."

CyBOK

For the first time, a guide collating the knowledge of the world's leading cyber security experts was created this year. Sponsored by the NCSC, the CyBOK is an 828-page resource offering a foundation for education, training and professional practice.

The comprehensive Body of Knowledge will inform and underpin education and professional training for the cyber sector. Launched at London's Science Museum in January, it covers the foundations of cyber security, ranging from the human element through to issues in computer hardware security.

The development of CyBOK was led by the University of Bristol and is funded by the National Cyber Security Programme with support from DCMS. The NCSC now uses CyBOK as the basis for describing the course content of the certified undergraduate and postgraduate cyber security degrees programme, as well as that for certified training.





Chris Ensor, NCSC Deputy Director for Cyber Skills and Growth

"This guide will act as a real enabler for developing cyber security as a profession. It's been developed by the community, for the community and will play a major role in education, training and professional practice."

Creating a talent pipeline

One of the most important programmes in the NCSC's future skills agenda is CyberFirst, which encourages and supports young people into the world of cyber security.

It's been an exciting year for the team and for the thousands of secondary and undergraduate students who took part in courses, competitions and applied for career-defining university bursaries to learn a host of interesting subjects such as digital forensics, ethical hacking, cryptography and cyber security challenges.



CyberFirst courses

Every summer, 1,100 free places are made available on five-day residential courses at universities across the UK. Courses were offered at three levels; Defenders (14 to 15-year-olds), Futures (15 to 16-year-olds), and Advanced (16 to 17-year-olds) – aimed at helping pupils develop the digital and problem-solving skills needed to operate in the field of cyber security.

In response to the pandemic the NCSC moved the summer courses online, with virtual classes led by instructors running from June through to August.

This year saw the highest number of applications yet (3,992) and an increase in applications from ethnic minority students (making up 23% of the total applicants) compared to previous years.

CyberFirst Bursary and Academy

The Bursary scheme continued to grow this year, attracting highly motivated and talented undergraduates. There are now more than 900 hand-picked students either currently on or recently graduated from the scheme.

This summer, 165 undergraduates attended an eight-week virtual CyberFirst Academy programme and a further 224 students were placed with industry and government members or on further online training programmes – providing invaluable work experience to help make the UK the safest place to live and work online.

CyberFirst Schools

Since 2018, the NCSC has been piloting a Cyber Schools Hub (CSH) programme in Gloucestershire. The CSH has encouraged collaboration between schools, the NCSC and national and local organisations which share the aim of encouraging young people to engage with computer science and the application of cyber security in everyday technology.

The CyberFirst Schools programme was officially launched on 26 February and is currently available to schools in Gloucestershire, Wales, Northern Ireland and the North East of England.

CyberFirst Bursary Student, end of year review

"The Academy was an amazing experience that has had a massive impact on me and my summer placement was amazing.

"I had a great time and discovered so much more about cyber security, possibly even solidifying what I want to do going into the future in terms of career choice."

CyberFirst Bursary student, end of year review

"I'm incredibly pleased with my summer placement, the project was joint with a government agency and I was able to conduct research and learn aspects of cyber security which I'd never have considered previously."

CyberFirst Girls' Competition Winners



Kirsty Williams, Minister for Education, Welsh Government

"I'm really pleased that the NCSC also chose to pilot the CyberFirst Schools programme here in Wales, and we'll continue to work closely with the NCSC to actively encourage schools and colleges in Wales to take advantage of the excellent opportunities provided by CyberFirst."

Carole Pennington, Chief Commissioner of Girlguiding South West

"Awareness of cyber security is vital for all our members, and the activities in the resource have been designed to provide fun ways of learning about computer systems and cyber security.

"Because many of our units meet in locations with no internet or computer access, the activities are not reliant on their use and can be enjoyed by everyone, wherever they meet. I'm sure this resource and the related badges will prove to be very popular."

Girl Guides

As part of its ongoing drive to increase female representation in cyber security, the NCSC worked with the South West division of Girlguiding UK to develop a badge and supporting activity pack called 'On the Net'.

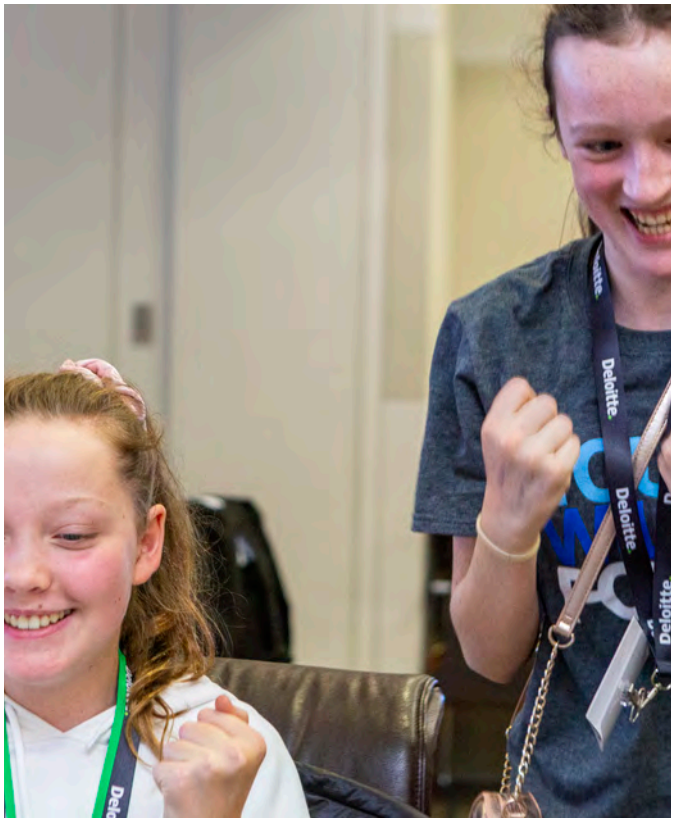
The initiative was launched in February at the University of the West of England (UWE), where 100 girls aged between 12 and 14 were invited to learn about online safety and how cyber skills can lead to career opportunities in cyber security – a field in which women remain under-represented.

During the event the girls participated in a series of interactive sessions, with the topics ranging from website customisation and use of big data to digital forensics and cryptography. Fictional scenarios were used to help the participants see the relevance of the skills they were learning. The day presented an opportunity to learn about the variety of jobs and career paths in cyber security which studying computer science can lead to.

The pack produced by the NCSC and Girlguiding South West includes a range of activities for girls to complete within their units before badges can be collected. It covers all ages within Guiding, from Rainbows to Rangers.

CyberFirst Girls' Competition 2020



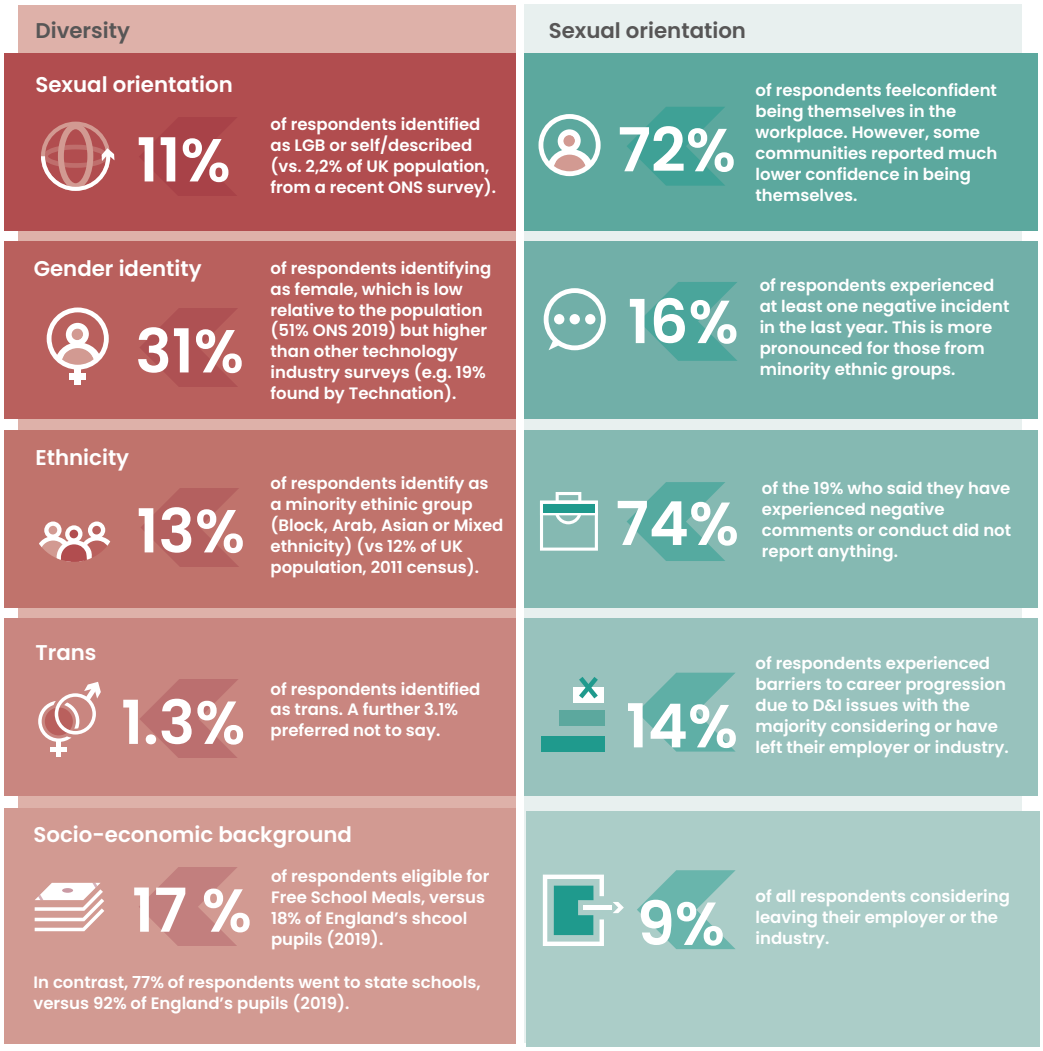


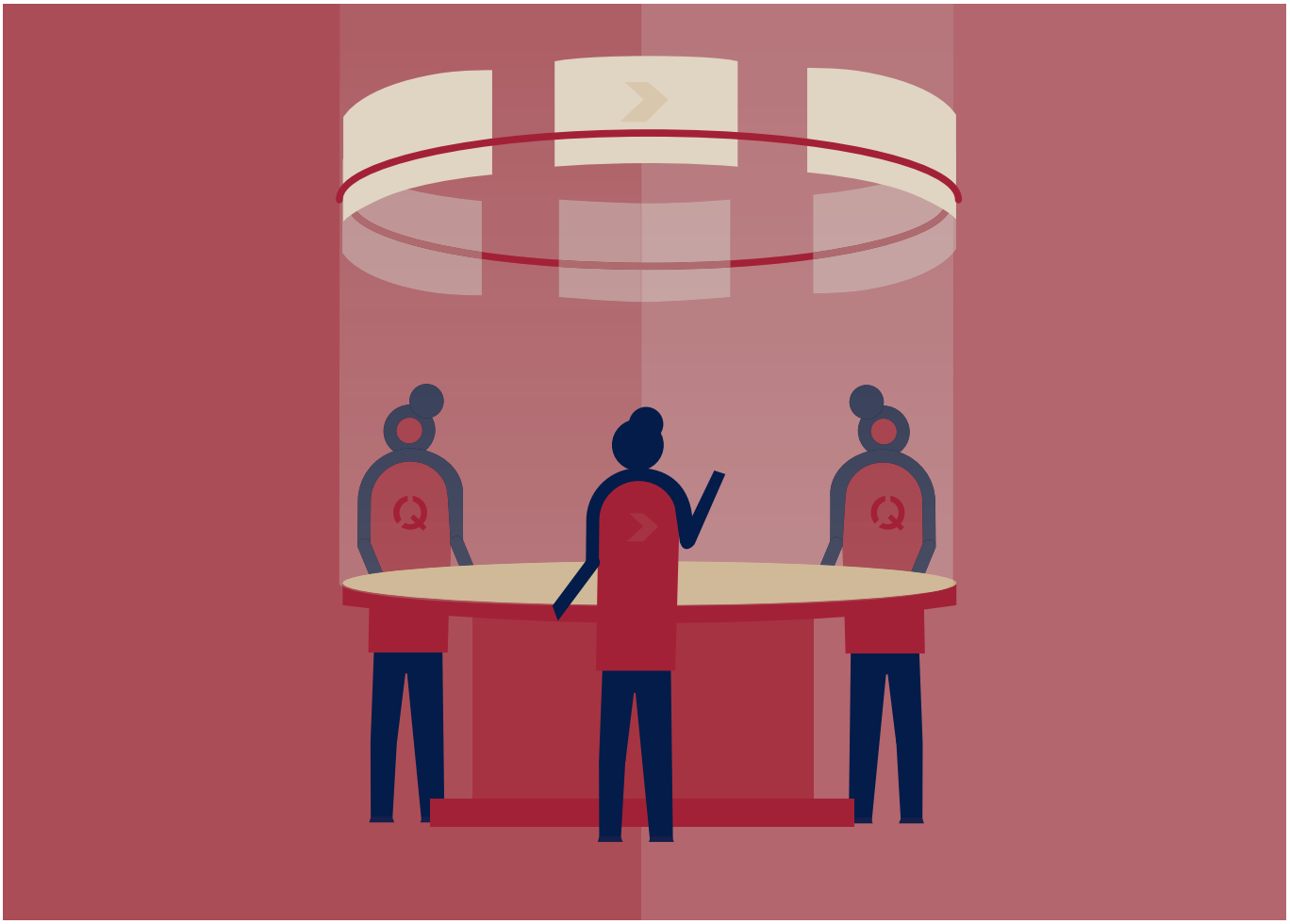
Diversity and inclusion

The NCSC partnered with KPMG to produce the first-ever review of diversity and inclusion in the cyber security sector. The report set an initial benchmark in the UK's cyber security industry and began a long-term programme to make the profession more diverse and inclusive.

Inclusive language

In April, the NCSC published a blog post talking about the decision to stop using the terms "blacklist" and "whitelist" on its website. It's a small change, but one that the NCSC hopes is useful as part of the organisation's wider anti-racism efforts. The blog post resonated with many people across the UK, with several getting in touch to thank the NCSC for taking this step, and to say that this leadership has emboldened them to make similar changes in their own workplaces. The NCSC is proud to have added its voice to the wider discussion around the use of discriminatory terminology in tech. The organisation wants cyber security to be an inclusive and welcoming place for everyone, and recognises that its language should always reflect that.





Manchester Hub

In September, a team from the NCSC joined colleagues at GCHQ who have established a new research hub in the centre of Manchester, with the aim to foster increased collaboration with the city's burgeoning number of tech experts in business and academia.

Acknowledging that the city has one of the fastest growing digital and creative communities in Europe, the NCSC will be recruiting further personnel to join those experts already in place, with a brief to support its mission on protecting CNI. The CNI mission at the Manchester Hub will include such areas as energy, transport, finance and smart cities.



7

International influence

It has been a year of two halves for the NCSC in terms of how it has engaged internationally. Between September 2019 and March 2020, the NCSC welcomed delegations from more than 20 different countries, and NCSC representatives visited a similar number for bilateral and multilateral engagements, and participated in cyber security conferences.

However, the impact of the coronavirus pandemic necessitated a shift to virtual engagement. Since March, the NCSC has taken part in 46 international engagements – meaning despite fewer face-to-face meetings, it has still been possible to maintain global reach and influence.

A global perspective

The NCSC's technical expertise affords the UK a vital source of thought leadership and influence overseas. International engagement with partners continues to be a central component of the NCSC's work to enhance the UK's cyber security and resilience. The NCSC regards cyber security as a global issue that is most effectively addressed together. By sharing information and working with international partners, not only can the NCSC better protect the UK, but it can also influence and assist its partners to do the same for their own countries.

Owing to the unique nature of cyber security as a domain, the NCSC's international collaboration goes beyond conventional forms of engagement, or cyber diplomacy.

Examples include:

- Time-critical emergency response collaboration on live cyber incidents
- Engaging with cyber security leaders on policy matters in global forums
- Sharing best practice on operational technologies with overseas cyber security agencies
- Working with companies headquartered overseas with links to the UK to ensure their cyber security practices are robust
- Sharing ACD services

Dr Henry Pearson, UK Cyber Security Ambassador, Department for International Trade

"From my engagements in many countries around the world it is very clear that the NCSC continues to set the benchmark against which other national cyber security organisations can measure themselves. It forms a cornerstone to the UK's continued ambitions as a cyber power and an important underpinning element of UK cyber security companies' offer in their overseas markets."





Stronger together

The UK has a long-held security alliance with the USA, Canada, Australia and New Zealand, known as "the Five Eyes". The alignment between the countries facilitates greater information-sharing across a wide range of cyber security issues.

One such example of this close working relationship was the creation an incident response playbook that could be applicable to the widest set of countries and situations possible.

With the NCSC leading the agenda, using its experiences and skills in incident management, the objective was to offer a product that an organisation or institution overseas could grab "off the shelf' during a crisis, providing best practice on starting an investigation and serving as a check list for a cyber incident response.

As cyber threats become more numerous, more technically diverse and more damaging, the NCSC continues to drive the agenda in international collaboration to help boost the resilience of its strategic partners and to help deter the UK's adversaries.

Paul Chichester, NCSC Director of Operations

"Cyber security is a global issue that requires a collaborative international effort to protect our most critical assets.

"This advisory will help organisations understand how to investigate cyber incidents and protect themselves online, and we would urge them to follow the guidance carefully.

"Working closely with our allies, and with the help of organisations and the wider public, we will continue to strengthen our defences to make us the hardest possible target for our adversaries."



Chris Krebs, Director, Cybersecurity and Infrastructure Security Agenda, USA

"With our allied cyber security government partners, we work together every day to help improve and strengthen the cyber security of organisations and sectors of our economy that are increasingly targeted by criminals and nation states alike.

"Fortunately, there's strength in numbers and this unified approach to combining our experiences with a range of malicious actors means that we're able to extend our defensive umbrella on a global scale."

Abigail Bradshaw CSC, Head of the Australian Cyber Security Centre

"At the Australian Cyber Security Centre, we collaborate closely with our international partners by sharing threat intelligence, technical tradecraft and indicators of compromise. Our joint advisories with Five Eyes nations are crucial to ensuring that valuable threat information is shared quickly and efficiently, to mitigate and protect against malicious cyber activity around the world.

"The long-standing relationship between the Australian Signals Directorate (ASD) and GCHQ is an important force multiplier for our cyber security efforts, and our joint operations to combat cyber criminals is a prime example. In one case from the last year, our collaboration identified over 200,000 stolen credit cards globally, including over 11,000 stolen Australian cards. These stolen credit cards represent potential losses of over A$90 million globally, and over A$7.5 million within Australia."

Scott Jones, Head, Canadian Centre for Cyber Security, Communications Security Establishment

"Coronavirus has had a profound impact on the world. This uncertain environment is ripe for exploitation by threat actors seeking to advance their own interests. To counter these threats, the Canadian Centre for Cyber Security (Cyber Centre) is working hand-in-hand with the NCSC to detect and disrupt shared threats. We exchange information to better protect our health sectors and over the past year, we have released cyber alerts and threat bulletins leveraging each other's reporting and advice. Furthermore, we issued technical information about cyber threat activity directed at Canadian and United Kingdom organisations, including vaccine research entities, involved in coronavirus response and recovery efforts.

"The Cyber Centre and the NCSC continue to work together to protect critical infrastructure sectors from cyber threats, through regular information exchanges and by working collaboratively on joint programmes and initiatives. For example, the NCSC has leveraged and deployed some of the Cyber Centre's defensive capabilities across UK Government departments. Similarly, the Cyber Centre has been promoting items such as DMARC where the NCSC was leading.

"We continue to share knowledge and threat information with each other on important and challenging topics including cloud security, encryption and cryptology, and election security. Looking ahead, we will continue to amplify each other's notifications on critical cyber threats to raise awareness of the evolving threats in our respective countries."

Singapore Cyber Week

In October, then NCSC CEO Ciaran Martin led a UK delegation at one of the most significant cyber policy gatherings in the Asia-Pacific region: Singapore International Cyber Week (SICW). He was accompanied by representatives from the UK cyber industry, academia and government.

At a bilateral meeting between the UK and Singapore, covering issues including information-sharing and collaboration on emerging priorities and technology, the two countries signed an IoT Security Statement. The signing demonstrated the UK's international leadership in improvements in the security of smart consumer products, and strengthened the relationship with a partner in a region of strategic importance to UK interests.



Natalie Black, HM Trade Commissioner for Asia Pacific

"The UK was delighted to play an active role in SICW 2019. International partnerships across industry, academia and government are key to a safe and secure cyberspace.

"We were particularly pleased that the CEO of the NCSC joined us in Singapore and signed a joint statement of cooperation between our two nations on the Internet of Things."

Global cooperation on operational technology and industrial control systems

The UK's CNI has a number of dependencies overseas with Operational Technology (OT) and related Industrial Control Systems (ICS) being used across the world to monitor, control and manage the operation of physical assets linked to key CNI areas such as energy and finance. The threat to OT / ICS is real, and the NCSC has seen examples internationally, where OT has been negatively impacted by cyber attacks, ranging from modifying how an industrial process operates, through to disrupting them altogether.

Strengthening the cyber resilience of the global OT and ICS is a priority for the NCSC and its international partners. Some of the NCSC's virtual engagements on this matter this year included joint working with counterparts in the US. The NCSC's 'Secure Design Principles' blog and CISA's 'Industrial Controls Systems Cybersecurity Best Practices' guide, launched in May, signified a joint commitment by the UK and United States to protecting their nations' respective ICS infrastructure.

The joint venture set out risks faced by ICS owners and operators of interconnected operational and information technology including IoT, to help them design and secure ICS, mitigate risks, and protect against the ever-evolving threats.

The product also features operational CISA assessments data, along with proactive defensive practices to help CNI stakeholders defend ICS against cyber attacks and encourage a long-term, strategic approach to ICS protection.

Looking ahead, the coordination and sharing of technical research, resulting in multi-national publications, will continue to be an important area for the UK ICS Community of Interest contribution – and a key way in which technical collaboration can enhance the security of the UK and overseas partners.

Bryan Ware, Assistant Director for Cybersecurity, US Cybersecurity and Infrastructure Security Agency

"Cyber threats don't care about borders, so collaboration between international partners is key to raising our collective cyber security.

"CISA and the NCSC have worked together on a number of important efforts over the past year, such as the NCSC's 'Secure Design Principles' blog, CISA's 'Industrial Control Systems Cybersecurity Best Practices' infographic and joint advisories about nation state and malicious cyber actors.

"We look forward to working with the NCSC on other actionable, informative and timely products to protect critical infrastructure and our citizens."

Collective action on incidents

The NCSC is proud to work with global partners to detect and disrupt shared threats. One of its key strengths in international collaboration is on cyber incident management and response, in which the ability to work alongside international partners is fundamental. For example, when investigating reports of a ransomware infection that had not been seen in the UK before, law enforcement colleagues in the NCA observed and reported that their investigations had shown a similar ransomware strain that had previously been decrypted by the Polish NCSC equivalent, CERT Polska.

The NCSC contacted the CERT Polska team to gain further information on the ransomware variant, and about the tool it had developed to decrypt it. The team at CERT Polska was open to collaboration and provided the NCSC with the code behind its decryptor, explaining how this could be turned into a standalone tool that could be used to support the UK victim.

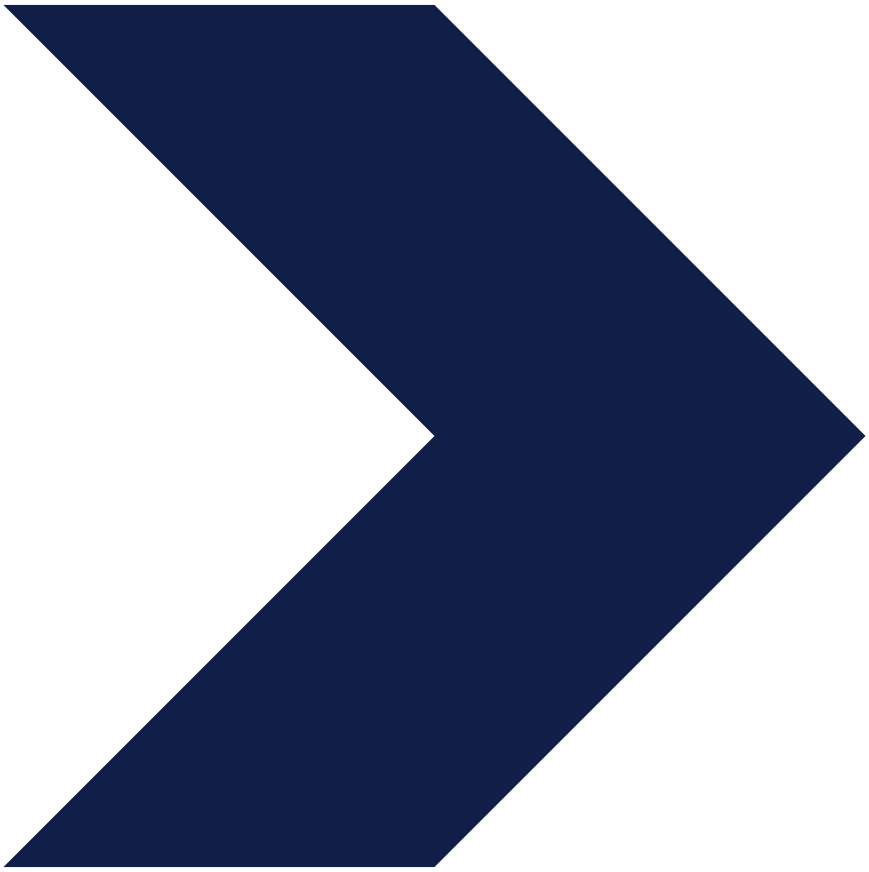
The NCSC's cryptographic architects built a proof of concept using the CERT Polska decryptor and the tool was launched for real-world use. Working with NCC Group, the UK victim's accredited cyber security incident response provider, the NCSC was able to provide corresponding decryption keys to create multiple versions of the tool, scaling up the number of simultaneous decryptions to support the victim's recovery.

This example of operational collaboration between the NCSC and international and industry partners, meant that the NCSC could scale-up the number of decryption jobs running at any one time – essential when dealing with multiple different ransomware events, each with a separate decryption key. It also demonstrated the value of the UK's incident response approach with overseas partners – one that keeps the victim at the centre of the response.

Will Middleton, Director Cyber, Foreign, Commonwealth and Development Office

"The NCSC's world-leading expertise has provided a strong foundation at home for our efforts overseas to protect and promote a free, open, peaceful and secure cyberspace.

"The respect and admiration it commands from international partners has opened doors for our diplomats, and it has been generous in sharing its skills and knowledge to strengthen global resilience and security."



Annual Review 2020

Making the UK the safest place to live and work online

ncsc.gov.uk/annual-review-2020

National Cyber Security Centre | Annual Review 2020

@NCSC

National Cyber Security Centre

@cyberhq

To request the information in this document in an alternative format please email enquiries@ncsc.gov.uk

© Crown copyright 2020. Photographs produced with permission from third parties. NCSC information licensed for re-use under Open Government Licence(http://www.nationalarchives.gov.uk/doc/open-government-licence).

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C113965