National Cyber Security Centre
a part of GCHQ

Annual Review 2019

Making the UK the safest place to live and work online

Welcome

Since the National Cyber Security Centre (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 review of its third year provides an update on some of the latest developments and highlights, with interviews, data and a chance to hear from some of the people working on the NCSC's mission. It provides a snapshot of the organisation's work over the period 1 September 2018 to 31 August 2019, with some key milestones along the way.

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-2019

National Cyber Security Centre
a part of GCHQ

GCHQ

Ministerial foreword

The United Kingdom has one of the most digitally-developed economies in the world, transforming the lives of citizens, driving innovation, and fuelling job opportunities and national growth. We can be proud that in the National Cyber Security Centre (NCSC) we have a world-leading body for digital protection which, since its launch in 2016, has made the UK safer and its defences stronger. Ensuring the UK remains the most secure place to live and do business online, and upholding public trust in our digital systems, are personal priorities for me and a key part of this government's vision for the UK. As the Cabinet Office Minister responsible for resilience and the National Cyber Security Strategy, I very much welcome the achievements and progress laid out in this Annual Review.

Establishing the NCSC was a key pillar of the National Cyber Security Strategy 2016-2021, which has transformed the UK's fight against evolving online threats posed by criminals, hacktivists and hostile nation states. Backed by £1.9 billion in funding, and with a deliberately interventionist and comprehensive approach, the Strategy is acclaimed by other nations as a model of its kind. Any digital economy must be alert to new threats, and to changes in existing threats. The NCSC benefits from being part of GCHQ: it fuses the best of our national security capabilities with cutting-edge technical knowledge to thwart the menace of global cyber crime. In October 2018, for example, its work ensured that the UK and our allies were able to expose attacks launched by Russian military intelligence on political institutions, and business, media and sporting interests.

The NCSC works on behalf of many millions of citizens and organisations. This Annual Review reveals important technical interventions on behalf of individuals and families, as well as for businesses, national and local government, and critical national infrastructure. One such example of this is the ground-breaking work it has done to reduce credit card fraud, preventing hundreds of thousands of cases in the past year.

On the international stage, too, the NCSC is extremely active. It shares the UK's specialist knowledge across borders to help strengthen global cyber defences and shape global attitudes to deterring and tackling cyber crime wherever it may originate. Over the past year this has included a drive to increase the security protection on the "Internet of Things" – digital devices embedded in everyday objects manufactured around the world, ranging from video doorbells and "nanny-cams" to fridges and ovens, which enable them to send and receive data. This is a concern for our government, as the Prime Minister made clear in September 2019 during his speech to the United Nations General Assembly, when he called for emerging technologies to be designed with the right safeguards already in place to protect people. We can all be proud of the NCSC's influence already in this area, working closely with partners across government and internationally.

Every chapter of the NCSC's Annual Review is testament to the hard work and achievements of its staff and leadership. The NCSC operates in a complex landscape in which the contours are constantly changing and there is no room for complacency. Securing the internet is a 24/7 challenge, 365 days a year, and cannot be shouldered by any one organisation. While the government, through the National Cyber Security Strategy and Centre, can lead the way, we are also dependent on our partners in industry and academia - and across society as a whole - for a joint approach to tackling cyber security. This is a long-term mission, and I congratulate the NCSC for helping to build a pipeline of specialist talent for the future to achieve this. One of the many ways it supports this mission is through its CyberFirst programme, which develops the careers and expertise of our younger digital natives and brings new generations into the UK's fight for a more resilient digital future.

It is impossible to predict what the future will look like. But we know that we have the organisation and the tools we need to look ahead and remain resilient. Through the Strategy, and the tireless work of the NCSC, we are scaling up the systems, structures and capabilities necessary to respond quickly to threats – not only now, but to the end of the Strategy and beyond.

Rt Hon Oliver Dowden CBE MP,
Paymaster General and Minister for the Cabinet Office

Contents

Annual Review 2019

CEO foreword

It is a privilege to present the National Cyber Security Centre's third Annual Review.

It's very hard to condense the world-leading work the NCSC does in 12 months into one document, but I hope this review gives you an insight into what we are doing to understand, reduce and respond to cyber attacks.

There certainly is a lot to be proud of – for example, thanks to the innovation of our technical experts, we have been able to increase the number of threat indicators we share by tenfold to more than 1,000 per month, and the speed we process them from days to seconds.

There is of course much work to do – as shown by the 658 incidents we supported this year. For the first time ever, in this review, these incidents are broken down into the most affected sectors. We believe that being transparent helps to target the interventions we need to help those who are most vulnerable.

However, sometimes transparency has its limits. A significant proportion of our work has continued to take the form of defending against hostile state actors. We can say that Russia, China, Iran and North Korea continue to pose strategic national security threats to the UK, but we can't often talk about the operational successes and the full range of the NCSC, GCHQ and wider state capabilities that are deployed against them.

Whether it's state attacks or global cyber crime, it's the basics that matter. The most immediate threats to UK citizens and businesses come from large scale global cyber crime. Despite often being low in sophistication, these attacks threaten our social fabric, our way of life and our economic prosperity. That is why so much of the NCSC's efforts are geared towards raising our defences against all threats in cyberspace. There are many operational successes in this field – particularly our pioneering Active Cyber Defence work.

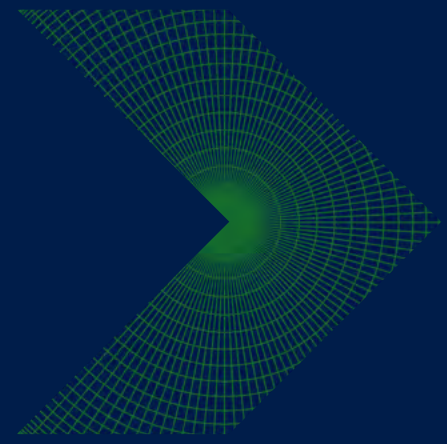
Looking ahead, there is also the risk that advanced cyber attack techniques could find their way into the hands of new actors, through proliferation of such tools on the open market. Additionally, we must always be mindful of the risk of accidental impact from other attacks. Cyber security has moved away from the exclusive prevail of security and intelligence agencies towards one that needs the involvement of all of government, and indeed all of society.

The importance of partnerships in cyber security, both at home and abroad, cannot be over emphasised. We are learning that securing the nation's digital future is not just about protecting networks and devices – it's about inspiring a safe and trusted product base, and a skilled and diverse workforce who can make the cyber landscape work for the whole of the UK.

At a time when confidence in the internet across the world is under strain, there is much within this review to inspire pride and optimism. The NCSC is proud to have helped to deliver the Cabinet Office-led strategy to make the country the safest place to live and work online, and this year the UK was rated first in the Global Cyber Security Index published by the International Telecommunication Union (ITU).

None of our achievements would be possible if it were not for the exceptional people I am delighted to call my colleagues at the NCSC. The work they do inspires me on a daily basis, and it is an honour to lead them.

Ciaran Martin
CEO of the National Cyber Security Centre



Timeline

This covers the period **1 September 2018 to 31 August 2019**

2018

12 Sept
NCSC CEO delivers speech at the Confederation of British Industry's Cyber Conference to help business leaders understand and manage cyber security risks

14 Oct
Secure by Design 'Code of Practice for Consumer Internet of Things Security' published with the Department of Digital, Culture, Media and Sport

23 Nov
Advice to shop safely online on Black Friday and Cyber Monday published in partnership with retailers

20 Dec
UK and allies expose APT10 of cyber attacks on intellectual property and sensitive commercial data in Europe, Asia and the US

03 Oct
UK, Dutch and other allies expose GRU (Russian military intelligence) cyber attacks targeting political institutions, businesses, media and sport

22 Nov
NCSC CEO meets with the First Minister of Scotland, Members of the Scottish Parliament and the Chief Constable of Police Scotland in Edinburgh to discuss ways to boost cyber security in Scotland

29 Nov
UK's 'Equities Process' published on how vulnerabilities are identified and handled

2019

7 Jan
Guidance on cyber security for major events published

13 Feb
NCSC Directors meet with Ministers at the National Assembly for Wales in Cardiff to discuss how to boost Welsh cyber defences

21 Mar
NCSC Board Toolkit launched to encourage essential cyber security discussions between the Board and their technical experts

28 Mar
Fifth annual report from the Huawei Cyber Security Evaluation Centre Oversight Board published

29 Jan
Academic Centres of Excellence in Cyber Security Research visit NCSC headquarters to take part in strategic discussions

12 Mar
New NCSC web platform launched including bespoke guidance for six new audience categories

24-25 Mar
Royal Masonic School for Girls crowned winners of the NCSC's CyberFirst Girls Competition at the final which took place in Edinburgh

Annual Review 2019

24-25 Apr
CYBERUK 2019 hosted in Glasgow

23 May
NATO Cyber Defence Pledge Conference held at NCSC headquarters

13 June
'Top Tips for Staff' e-learning package launched

25 June
De Montfort and Northumbria Universities recognised as Academic Centres of Excellence in Cyber Security Research

16 July
'Active Cyber Defence – the second year' report published

Aug
Appointment of IASME Consortium Ltd as new Cyber Essentials partner

2019

25 Apr
Exercise in a Box online tool launched to help organisations test and practice their response to a cyber attack

11 June
Guidance for small businesses to respond and recover from a cyber incident published

18 June
150 women from across the UK's intelligence, government and security communities attended the 'Women in Security Network' event held at NCSC headquarters

10 July
Seven companies graduate from the NCSC Cyber Accelerator for innovative start-ups

July / Aug
22 CyberFirst summer courses for children and young adults held throughout the country to develop the UK's next generation of cyber professionals

Year Three Highlight Statistics

- Handled **658** incidents
- Provided support to almost **900** victim organisations
- Produced **154** threat assessments
- Took down **177,335** phishing URLs, **62.4%** of which were removed within 24 hours
- **2.8 million** visitors to the NCSC's website
- Added more than **5,000** new members onto the Cyber Security Information Sharing Partnership
- Produced **108,411** physical items for **170** customers through the UK Key Production Authority
- Produced **34** pieces of guidance and **69** blogs
- Awarded **14,234** Cyber Essentials certificates
- Enabled **2,886** small businesses across the UK to do simulated cyber exercising for themselves
- Challenged **11,802** girls in the 2019 CyberFirst Girls Competition
- Engaged with **2,614** students on the NCSC's CyberFirst courses
- Supported **250** extra teaching hours of computer science across **4** schools through Cyber Schools Hub activities
- Delivered, along with sector and law enforcement partners, cyber security awareness and training sessions to more than **2,700** charities
- **20** countries visited by the NCSC
- Welcomed visiting delegations from **56** countries
- Hosted **197** events, with more than **9,000** attendees

1 Cyber security for individuals and families

The government's vision is for the UK to be prosperous and confident in the digital world whilst remaining secure and resilient to cyber threats. Central to the NCSC's mission is ensuring people of all ages across the UK are more secure when using internet-connected devices and online services.

The NCSC understands people's attitudes and behaviours towards cyber security and targets efforts based on its understanding of risk and vulnerability. The NCSC's approach enables constant learning, by joining up the threat picture and intelligence with continually evolving insight, based on deep experience of managing incidents.

It will take a holistic approach to deliver cyber security for individuals and families through the following interventions:

Reducing the burden
The general public is protected from the majority of online harm ever reaching them. The action they need to take to secure their devices and online services is minimal.

Making it easier
Citizens can act upon the cyber security advice they receive, whatever device or online service they use.

Equipping the nation
People are given the confidence and tools to protect themselves and those around them.

Raising awareness
Enabling the general public to better protect themselves and share knowledge with others.

Understanding the threat

In the year ending March 2019, it is estimated that there were just under one million (966,000) incidents of computer misuse experienced by adults aged 16 and over.[1]

Whilst this represents a significant reduction on the previous year, the large volume still shows that we cannot be complacent.

Some typical ways in which criminals access citizens' online activity are through sending malicious emails, social engineering (the manipulation of people into performing an action or giving away confidential information), water holing (a website infected with malware or containing a link to malware) and by making them download malicious software and apps.

Once the criminals have access, they can use malware and ransomware to access individuals' accounts, steal data, and even stop people accessing their own files, accounts and devices.

Making cyber security relevant to people in their everyday lives

The NCSC's approach to 'you-shaped' security

The NCSC is dedicated to finding ways of making cyber security relevant to people in their everyday lives.

"We look at the interaction between people and technology and try to make it easier for people to be secure as they get on with all the things they need to do," says the NCSC's Helen.

"One of the most important things we've seen is the changing mindset between the idea of 'let's alter the behaviour of the person or assume they are going to make a mistake' to 'how can we support developers to make more secure and user-friendly products?'"

Ceri, another NCSC expert, says "We are looking to move security away from being mainly about threat and vulnerability – the idea that there's always somebody trying to attack you – to a more positive conversation that shows people security should not be a barrier to things they want to do.

"Instead of forcing security rules on people, we are aiming to make it more approachable through clearer language. To do this, we look towards experts in communications, marketing and advertising, to refresh the message, always with the aim of ensuring the public feel that security is a help, not a hindrance. There is a lot of work that goes into ensuring that a simple message reaches the right spot."

The NCSC's advice for individuals and families

Protect your accounts...

- Use a unique and separate password for your email
- Use three random words to create a strong and memorable password
- Store your passwords somewhere safe: save to your browser or use a password manager
- Add extra security to important online accounts: turn on two-factor authentication

Look after your devices...

- Set your phone and tablet to automatically update
- Install the latest updates on your phone and tablet when prompted
- Turn on back up for data stored on your phone and tablet

1 Crime Survey for England and Wales 2019

Reducing the burden: Secure by Design

Many consumer products that are connected to the internet are found to lack basic security features, putting consumers' privacy and security at risk. The NCSC has been working closely with the Department for Digital, Culture, Media and Sport (DCMS) to support consumer 'Internet of Things' (IoT) manufacturers of all sizes to ensure their devices have good cyber security practices built in from the design stage.

As the UK's lead technical authority, the NCSC provided the technical grounding and insight for the government's Secure by Design Code of Practice for consumer IoT security, published in October 2018. The code presents a clear set of 13 guidelines for manufacturers to embed into their devices.

The NCSC and DCMS engage with international standards bodies that create industry-led standards for IoT security. In February 2019, the European Telecommunications Standards Institute (ETSI) launched the first globally applicable standard on the cyber security of internet-connected consumer devices, ETSI TS 103 645. This technical specification builds on the Code of Practice, creating a community-driven standard with a global scope.

The NCSC and DCMS do not think it is right to expect all consumers to be 'cyber security experts' and wish to remove the burden from them having to differentiate products that do or do not take their responsibility to security seriously. That's why the NCSC has also worked closely with DCMS' consultation on regulation, preparing to eradicate worst practice and embed transparency between the manufacturer and the consumer at the point of purchase.

Alongside work encouraging, and eventually mandating, manufacturers to make (and keep) their products secure, the NCSC and DCMS have published guidance to help people protect themselves. Grounded in its technical expertise, this includes advice on setting up devices, checking default settings, and managing updates.

"The progress we have made on 'Secure by Design' has been the product of a great partnership between DCMS and the NCSC. Both on the development of standards that are based in the language of our Code of Practice, or through productive challenge sessions on our future regulation proposals, we work together as a united front towards our ambition of protecting citizens and the wider economy from harm."

Peter Stephens, Head of Secure by Design, Department for Digital, Culture, Media and Sport

"Everybody needs to know how to stay safe online, and our new website is full of actionable advice to protect you and your loved ones.

"While it is formed from the expertise of the UK's top cyber security brains, it's vital that the advice can be understood by everyone."

Nicola Hudson, Director Policy and Communications, NCSC

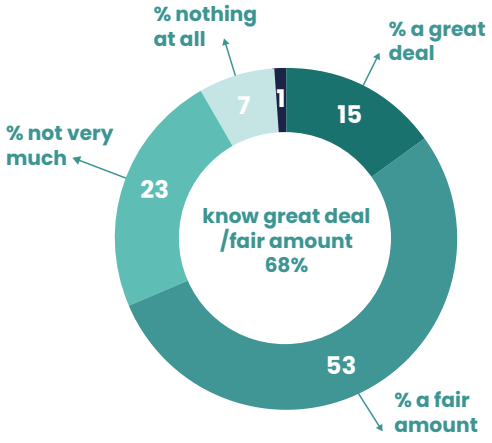
UK Cyber Survey 2019

The first UK Cyber Survey was conducted this year to better understand what the general public and organisations think, feel and do – and don't do – about cyber security across the country.

The polling was independently carried out on behalf of the NCSC and DCMS.

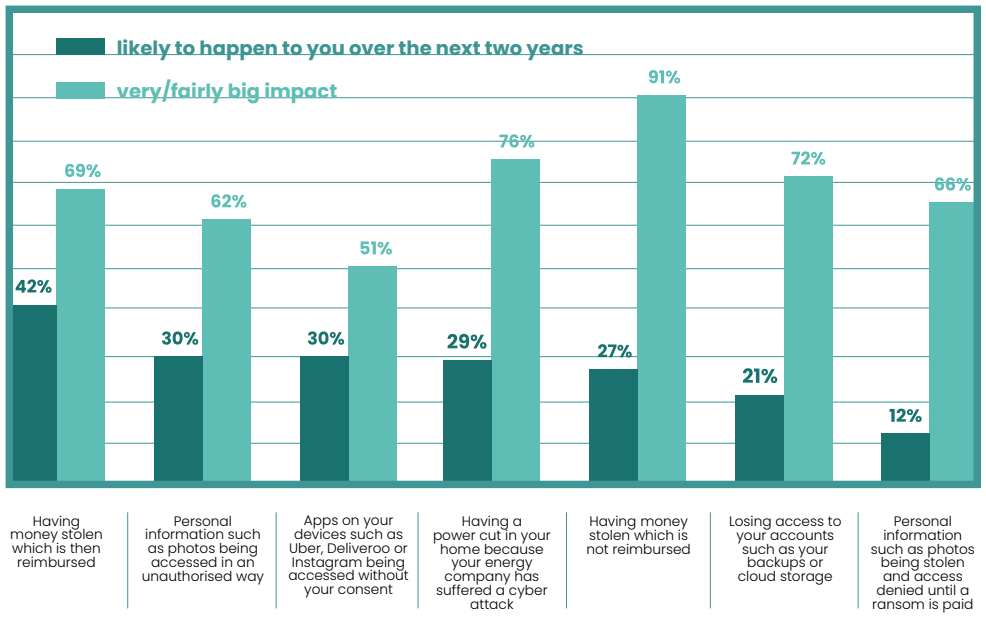
The UK Cyber Survey found that people are concerned, confused and, to some extent, fatalistic that they will become victims of cyber crime.

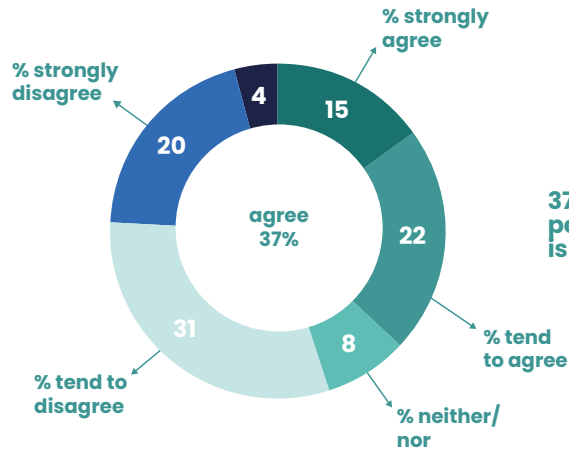
The insights are informing the government's approach, and the guidance offered by the NCSC, to help organisations and the public protect themselves against cyber threats.



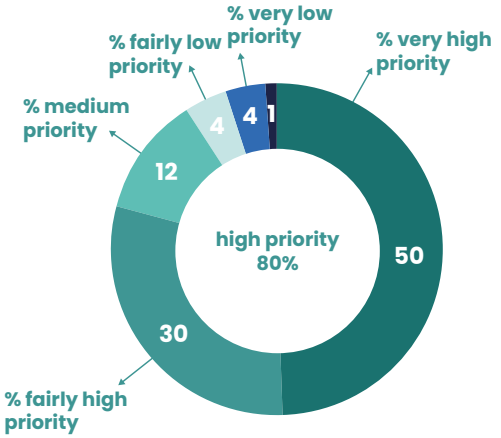
Two in three say they know a great deal/fair amount about how to protect themselves online.

70% believe they will likely be a victim of at least one specific type of cyber crime over the next two years, and most feel there would be a big personal impact.

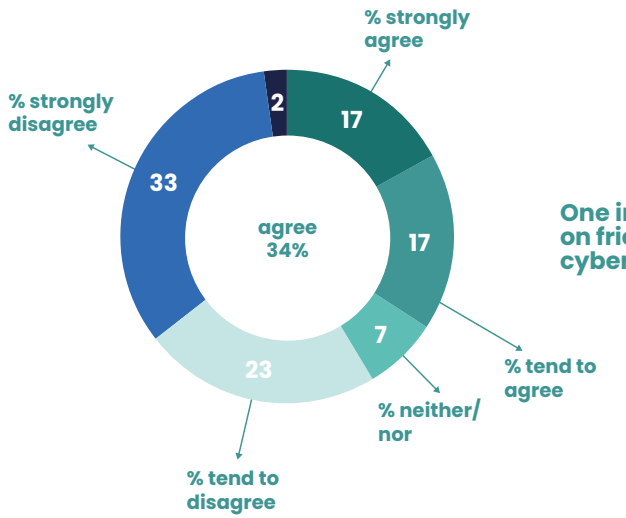




37% agree that losing money or personal details over the internet is unavoidable these days.



80% say cyber security is a high priority to them, half citing it a 'very' high priority.



One in three rely to some extent on friends and family for help on cyber security.

Note
The UK Cyber Survey 2019 was commissioned by the National Cyber Security Centre and Department for Digital, Culture, Media and Sport as part of the UK government's National Cyber Security Programme.

Ipsos MORI surveyed 2,700+ respondents: general public aged 16+, businesses, charities and public sector representatives from November 2018 to January 2019 via telephone.

Quietly fixing the technology

A significant priority for the NCSC is keeping individuals and families safe from cyber threats. It does this by bringing its technical and operational expertise to bear, to identify and fix cyber security problems.

By working behind the scenes, the NCSC can ensure that cyber security issues have as little impact on UK citizens as possible, in many cases resolving problems before they arise. After all, prevention is better than cure.

Haulster: Automated defence of credit cards

The NCSC's pioneering Haulster operation has disrupted financial cyber crime by flagging fraudulent intention against more than one million stolen credit cards. It is in the process of scaling this operation, and hope to reduce considerably more attacks in the near future.

Increasingly, criminal groups are using criminal marketplaces in cyberspace to buy and sell personal information and credit card details. Haulster takes stolen credit cards collected by the NCSC and partners, then, working with UK Finance, repatriates them to banks, often before they are ever used for crime. Card providers are then able to block cards to protect both financial institutions and the public.

In most cases, this has been done before a crime has taken place, meaning hundreds of thousands of victims of high-end cyber crime were protected before they lost a penny.

Online shopping

Criminals had been exploiting Magento, an open source ecommerce shopping platform commonly deployed on many websites. They had written malicious JavaScript code which copied all credit card transactions and silently sent the results to domains controlled by them. The NCSC conducted a successful trial to identify and mitigate vulnerable Magento carts via take down to protect the public. The work now continues. To date, the NCSC has taken down 1,102 attacks running skimming code (with 19% taken down within 24 hours of discovery). Without the NCSC's Active Cyber Defence intervention, it is likely these attacks would have continued indefinitely.

Securing the UK's mobile networks

Mobile networks worldwide establish signalling connections between one another to support a range of services, such as international calls and roaming. As these connections could also be used to negatively impact services in the UK, the NCSC has worked with mobile operators to perform live security testing of the UK's signalling interfaces. The NCSC has now tested 19 networks of different types across the six major mobile operators and has fed back the results of the testing to those operators.

This has helped the operators, with the support of the NCSC, to better understand the risk, share best practice and make improvements. Ultimately, this will help to ensure the UK's mobile services become more secure and robust.

Protecting our internet routing

The Border Gateway Protocol (BGP) is used to route the internet between Internet Service Providers (ISPs) around the world. When BGP is misused, either accidentally or maliciously, it can disrupt the internet until the issue is resolved. For example, sending data via an attacker's network.

The quicker misuse is discovered, the lower the impact, which is why the NCSC has worked with a major UK carrier to speed up the UK's response to BGP misuse. The NCSC has built BGP Spotlight, a detection and analysis system for BGP, that will alert the UK's carriers when BGP misuse occurs to allow them to respond quickly, analyse the cause, and minimise disruption to the UK's internet.

BGP Spotlight processes 25 million messages per hour from over 200 sources, converting these into 800,000 daily events across 240,000 unique destinations, a number which is set to expand as UK ISPs are in the process of adding data to, and receiving alerts from, the BGP Spotlight system.

The NCSC has published analysis of the 100,000 most commonly re-occurring passwords accessed by third parties in global cyber breaches, having been sold or shared by hackers.

The NCSC aims to reduce risk of further breaches by building awareness of how attackers use easy-to-guess passwords.

Most_Hacked_Passwords

Most used in total

123456	23.2m
123456789	7.7m
qwerty	3.8m
password	3.6m
1111111	3.1m

Names

Ashley	432,276
Michael	425,291
Daniel	368,227
Jessica	324,125
Charlie	308,939

Premier League football teams

liverpool	280,723
chelsea	216,677
arsenal	179,095
manutd	59,440
everton	46,619

Musicians

blink182	285,706
50cent	191,153
eminem	167,983
metallica	140,841
slipknot	140,833

Fictional characters

superman	333,139
naruto	242,749
tigger	237,290
pokemon	226,947
batman	203,116

List created in April 2019 after breached usernames and passwords were published on 'Have I Been Pwned' website.

2 Targeting the biggest risks:

what *we* do to protect people

The UK continues to be one of the most digitally advanced countries in the world, with our lives being online more than ever before. As this digitisation continues, it is vital that the UK remains able to protect its organisations, business and citizens against cyber crime.

The NCSC's breadth of work, programmes and projects, together with its close partnerships with industry and government, mean that it is able to help protect the institutions, infrastructure and services that people so heavily rely on day to day.

Active Cyber Defence

A cooperative approach: the UK's Active Cyber Defence programme

The ultimate goal for Active Cyber Defence (ACD) is for there to be fewer cyber attacks in the world, causing less harm. It represents a significant step-change in the country's approach to cyber security, because of its voluntary, non-regulatory, non-statutory approach delivered in partnership with central government, local government and business.

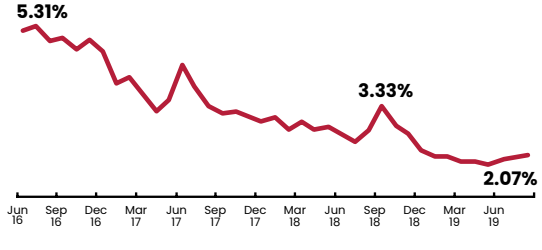
As difficult as this sounds, the NCSC can provide evidence that it works. In sharing this knowledge, it hopes to inspire other countries to adopt bold measures, in partnership with industry, to protect their digital homelands.

Active Cyber Defence includes some of the following pioneering programmes:

1. **Web Check** helps make websites a less attractive target, by finding obvious security issues and pointing them out to the website's owner so that they can be fixed.
2. **Protective DNS (PDNS)** blocks public sector organisations from accessing known malicious domains or allowing malware on already compromised networks from calling home.
3. **Takedown Service** finds malicious sites and sends notifications to the host or owner to get them removed from the internet.
4. **Mail Check** helps public sector organisations take control of their emails, making phishing attacks which spoof those organisations more difficult.

UK share of visible global phishing attacks reduced to 2.1% (August 2019).

UK share of global phishing – change over time from June 2016 to Aug 2019



In 2016, HMRC was the 16th most phished brand globally. In Sept 2019, as a result of ACD services and HMRC countermeasures, their ranking had dropped to 126th in the world.

Takedown Service

98% of phishing URLs

discovered to be malicious were successfully taken down.

This totalled

177,335 phishing URLs

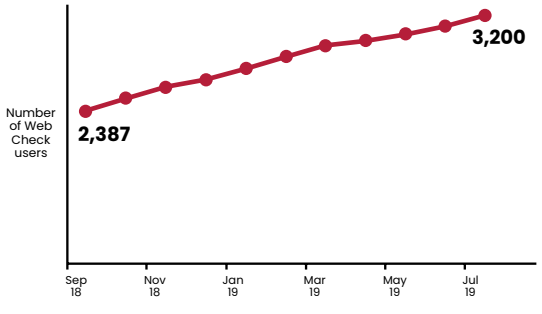
(23,311 attacks by group).

62.4%

of these were removed within 24 hours of being determined malicious.

Web Check

Change over time of the number of users signed up to Web Check, by month.



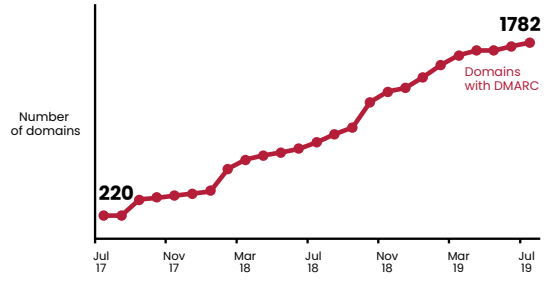
The number of urgent findings resolved by users after being detected by Web Check doubled to a level of approximately

500 per month

Mail Check

More government domains are now using DMARC, the email authentication, policy and reporting protocol, making phishing attacks which spoof these domains more difficult.

Change over time of the number of gov.uk domains using Mail Check/DMARC, by month.



Protective DNS

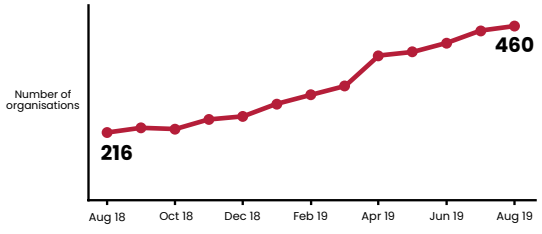
More than double

the number of government organisations are now protected by the PDNS, preventing them from accessing websites hosting known malicious content.

460+ organisations

are using the service and it blocks around 20,000 unique domains at a rate of 6.5 million times per month.

Change over time of the number of active organisations using PDNS, by month for the period of this report.



Case studies

Protecting schools

Active Cyber Defence tools highlighted a local authority (LA) primary school network behaving as though infected with Ramnit – a worm which affects Windows systems. The LA was notified, and an investigation found that the antivirus that was installed on the school's systems was not working. As a result, the school had a wide level of infection. Not only did the Active Cyber Defence tool block the malicious connections, containing any harm, it also identified the malware and notified the LA. The LA was able to install a working antivirus and the infection was cleaned up within a day.

Protecting the legal sector

For the first time, the NCSC used ACD tools to tackle advanced fee fraud impersonating the UK legal sector. Both bogus law firms, and impersonation of legitimate law firms, are techniques used by fraudsters in an attempt to increase the credibility of their attacks. Increasingly, scammers use real law firms and other entities to try to make their attacks look more legitimate.

Protecting airports

The NCSC has been tackling the abuse of public sector email domains in the UK. One such incident occurred when criminals tried to send in excess of 200,000 emails purporting to be from a UK airport, using a non-existent gov.uk address in a bid to defraud people. However, the emails never reached the intended recipients' inboxes because the Active Cyber Defence system automatically detected the suspicious domain name and the recipients' mail providers never delivered the spoof messages. The email account used by the criminals to communicate with victims was also taken down.

Protecting emergency services

Two fire services merged to form a new super service with a new name and associated internet domain. One of the organisations subsequently deregistered their original domain. However in just three months, Synthetic DMARC blocked more than 150,000 emails from this now non-existent domain. There is no way of knowing whether these were as a result of fraudulent purposes or misconfiguration, but shows the necessity to correctly curate domains throughout their lifecycle.

"The NCSC is not the only organisation with good ideas, and the UK is not the only country connected to the internet. We welcome partnerships with people and organisations who wish to contribute to the Active Cyber Defence service ecosystem, analysis of the data, contributing data or infrastructure to help it make better inferences. We believe that evidence-based cyber security policy – driven by evidence and data rather than hyperbole and fear – is the way forward."

Dr. Ian Levy, Technical Director, NCSC

What's next for Active Cyber Defence?

Active Cyber Defence has protected thousands of UK citizens and further reduced the threat of UK brands being exploited by criminals.

While these successes are encouraging, the NCSC knows there is more to do and it has a number of projects in the pipeline, including:

- An automated system which acts on information from the public to take down malicious sites.
- The NCSC 'Internet Weather Centre', which will aim to draw on multiple data sources to enable full understanding of the UK's digital landscape.
- The Infrastructure Check service: a web-based tool to help public sector and critical national infrastructure providers scan their internet connected infrastructure for vulnerabilities.
- Breach Check: a web-based tool to help government and private sector organisations check whether employee email addresses have been compromised in a data breach.
- The NCSC is also exploring additional ways to use the data created as part of the normal operation of the public sector protective DNS service to help users better understand and protect the technologies in use on their networks.

Protective DNS is actively engaging with organisations from central government, local authorities, emergency services, devolved administrations, the NHS and Ministry of Defence (MoD). For those sectors that are not eligible to use PDNS, the NCSC is working with industry to broaden the benefits of the service. The NCSC intends to share indicators of compromise with DNS providers to use on their own services. This will mean organisations and individuals who are not eligible for the PDNS still benefit from the NCSC's knowledge and expertise. Through the NCSC and industry working together, a greater number of users can benefit from DNS filtering.

Raising cyber resilience across government and the public sector

The NCSC works closely with public sector bodies to protect the networks, data and services which the UK depends upon.

Working with central government

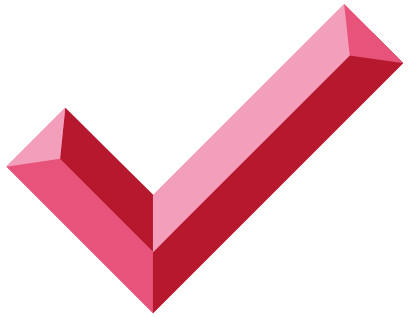
The NCSC provides assurance on key systems across central government departments and agencies, assisting them to develop their security strategies and secure their networks.

Building on the success of the Transforming Government Security Programme, the NCSC is working with the Cabinet Office's Government Security Group, providing advice and guidance to shape policy development on cyber security.

Mail Check monitors

6,273

domains classed as public sector.



The number of public sector domains protected by DMARC [an Active Cyber Defence tool] more than tripled

from 412

at the end of December 2017

to 1,940

in September 2019.

Working with local government

The NCSC assists local government both through direct engagement at a local level, supporting its networks of technical staff, and working with representatives from member organisations including the Local Government Association (LGA) and the Society of Local Authority Chief Executives (SOLACE).

Commissioned by the Ministry of Housing, Communities and Local Government (MHCLG), and funded by the National Cyber Security Programme, the NCSC is supporting the design and delivery of the MHCLG 'Think Cyber, Think Resilience', Cyber Pathfinder training scheme. This provides a series of workshops for senior leaders, policy makers and practitioners across the English regions, to build understanding of cyber threat and foster good practice to manage risk. As a result, 85% of delegates have said they would make changes to their cyber security practice.

Digital Government Lofts

The successful sharing of the NCSC's expert advice and guidance across UK government and the public sector through Digital Lofts continues. This year's locations and hosts have included Warwickshire County Council, the Met Office in Exeter, as well as the Scottish government in Edinburgh.

Web Check for Local Authorities

Local Authorities		% Using Web Check
England	336	97%
Wales	22	100%
Scotland	32	100%
NI	11	90%
UK	401	97.75%

Cyber health check for the NHS

The NCSC is working with health authorities across the UK to reduce the risk of another major cyber attack affecting the NHS.

The WannaCry ransomware attack of 2017 caused disruption in a third of all hospital trusts across England, leading to cancelled operations and appointments for many patients. The incident brought to light a number of weaknesses in the cyber defences of the NHS.

For this reason, the NCSC has been working with NHS Digital, the national information and technology partner for the health service in England, on the procurement of a new perimeter security solution for the NHS. The NCSC lent its technical expertise, providing cyber experts to review the bids against security standards.

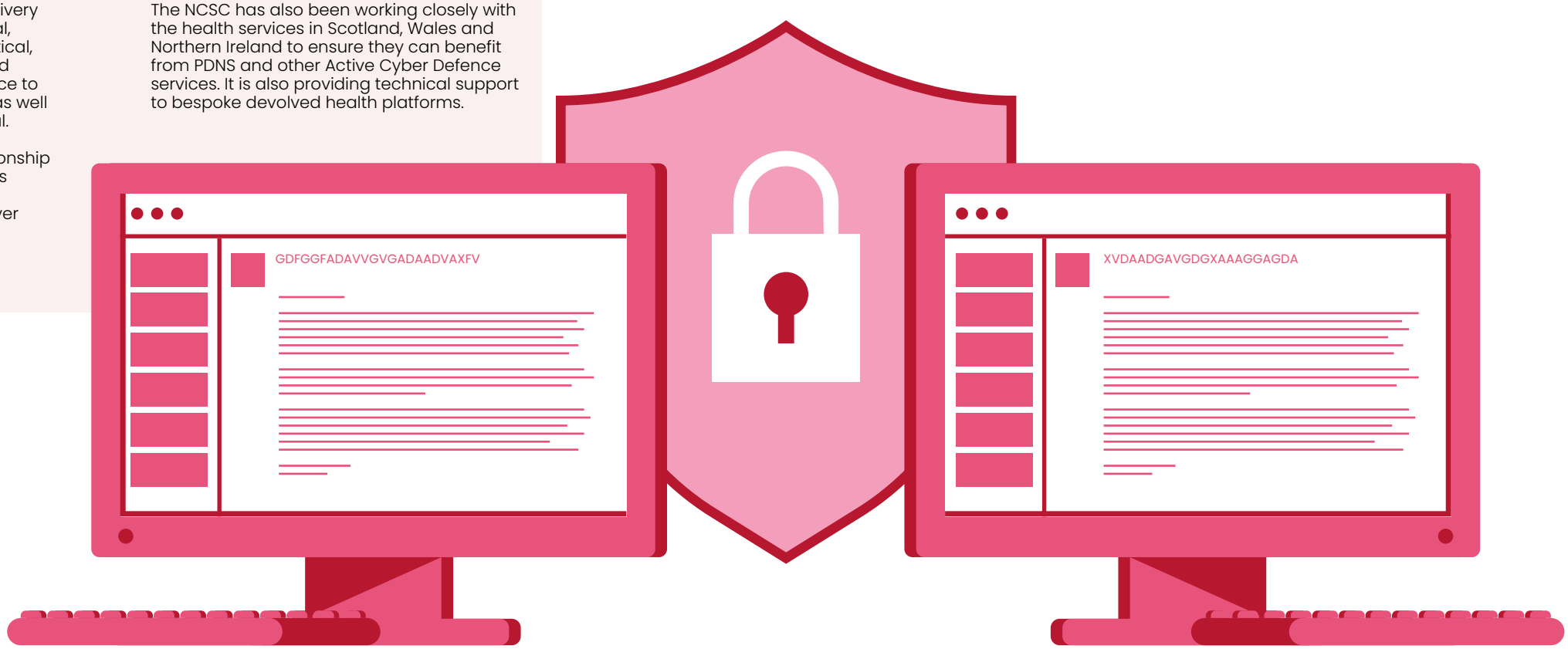
Dan Jeffery, Head of Innovation, Delivery & Business Operations at NHS Digital, stated: "The NCSC has provided critical, timely, and invaluable technical and strategic advice, input, and guidance to the Secure Boundary programme as well as the Cyber Programme in general.

"The enduring strength of the relationship between the NCSC and NHS Digital's Data Security Centre is one of the reasons we have been able to deliver such progress and improvement to the security posture and resilience of Health and Care in such a short period of time."

All hospital trusts in England will be offered the free Secure Boundary solution which includes next generation firewalls and the NCSC's Protective Domain Name System (PDNS) service. This will help NHS organisations to defend against future attacks, including ransomware, and enable them to keep providing care for patients.

Another benefit of the new system is that it will be possible to spot when a cyber attack is attempted on a particular hospital trust. NHS Digital will use this information to better understand the threats facing the health sector and also to give tailored advice to specific hospitals.

The NCSC has also been working closely with the health services in Scotland, Wales and Northern Ireland to ensure they can benefit from PDNS and other Active Cyber Defence services. It is also providing technical support to bespoke devolved health platforms.



Vulnerability Disclosure

If someone finds a vulnerability in a UK government website and cannot contact the system owner, they can report the vulnerability to the NCSC's Vulnerability Reporting Service. This is part of its wider efforts to improve vulnerability handling across the public sector. Following the service's launch, the NCSC has received reports covering a number of security issues including cross-site scripting and subdomain takeover.

In addition to the Reporting Service, the NCSC also launched the Vulnerability Disclosure Pilot, working with a number of UK government departments to kick start best practice in vulnerability disclosure across the public sector.

Detect and forewarn to protect government departments

The NCSC's Host-Based Capability tool collects and analyses technical metadata to help government departments understand the threats they face. Following a successful pilot year, the service has been deployed to 35,000 government devices across nine departments. The capability is complementary to departments' own security measures. The data the NCSC collects is used to detect malicious activity, provide monthly threat reporting and assess exposure to serious cyber threats.

Defending democracy

The foundations of liberal democracy are under increasing threat from cyber attacks and the NCSC plays a key role in defending the UK's political process.

The NCSC meets with UK political parties (which take up at least two seats in the House of Commons) every three months and regularly gives cyber security advice to parliamentarians. During the local elections (March 2019) and European elections (May 2019), the NCSC provided guidance, informed by comprehensive cyber threat assessment, on risks and advice on protecting systems and people to political parties.

The NCSC monitors known adversaries who look to target parties or even politicians. If threats are detected, the NCSC shares the details of the threat and tailored advice, allowing the individual or organisation to put mitigations in place.

"The NCSC is very proactive and efficient in quickly speaking to all the relevant staff here to alert us to an issue. Beyond just dealing with incidents at hand, we have also received a number of very clear and helpful recommendations to further harden our systems which we have subsequently undertaken. It was great to have the support at the time, but also to have our contact follow up with us some weeks later to check whether any further support was needed or desired."

Sian Waddington, Director of Operations,
Liberal Democrats

"The role of Chief Information Officer, for one of the UK's major political parties, has its stressful moments. Having the NCSC on hand helps you sleep at night. The online briefing material is excellent and is frequently quoted. When an incident happens, their support and advice quickly gets the incident under control and helps calm senior management."

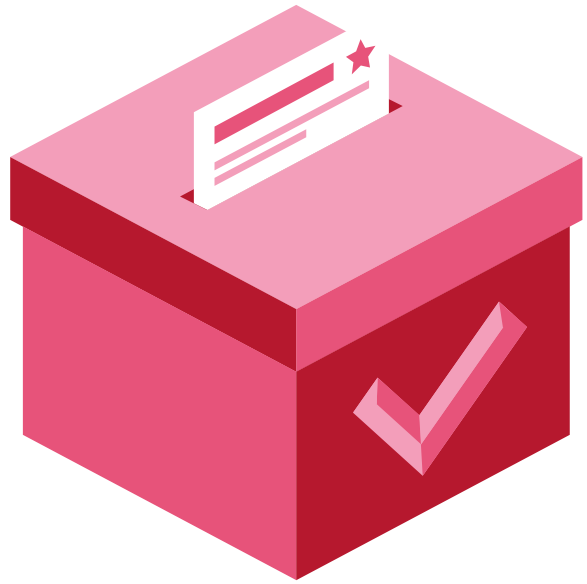
Paul D Bolton, Chief Information Officer,
Conservative Campaign Headquarters

"We depend on the work of hundreds of thousands of volunteers, and so collect and hold a great deal of data – and we work hard to keep it safe. Knowing the NCSC is also there to look after the integrity of our information, especially at election time, is a tremendous reassurance. The NCSC's advice has been invaluable in making our systems more secure."

Tim Waters, Director of Data & Targeting,
The Labour Party

"Digital technology continues to change the way that elections are run and fought; it also changes the way that voters are informed and influenced. Since its creation, the NCSC has provided valued support to the Commission and wider electoral sector, to mitigate the risks posed by these innovations. We welcome their important role in supporting the ongoing integrity of elections in the UK."

Bob Posner, Chief Executive.,
The Electoral Commission



Serving every part of the UK

The NCSC continues to work across the whole of the UK. This includes support to devolved administrations in Wales, Scotland and Northern Ireland, raising cyber resilience across all sectors.

The NCSC worked with Welsh government to ensure its advice for citizens and families was included in its Digital Inclusion Programme, to help all citizens to get online safely. In support of the TARIAN and North West Regional Organised Crime Units, the NCSC provided materials and speakers for the Welsh Cyber Bus Tour, supporting local business, community groups and the public to enhance their cyber resilience. The NCSC also provided technical security advice to the Welsh Revenue Authority, which collects and manages devolved taxes in Wales.

In Northern Ireland, the NCSC advised on IT controls, protecting the country's ~1.75m citizen electoral records. It continues to build partnerships across the economy and society in Northern Ireland, including delivering briefings to charity leaders in partnership with the Northern Ireland Council for Voluntary Action, helping to ensure cyber is considered alongside business risks. The NCSC also partnered with Northern Ireland Department for Education to improve cyber resilience in schools across the country.

In Scotland, the NCSC has provided significant bespoke technical advice on several new online services. This includes the new Scottish online platform for payment of devolved benefits to citizens, plus their platform for supplier payments. This year, the NCSC hosted the CyberFirst Girls Competition final in Edinburgh and CYBERUK 2019 in Glasgow, with Scottish government taking the opportunity to showcase in parallel the work of the Scottish Cyber community with a number of side events, including "Scotland Cyber Week".

The NCSC worked in partnership with Scottish government to deliver bespoke workshops for small businesses, charities, CEOs, and launched the Exercise in a Box tool. It continued its support of the cyber catalyst network, ensuring effective peer to peer sharing of best practice and NCSC guidance.

The Scottish Qualifications Authority and Scottish Credit Qualification Framework have also approved the NCSC's CyberFirst awards for Defenders, Futures and Advanced courses, meaning that anyone completing these courses will now receive recognised learning credits.

Take up of the NCSC's Active Cyber Defence continues across all three devolved administrations, helping to protect local government and other public online services. In Scotland, the majority of public sector organisations are using one or more of the tools, and increased take-up in Wales and Northern Ireland continues at pace.

"Our engagement with the NCSC has helped us to establish our executive agency, Social Security Scotland, followed by the launch of our public facing cloud based digital platform, which underpins the delivery of the first live devolved benefit payments Scotland. The NCSC has provided us with expert advice and guidance through technical workshops and engaging its partners to share experiences. This has given us valuable assurance in support of our strategic security objectives and our own 'Secure by Design' principle."

John Campbell, Head of Digital Risk & Security Social Security Directorate, Scottish Government

"We have made significant investments in improving our cyber defences and cyber hygiene. The NCSC has proven to be an expert advisor in defining and refining our requirements, most especially in our plans to implement a Security Information and Events Management Service and associated Security Operating Centre. Their experience of forensics, analytics, alerts and appropriate approaches to monitoring has been invaluable."

Chief Strategy Officer, Northern Ireland Civil Service

"The NCSC continues to provide valuable advice and guidance for us to share with Welsh stakeholders which greatly contributes to increasing cyber security capability within Wales. We value the engagement and ongoing support in several areas, including increasing take-up of Active Cyber Defence tools in the Welsh public sector and encouraging participation of Welsh students on CyberFirst courses."

Representative, Welsh government

Critical National Infrastructure

Everyone in the country relies on the UK's Critical National Infrastructure (CNI) day in, day out. We all need the country's communications networks to keep in touch with friends and family, transport networks to travel to work and school, and energy networks to power and heat our homes. Interruption to any of these critical services could cause serious disruption to our lives and potentially damage the economy.

Strengthening the cyber resilience of the UK's most critical systems therefore remains a top priority.

The NCSC's work spans CNI in the public sector, as well as a focus on nine critical private sectors: communications, transport, energy, civil nuclear, finance, water, chemicals, space and food. It provides direct support to hundreds of public and private sector organisations that own, manage and maintain CNI assets in the UK. This includes one-to-one technical advice, sharing threat information, facilitating cyber exercises and running information on exchanges for organisations to share knowledge and expertise.

Thwarting ATM attacks

On multiple occasions, the NCSC has alerted UK financial institutions to imminent threats from ATM cash-out fraud at home and abroad. This is where cyber criminals compromise banking and payment infrastructure, and obtain card details that can be used to withdraw large sums of cash from ATMs. Once already in progress, these attacks can be difficult to stop.

The NCSC works with industry and government partners around the world to share information and disseminate alerts about threats and anticipated malicious activity.

As a result, banks swiftly put defensive measures in place that protect them against financial loss and reputational damage. Most recently, the NCSC alerted 56 banks to a specific ATM cash-out threat after receiving actionable information. As a result, the banks were able to block any attempt by the attackers to fraudulently withdraw money from customer accounts.

Defending online banking

There has recently been a rise in the sophistication of SMS-interception attacks, with multiple financial institutions and Communications Service Providers (CSPs) being affected.

The attackers intercepted SMS messages sent as part of the two-factor authentication (2FA) needed for online banking. Whilst 2FA is generally recommended by the NCSC, in this case messages from multiple banks via multiple mobile networks were targeted, allowing the criminals to make fraudulent payments to their accounts at the expense of the wider public. The NCSC was in a unique position to bring experts in the telecoms and finance industries together to share information regarding the attacks, determine how they were being carried out, and develop mitigations. This information sharing continues through the NCSC's Cyber Security Information Sharing Partnership (CiSP) platform.

"At the heart of the NCSC's mission is protecting critical pieces of our infrastructure; keeping the service they provide secure keeps the country running. It's only through these partnerships with industry that we can understand the risk we face, protect current systems and secure the infrastructure of tomorrow."

Clare Gardiner, Director National Resilience & Strategy, NCSC

Keeping the lights on

A successful cyber attack against the energy sector could disrupt the fuel and power supplies our country so heavily relies on. That's why the NCSC's work with energy firms has been diverse and extensive.

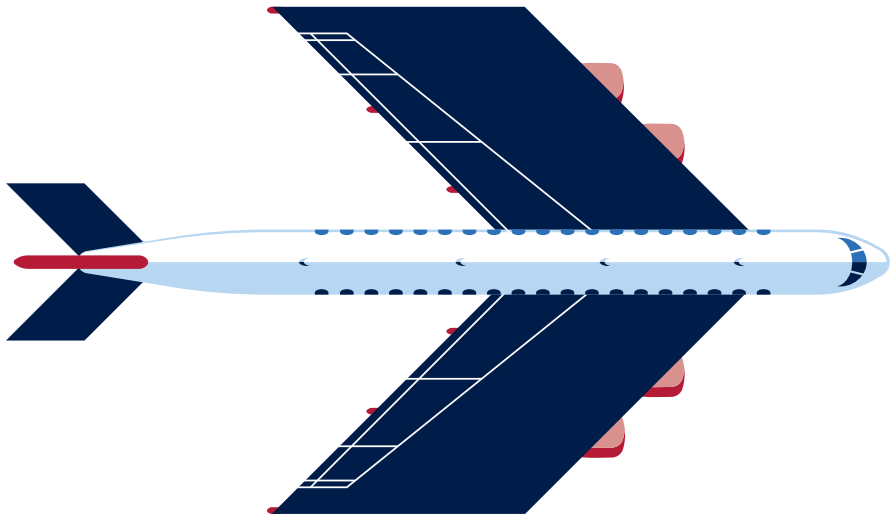
This year the NCSC worked with one of the UK's largest oil refineries to review and advise on an upgrade to its systems, greatly increasing its resilience. The NCSC's Cyber Adversary Simulation team also conducted an exercise against a critical supplier of road fuels, which identified vulnerabilities that the company has since protected itself against.

In partnership with the Department for Business, Energy and Industrial Strategy (BEIS), the NCSC held a complex technical exercise with electricity distribution network operators. It was the culmination of a two-year project and involved more than 170 participants at 13 different UK locations to test the sector's response to a national-level incident.

Digital integration is only adding to the security challenge. The NCSC's recent review of smart metering infrastructure for BEIS, and the recommendations it produced, is one illustration of how the NCSC works with government departments to ensure the highest cyber security standards across the sector.

"We would like to thank the NCSC for the invitation and our subsequent involvement in the sector-wide cyber security test. The challenge and results from the scenario exercising has been invaluable in applying improvements to our emergency planning and resilience processes, along with recognising the importance of cross industry support and alignment during such events."

John, Scottish and Southern Electricity Networks



Threats to air passenger data

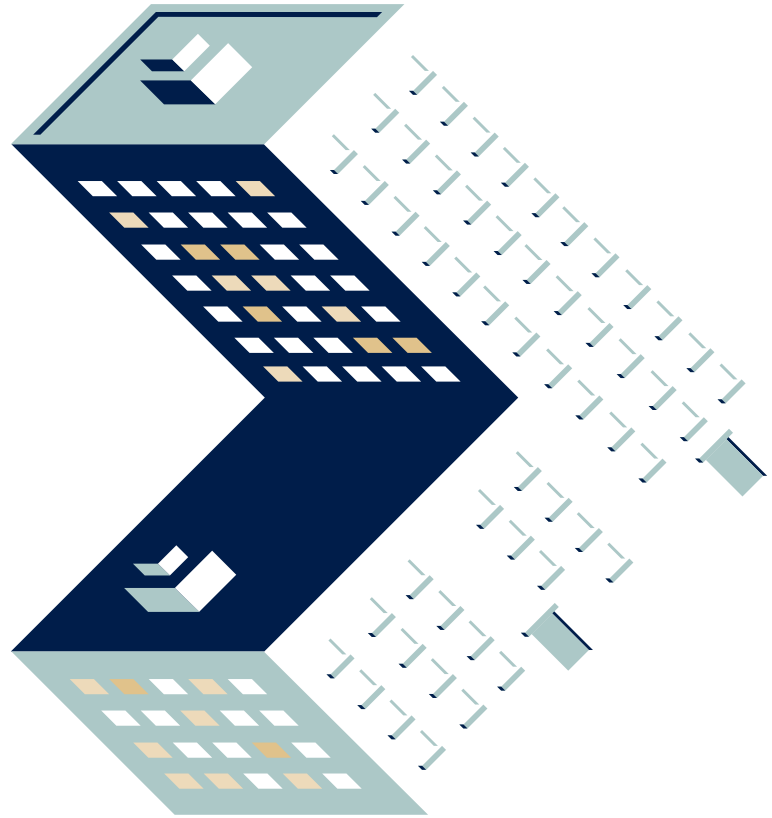
The aviation sector has continued to be an attractive target for cyber attackers. Airlines store vast amounts of personal identifiable information (PII), which criminals can sell or use for spear phishing and identity theft. State actors may also be interested in airline PII for counter-intelligence purposes or tracking dissidents.

The NCSC's work with the sector has included assisting UK airlines targeted by a group known as Chafer. This group, which security companies have linked to Iran, has a history of targeting global organisations for bulk personal data sets. The NCSC helped the airlines identify potential risks to their networks and offered mitigation advice, minimising the impact.

It has also continued working with NATS, the main air navigation service provider in the UK, to review the cyber security of their air traffic control and management system.

"The challenge and results from the scenario exercising have been invaluable in applying improvements to our emergency planning and resilience processes, along with recognising the importance of cross industry support and alignment during such events."

NATS, the UK's leading provider of air traffic control service



Securing the future: Smart cities

Across all sectors the drive to reduce costs, increase efficiency and provide new data-driven services is leading to increased digitisation and automation. Cities are no exception, with councils looking to technology to help with a suite of challenges including reducing congestion, improving public safety, and enhancing local health care services.

There are two main themes to the security challenges in smart cities. The first is ensuring that citizen privacy is maintained, and that personal details required to operate the services are secured. The second is understanding the interdependencies between a smart city's services, and the impact of failure. For example, computerised road signs may depend on power and a data connection in order to work effectively. While it would take a lot of paint and physical presence to manually deface all the traditional road signs in an area, it could be possible to change all the signs in a city without ever setting foot in it, if smart signage projects are badly implemented.

The NCSC is applying its experience in helping national and local government ensure that personal data is protected, and its understanding of the security challenges in critical national infrastructure, to the new and emerging challenges presented by smart cities.

In one real-world example, a council is using traffic flow data to adjust road signs in the city to divert traffic, saving citizens an average of 60 hours per year on their journey times.

"I think the creation of the NCSC, together with the value that has been seen for well over a year now, is proof that it was needed, together with it being stocked with the best of the best. Whilst it will always be a when not an if, in terms of the next attack/breach/ransom, I know we can all rest a little bit easier than previously, safe in the knowledge that we are all working together."

Bill Schindler, Head of Infrastructure Service & Strategy, Severn Trent Water

Telecoms Supply Chain Review

When the Department for Digital, Culture, Media and Sport (DCMS) launched the Telecoms Supply Chain Review, the NCSC was asked to examine the cyber security risks in the UK's telecoms supply chain, to ensure that the review was supported by expert technical analysis. The analysis highlighted a range of cyber risks to the sector, leading to the recommendation that policy changes were needed to drive security improvements in the telecoms sector.

Peter, the NCSC's Technical Director for Telecommunications, said: "In the first three months of the review, we talked to all the major operators to see how they manage their supply chain, what risks they faced and what their security arrangements were.

"We found that the cyber threat has changed significantly over the last 10 years and the market drivers are not there to ensure companies are responding, meaning we are faced with increasing national risks in the sector.

"While we had just six months to produce our analysis, we were fortunate to be building on a significant knowledge base. Within the NCSC there is a wealth of experience in threat assessment, incidents, direct consultancy with industry and security research, both applied directly to the telecoms sector and more broadly. Through this experience and armed with the information provided by industry, we could identify where our operators were most vulnerable and then consider how other sectors have successfully reduced similar risks. This put us in a unique position to support the review."

The review's major conclusion that the government will pursue a robust new security framework for telecoms, will be supported by the NCSC's current risk-mitigation model, which will be adapted as necessary as telecoms networks evolve towards 5G and full-fibre coverage.

This new framework will be placed on a statutory footing once government legislates to strengthen the enforcement powers of the telecoms regulator, Ofcom, and to provide new national security powers for government to respond to supply chain risks in the future.

The NCSC continues to forge close relationships with the UK's major telecoms providers right up to board level. This includes regularly hosting CEOs and CISOs at the NCSC's headquarters for discussions on how government and industry could work together to improve cyber resilience in the sector.

Regulation

Considerable progress has been made in making use of the new regulatory provisions introduced by the Network and Information Systems (NIS) Regulations 2018. These are starting to drive real improvements in CNI cyber security. Several new sector-focussed regulators, known as Competent Authorities (CAs), now have the sole authority for all regulatory and enforcement decisions involving organisations designated as operators of essential services (OES). The NCSC is providing extensive support to the CAs, including the development of cyber security guidance and standards, as well as cyber security training.

The NCSC's Cyber Assessment Framework (CAF) has been adopted by most of the CAs, with a significant number of OES across multiple sectors completing self-assessments of their cyber security against these NCSC principles. This represents a ground-breaking step forward in building a cross-sector picture of CNI cyber security, providing a valuable evidence-base for future decision-making.

GDPR update

In May 2018, the General Data Protection Regulation (GDPR) came into force alongside the Data Protection Act 2018, placing a comprehensive set of new obligations on public and private sector organisations to protect all the personal data that they collect and process.

The NCSC has continued to build on its partnership with the Information Commissioner's Office (ICO). Through this partnership, respective roles and responsibilities have been clarified in order to better help victims of GDPR understand which authority or organisation to deal with and when, as well as having access to better advice.

A framework of collaboration was announced by Ciaran Martin and ICO Deputy Commissioner James Dipple-Johnstone at CYBERUK 2019. Notably, it was also clarified that the NCSC will never pass sensitive information disclosed to it by a victim to a regulator without first seeking the consent of the organisation concerned.

"The NCSC has an important role to play in keeping UK organisations safe online, while our role reflects the impact cyber incidents have on the people whose personal data is lost, stolen or compromised."

James Dipple-Johnstone, ICO Deputy Commissioner – Operations

National security

The NCSC collaborates closely with government and industry partners to develop secure systems for national security at home, and with the UK's allies across the world. By doing this, the NCSC can help to ensure that critical operations continue globally.

The NCSC aims to develop, operate and maintain world-class technical security capabilities to counter the threat from the country's most capable adversaries, raising the cyber resilience across government and industry partners.

It's through these partnerships, as well as its investment in developing the country's cyber skills, that the NCSC can continue to help protect the UK from cyber threats.

Securing Britain's secrets

Government missions

The NCSC works with the defence sector and UK intelligence agencies to help preserve the country's national security. The NCSC's encryption expertise enables it to protect the UK's national defences in a range of ways.

The NCSC enables business focused solutions, supporting customers through the development of their skills and threat understanding, facilitating the availability of technology so that security enables rather than hinders, mission delivery.

Foxhound/ROSA

The NCSC has supported ROSA – a central government IT system – as it transitions to become a fully supported service across government. ROSA provides fixed and mobile SECRET collaborative tools and communications in 152 countries across the globe, allowing users to create and share data securely.

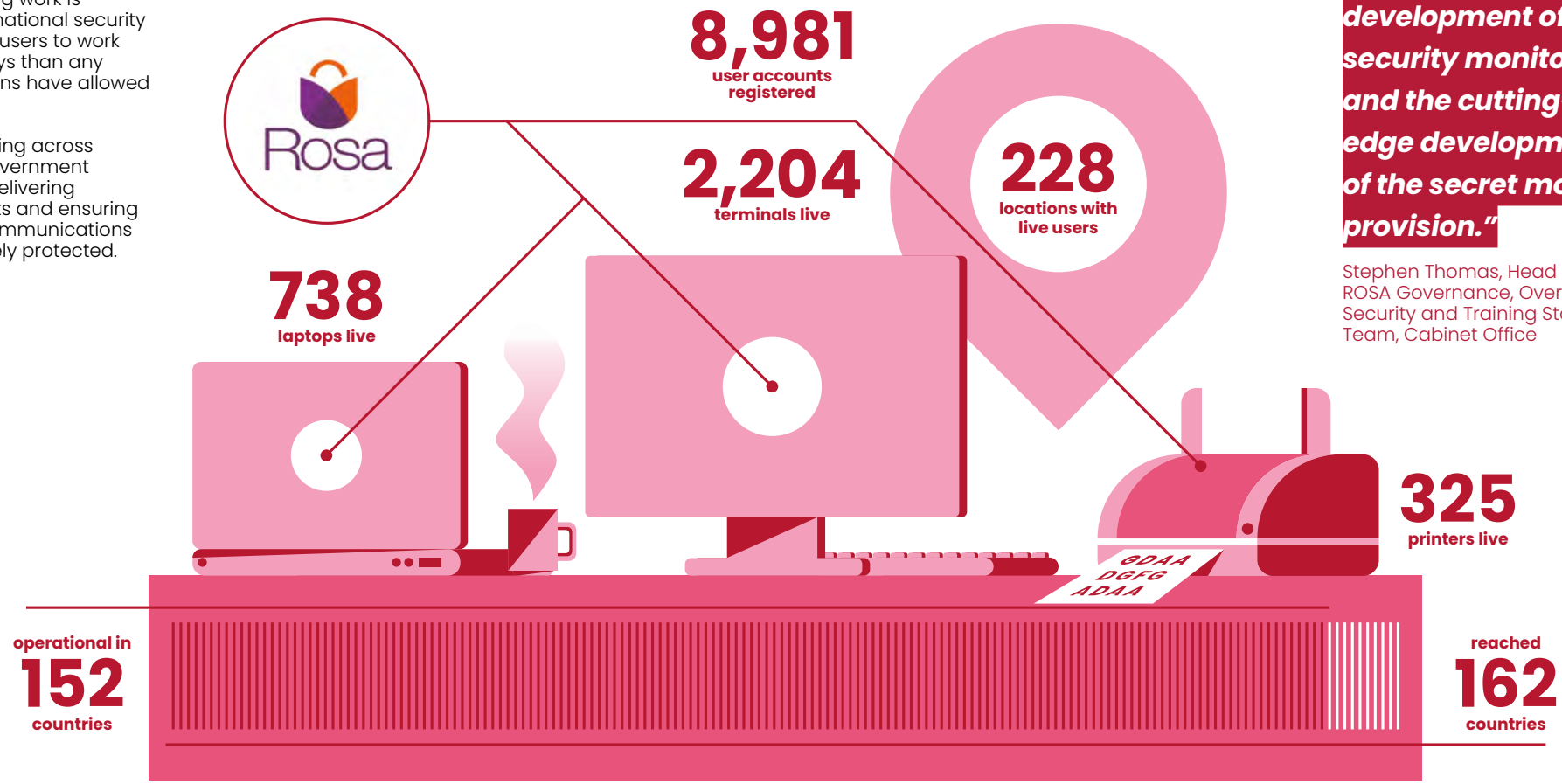
The NCSC itself uses ROSA to collaborate more effectively and securely with government customers and industry partners.

This year, NCSC experts designed new systems that enable easy mobile working at SECRET in a safe way. This ground-breaking work is protecting our national security whilst enabling users to work in far better ways than any previous solutions have allowed in this space.

ROSA is expanding across a number of government departments, delivering tangible benefits and ensuring government communications are appropriately protected.

"The ability to challenge, request or discuss any concerns from either a MoD or NCSC perspective – quickly and transparently – has been refreshing."

Matthew Trigg, Deputy Head of Accreditation Team, Ministry of Defence



Cyber Surgeries

The NCSC has expanded the use of its Cyber Surgeries. These high impact events have allowed the NCSC to present and discuss thinking around a number of technology challenges.

The surgeries are attended by a wide range of Ministry of Defence (MoD), and other government stakeholders, and are an effective way of ensuring that a wide range of stakeholders have the chance to listen to the NCSC's technical experts, who can share their thinking.

The surgeries also give the opportunity for discussion, challenge and feedback, ensuring that the NCSC's thought leadership is better able to meet the requirements of its stakeholders, in a world of ever-changing technological challenges.

"The continued provision of subject matter expertise by the NCSC has been key to both the enhancement of the functionality available within ROSA and also to its ongoing maturity. Of particular note is the input on the development of security monitoring and the cutting-edge development of the secret mobile provision."

Stephen Thomas, Head of the ROSA Governance, Oversight, Security and Training Standards Team, Cabinet Office

Defence, Security and Resilience

The NCSC continues to support the MoD to make the defence sector a more difficult target for those that threaten our national security.

Strategic Deterrent

The NCSC supports the Continuous at Sea Deterrent (CASD) through incident and threat reporting, providing advice on cyber security risk and policy, and identifying supply chain vulnerabilities. The NCSC has been asked to support the new Successor programme, which will deliver the replacement to the current Vanguard-class Trident submarine over the next 30 years.

Joint Strike Fighter

The NCSC has supported the F-35B as it enters service and deploys on operational flights over the skies of Syria and Iraq. Its support is part of the ongoing fight against Daesh, which sees the NCSC providing key material and working with UK industry, to sustain the UK's Freedom of Action to deploy the F-35B whenever and wherever needed.

Joint Crypt Key

The Joint Crypt Key Programme (JCKP) is a major programme of work within the wider Crypt Key Enterprise.

Working in collaboration with the MoD, JCKP is investing in products and services that use high end cryptography to help the UK keep its secrets secret, share information effectively and ensure information is available when and where required.

JCKP is ensuring that the NCSC IS able to sustain today's mission and develop the solutions required for the future.

JCKP has helped the UK maintain its standing as a world leader in cryptographic key services, enabling the country to keep pace with the scale of operational demand and increasing threat from adversaries.

UK Key Production Authority

The UK Key Production Authority (UKKPA) is a critical part of the NCSC's cryptographic defences. UKKPA generates, distributes and accounts for cryptographic key material for government, industry and allies overseas to support secure encrypted communications. In line with the UK's key management strategy, the UKKPA has further reduced the volume and range of physical keys that need to be distributed to the NCSC's customers, with an increased drive and investment towards electronic key distribution strengthening the timeliness and robustness for key delivery.

- There are 170 UKKPA customers across government, industry and law enforcement.
- Alongside the US, the UK is one of only two suppliers of key material to NATO.
- Annually the NCSC processes approximately 2,879 orders for key material, equating to 108,411 physical items, such as CDs and data tokens.
- Production figures for 'electronic' key over the last 12 months – 860,190.

Working with industry

The NCSC cannot do any of this alone. Its industry partners provide a vital service to keep the country's communications secure.

Sovereign Enabling Framework

The Sovereign Enabling Framework (SEF) has proven successful in absorbing the High Grade or High Assurance requirements of the two main users, Joint Crypt Key Programme (JCKP) and Initiate.

Initiate is a cross-government collaborative programme investing in the early stage development of technologies that will provide the foundation for future secure solutions in the UK. JCKP is the MoD-NCSC joint programme developing high end Crypt Key solutions for the future. Amongst other things, it draws in Initiate-funded technology.

Positive feedback is testament to the robust but flexible process allowing this important complex work to be completed at the pace required, having now let 125 tasks.

The eight sovereign suppliers are a mix of established large industry players and newer start-up companies. This provides a good balance of innovative thinking and challenge, with experience, legacy and resource, providing sustainability and support to the ambitious future direction for crypt key across government.

Wassenaar Arrangement

The NCSC's cyber exports team represented the UK government at the Wassenaar Experts Group, negotiating two important changes to the information security controls.

The first was updating the crypt definitions to include post-quantum cryptography. These new controls ensure that future strong cryptographic algorithms remain on the same standing as traditional cryptography within the licensing framework.

The second update is sizeable decontrol, meaning that many 'industrial-Internet of Things' devices employing cryptography no longer require export licenses. Alongside existing exemptions for consumer IoT, this change in regulation will have significant positive impact on UK exporters.

HMS Vengeance – the fourth and final Vanguard-class submarine of the Royal Navy

Telemetrics

Telemetrics is the process of collecting information about an object and sending the information somewhere electronically. In this case, those objects are vehicles and information can include things such as location.

During cyber surgeries with the client, experts discussed the threat environment (the risk faced by the client as a result of the products that collect this information being compromised), as well as how the telemetrics product that had been purchased could be improved for greater security, to provide the client with more assurance that the risk of data loss is minimised.

Impact

- Improved product for the Ministy of Defence.
- Improved understanding of risks in the telematics industry.
- Reduced risk of the telematics product being compromised, and data lost.

3 Countering the adversary

Countering cyber adversaries

The NCSC's Operations directorate leads the government response to counter and disrupt the UK's adversaries, capabilities and operations. While much of the team's work is secret by necessity, it is now publicising its strategy to keep the UK safe from malicious actions of other nations and serious organised criminals. The NCSC's vision is to be:

Impact driven

To prioritise efforts where the most harm to the UK is likely to be caused and where the NCSC can have the most impact in reducing it.

Threat focused

To disrupt the operation of cyber adversaries and contribute to harm reduction centres.

Vulnerability informed

Knowledge of which sectors in the UK are most at risk enables the team to determine which organisations need the most pressing support.

Inside the NCSC's Operations

To help explain what the NCSC does, it has highlighted three components of the three main functions of its operating model:

Threat Operations

The focal point for building the nation's technical knowledge of the threat and directing the strategic response to it.

Reduce harm by using the NCSC's unique intelligence and trusted partnerships to detect attacks directly and enable others' defence.

Increases the overall cost to cyber adversaries by developing and deploying counter cyber campaigns.

Incident Management (IM)

The NCSC is the lead government organisation for managing cyber incidents and has led on 658 incidents in the last year, providing support to almost 900 victim organisations, handling almost 1,800 incidents since commencing operations.

But the NCSC can't do this alone, and the IM team works closely with law enforcement, the UK intelligence community, wider government and the private sector.

The insights and knowledge derived from incidents is used to inform wider protective advice and guidance.

Assessments

Editorially independent but fully integrated into the NCSC's Operations, the Assessments team delivers all source, expert and independent assessment of cyber threats.

The team informs both policy and operational decision-making at the heart of government and also shares appropriately classified assessments to the wider UK economy and citizens.

Assessments also allow the NCSC to better predict adversaries' future behaviour and reduce impact.

In the last year the NCSC has led on

658

incidents

providing support to almost

900

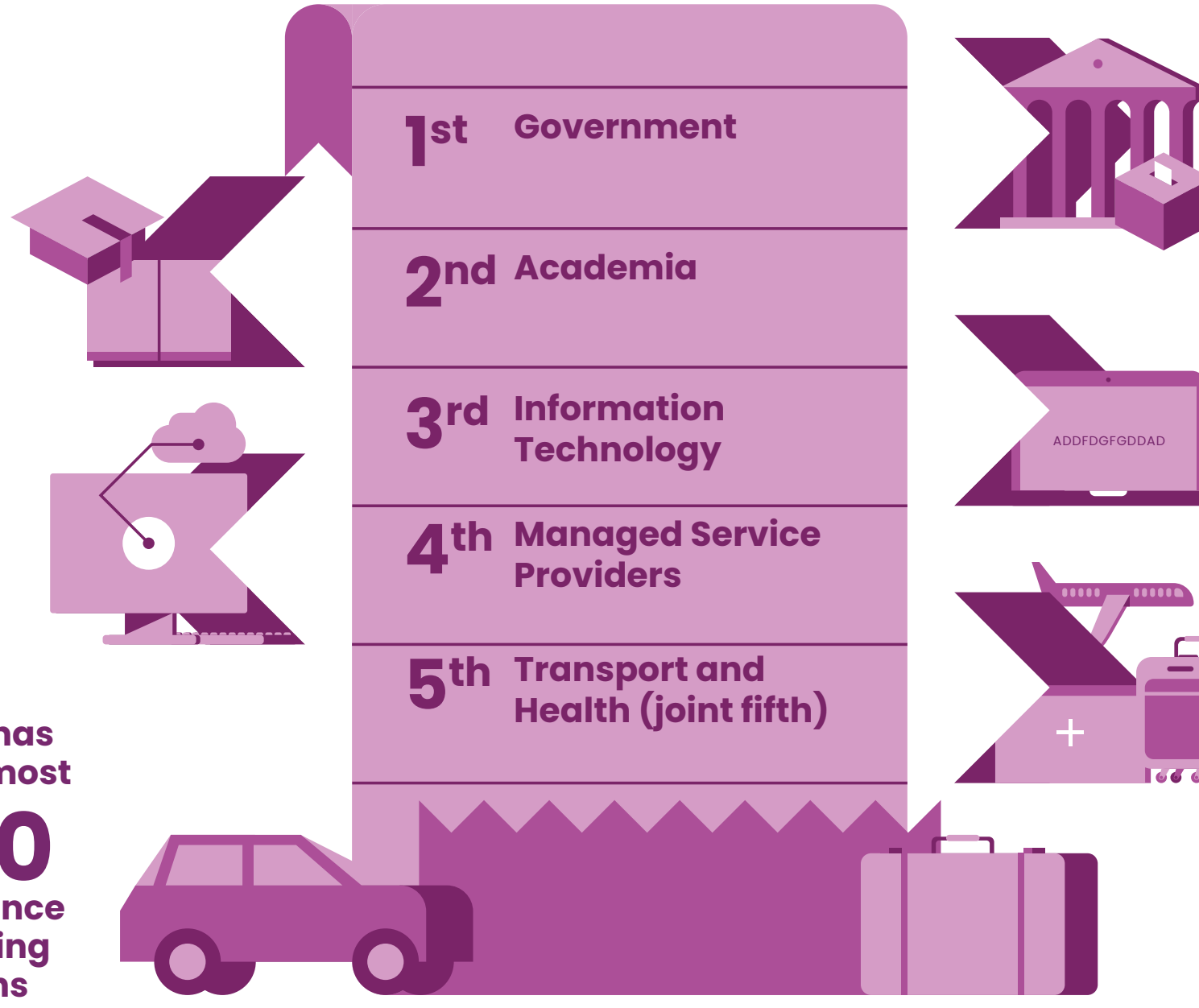
victim organisations

The NCSC has handled almost

1,800

incidents since commencing operations

The top five sectors supported by NCSC Incident Management



Calling out Hostile State Actors

The NCSC works collaboratively with a strong network of partners in the UK and internationally. Through this work with partners, the NCSC knows more about its main nation state threats, including Russia, China, Iran and North Korea, than it ever has before.

Working with the Foreign Commonwealth Office (FCO) on the public attributions of states (such as the Russian GRU being responsible for activity known in public as APT28), has been an overt action that shows other nation states that there will be consequences of their actions.

Underpinning a public attribution by government of this kind requires months of investigative work and sharing of information with partners, to build the investigative picture and a coalition of partners who will move in lockstep with UK government.

Knowledge Driven Operations

The NCSC strives to be an active organisation. That spirit has ensured the NCSC is recognised as a world leader – and the approach will not temper now the organisation is growing in maturity.

Central to the Operations team's work over the upcoming years will be a commitment to investigations into those who want to do harm to the UK. This means knowledge driven operations on the country's adversaries, their capabilities and their operations.

Working with law enforcement

"The NCSC is an invaluable partner as part of the National Crime Agency (NCA)-led Team Cyber UK law enforcement response to the scale and increasing complexity of cyber crime in the UK.

"Their expertise and joint working regularly helps the NCA to build the best possible intelligence picture of serious and organised crime threats.

"It has been extremely useful to have a one-stop shop that can coordinate information sharing in real time for live incidents - helping Team Cyber UK to better understand ongoing attacks, identify the next steps to mitigate the impact, develop attribution and deliver positive outcomes for the victims."

Jim Stokley, Deputy Director and Head of the NCA's National Cyber Crime Unit

Launching the NCSC's Cyber Defence Ecosystem

Information sharing is hardly a new concept and has been touted as a panacea for many years in the cyber security realm. The NCSC's ambition is to deliver an ecosystem that transforms cyber threat knowledge sharing, brings disparate initiatives together by giving them a clear purpose (to reduce harm), and enhances them in a coherent and coordinated way. Ultimately, the Cyber Defence Ecosystem (CDE) ensures the right knowledge gets to the right people at the right time, in the right format.

The CDE aims to foster a national (and hopefully international) ecosystem of collaborative threat analysis and automated threat sharing using open industry standards. The initiative complements the ACD programme, which since 2016 has shown how simple measures can greatly reduce commodity cyber attacks.

The purpose of the CDE is not to simply share information – it is to improve protection in service providers, enterprises and those who defend networks for their communities through driving concrete action based on shared knowledge.

The CDE is built on framework created by several years' work that now enables the NCSC to share understanding of threats and alert potential victims at rapid speed in an automated way.

This new ecosystem seeks to deliver four key outcomes:

1. Create a structured and automated ecosystem across the UK (and in time globally).
2. Share 'our part of the puzzle' to better defend the UK, partners and allies.
3. Build and enhance threat awareness to enable better detection and defence.
4. Rapidly alert enterprise victims of malicious activity.

"While we have responded to 658 incidents this year, we also want to help pass on knowledge to help organisations defend themselves.

"Working on hundreds of incidents has helped us to pull together advice to help organisations more effectively detect, respond to and resolve their own incidents.

"Having a well-planned and well-practised response plan will help minimise the damage caused by a cyber attack."

Paul Chichester, NCSC Director of Operations

The IOC Machine

The NCSC is committed to sharing as much of its knowledge in real time as possible. This has manifested itself in the creation of the Indicator of Compromise (IOC) Machine, which has transformed the way top sensitive material is 'declassified' into the public domain – greatly increasing the UK's resilience to cyber threats.

Since it went live this year, the technology has enabled a tenfold increase of vital indicators the NCSC shares with external internet service providers and industry partners. This now means that in an average month more than 1,000 vital indicators are being shared at the click of a button.

What has been changed?

The processes to determine whether information can be shared was previously done through a labour-intensive, manual process between various NCSC teams.

The IOC Machine, which sits in GCHQ's headquarters in Cheltenham, performs those thousands of checks in a matter of seconds. What would have previously distracted skilled analysts for a number of hours is now done within moments.

The ultimate power still rests with a human, as an analyst will consider the findings of the IOC Machine to determine whether the information around the compromise can be released. But the machine has rapidly expedited the process behind declassifying material that can be shared from the NCSC's top secret computers to people outside of the organisation.

As well as getting the information faster, the technology has freed up the NCSC's skilled analysts to concentrate on matters that maximise their expertise.

What does the IOC Machine declassify?

An 'Indicator of Compromise' can mean anything from understanding how an adversary works (their tools, techniques and practices), all the way through to specific information relating to an attacker, such as signatures of malware, or IP addresses frequently used by an adversary.

When it spots an adversary attacking the UK through intelligence, the NCSC wants to share that intelligence as quickly as possible, to defend itself and its allies against that threat before it causes damage. While being created as part of an intelligence agency has immeasurable benefits to the NCSC, it also presents some problems – and in particular, lengthy processes to declassify materials.

Previously, each indicator would need to be checked by an official to ensure it met a strict set of policies before being put into a queue for delivery. The process was so lengthy that by the time information got out it could be irrelevant.

Making the most of the NCSC's London headquarters

Situated in the heart of Victoria, London, the NCSC's 'Nova South' headquarters offer a dynamic environment to deliver the organisation's mission. It fosters a culture of innovation and ways of working fit to address 21st century security challenges.

Its central location, within walking distance to Whitehall, ensures the NSCS's expertise on key matters of national security can be called upon at short notice.

The facilities offer an open and flexible workspace, complemented by the full range of security capabilities enabling seamless working across classifications.

The NCSC maximises its London home to facilitate meetings, workshops and events all year round. It brings people together across economic sectors, the cyber security community and wider society to exchange ideas, share threat information and fix the things that matter.

The NCSC has welcomed a huge variety of guests, including prime ministers, ministers, senior officials and parliamentarians from across the world, through to industry leaders and the next generation of cyber talent with schools visits.

In the past year, the NCSC has hosted 197 events, with more than 9,000 attendees visiting its London headquarters.

The NCSC's London headquarters

4 International cooperation

Cyber attacks do not respect international boundaries, and many of the threats and vulnerabilities we face are shared around the globe.

Each state has sovereignty to defend itself as it sees fit, but it's vital that as a country, we work closely with our allies to make the internet as safe as possible.

Since its creation, the NCSC has worked with countries on every continent to help share information and improve cyber defence.

In the past year, the NCSC has welcomed international delegations from 56 countries.

NCSC representatives have visited more than 20 countries for bilateral and multilateral engagements, as well as participating as spokespeople in 30 international events.

The sentiments of partnership, friendship and common values of freedom, democracy and prosperity have been common themes throughout the NCSC's international engagements, which included visiting many other European countries, the USA, Australia, Canada and Japan among others.

International security cooperation

A range of international cyber dialogues were attended by leaders from across UK government including the Cabinet Office, the Foreign and Commonwealth Office, DCMS and the Department for International Trade. These conversations help develop the UK's relationships around cyber security and policy with its key partners. The NCSC's contributions include threat assessments, technical advice and insights from incident management practice to help coordinate operational approaches and enhance cyber security standards.

"The strength of the UK's cyber security export offer is built on our history of expertise, innovation, quality, and trustworthiness. The NCSC's support of the Department of International Trade and UK industry underlines all of these factors and is a vital part of our ability to increase the country's prosperity and improve national security."

The Rt Hon Elizabeth Truss MP,
Secretary of State for International Trade

"The NCSC's world-class capabilities and analysis have underpinned UK government attributions of malign cyber attacks. On the international front, the relationships it has built and the cyber capacity building programmes it has supported continue to play a vital role in delivering for Global Britain."

Alexander Evans, Director Cyber,
Foreign and Commonwealth Office

"As the next phase of the UK's relationship with the rest of Europe takes shape, we want to take our partnerships further and to develop new ones. I am proud of the increasing frequency with which I see my European counterparts and the deepening friendships we have nurtured, the boundaries we are removing and the ground we are breaking. The protection of our shared values of freedom, democracy and prosperity, all underpinned by the rule of law, is what we strive for."

Ciaran Martin, NCSC CEO speaking at the One Conference in the Netherlands

Jens Stoltenberg, NATO Secretary General at the Cyber Defence conference

Cyber Defence cooperation with NATO

The NCSC works closely with NATO to support its deterrence and defence objectives. As part of the Cyber Defence conference, NATO allies reinforced a pledge to ensure strong and resilient cyber defences.

The UK's Foreign and Defence secretaries hosted NATO's Secretary General, the North Atlantic Council Ambassadors and 120 cyber experts from 29 countries for conference sessions at the NCSC's headquarters and Lancaster House in London.

The NCSC strongly supports the full implementation of the Cyber Defence Pledge agreed in Warsaw in 2016, to ensure that the Alliance is cyber aware, cyber trained, cyber secure and cyber enabled.

"Hosting this NATO conference in London, at the NCSC, is a testimony to the strong commitment and leadership of the UK in the cyber domain. The NCSC is a model for national coordination, bringing together the best expertise to tackle a growing threat."

Jens Stoltenberg, NATO Secretary General

Five Eyes: Intelligence alliance at CYBERUK 2019

Experts from the 'Five Eyes' intelligence agency alliance advocated for global cyber attack resilience when sharing a stage together for the first time on UK soil.

The Five Eyes intelligence alliance comprises the UK, USA, Canada, Australia and New Zealand. Through the alliance, participating countries work closely together to keep their citizens safe from cyber threats.

The public session took place at the NCSC's annual conference, CYBERUK 2019, which saw 2,500 cyber security experts come together for a two-day event in Glasgow's Scottish Exhibition Centre.

The panel considered the shared threats and global vulnerabilities that exist in cyber systems. During the event, delegates had the opportunity to share their experiences of countering these threats and the different approaches used.

"What an excellent week at CYBERUK 2019! Scott Jones, Head of the Cyber Centre, was chuffed to represent Canada in Glasgow, especially during Wednesday's Five Eyes panel. It's always a pleasure to share the stage with our counterparts."

Canadian Centre for Cyber Security
via Twitter

NCSC CEO receives international award for cyber security leadership

The International Cyber Security Leadership Award was presented to Ciaran Martin at the Billington Cyber Security Summit in Washington DC.

The annual summit, held at the Washington Convention Centre, brings together a range of international experts in cyber security.

Before receiving the award, Ciaran Martin delivered a speech in which he reflected on the journey taken by the NCSC since he last spoke at the summit in 2016, shortly before the NCSC formally came into existence.

Five Eyes intelligence alliance panel chaired by Yasmin Brooks, Director of Cyber, DCMS

5 Securing the digital homeland:

How we help people do things for themselves

Smartphones, computers and the internet are now such a fundamental part of modern life, it's difficult to imagine how we'd function without them. That's why cyber security is so important.

From online banking and shopping, to email and social media, it's vital to take steps that can prevent cyber criminals getting hold of our personal accounts, data, and devices.

Confidence in the security of our digital lives is more and more important. If citizens don't think that their digital environment is safe, the country's prosperity and social cohesion is in trouble.

The NCSC is leading the way in supporting people and organisations to make sensible, informed, evidence-based decisions about the protective measures they can take, supporting them to manage their cyber security risk and make their online behaviour secure.

In tandem with this, the NCSC is doing more to take the burden of cyber security away from individuals by, for example, working closely with device manufacturers and online platform providers to build security into their products and services at the design stage, helping to protect people from the outset.

Supporting citizens

Cyber security is of growing importance, but many people do not understand the potential impact that threats can have, or how to manage them when they do. That's why the NCSC supports the UK's individuals and families to deal with the common cyber problems they may encounter in their everyday lives, helping them to stay secure.

The NCSC online

As well as advice on keeping secure at home and work by protecting people's devices and data, guidance is now easily accessible on topics such as how to shop online securely, how to use social media safely, and how to choose the right antivirus product.

The NCSC also offers advice on dealing with cyber crime, and how to report a problem when something goes wrong online. The NCSC's website includes tips for staying secure online, such as simple steps that can be taken in less than five minutes which significantly reduce the chance of falling victim to cyber crime. It also guides users on what to do if their computer has been attacked by a virus or an account has been hacked.

Additionally, there is more detailed advice on how to keep secure while enjoying online gaming, or ensuring the security of the increasing range of 'smart' technology available for the home.

The NCSC Enquiries Service

The NCSC's public enquiries service dealt with 11,000 queries over the past year, representing more than 200 enquiries every week.

The NCSC enquiries team can be contacted via enquiries@ncsc.gov.uk or by calling 0300 020 0964.

Building the NCSC's web presence

The NCSC has delivered a new and improved website that appeals to a wider audience by:

- **Responding to user feedback.**
- **Focusing on giving users an improved journey through the site with more intuitive navigation.**
- **Helping users to understand the importance of cyber security, and how they can protect themselves at work and at home.**
- **Making the platform as secure as necessary so as not to compromise on usability and functionality.**

The re-design included creating new sections on the website, designed around the specific needs of those using it.

The NCSC has conducted extensive user research to develop:

- **Quick-start guides tailored to each audience, so they can understand the information that's relevant for them.**
- **Multi-page articles to make it easier to work through complex topics.**
- **Shorter articles with more graphics so content can be quickly scanned.**
- **An alert banner on the homepage with important advice and guidance during cyber security incidents.**
- **A 'mobile-first' approach to make it just as easy (if not easier) to read content on smartphones and tablets.**

www.ncsc.gov.uk

Cyber Aware

The NCSC is working alongside the Cabinet Office, DCMS and the Home Office to deliver Cyber Aware – the national behaviour change campaign for cyber security.

The campaign establishes a single trusted voice to provide timely, accessible and consistent advice to individuals and smaller organisations, empowering them to take action to protect themselves online.

The Cyber Aware campaign is part of a wider set of initiatives across the NCSC and other government departments to better support individuals and families. This includes working with manufacturers to make software and systems secure by design, as well as some of the NCSC's Active Cyber Defence services.

The campaign connects with other government departments, the policing community and trusted third party supporters to help target the advice. The NCSC also works closely with a number of priority industry and voluntary sector partners to align messages and ensure all advice can be actioned.

Case study: WhatsApp

WhatsApp announced that it had found and fixed a security flaw in its messaging service that allowed hackers to compromise a device. In response, the NCSC published guidance advising users to update their WhatsApp app in order to protect themselves against potential attack. The guidance attracted a 54% increase in page views in its first week.

Case study: Black Friday and Cyber Monday

Shoppers were encouraged to learn and share simple cyber security steps to reduce the likelihood of falling victim to Black Friday and Cyber Monday scams. The NCSC published seven tips everybody should know before, during and after making an online purchase, teaming up with experts from Microsoft and the British Retail Consortium to challenge people to learn the tips and pass them on with a 'cyber chat'.

- Social media posts promoting the NCSC podcasts were shared 900+ times and liked 2,100+ times.
- The NCSC's Twitter following increased to over 50,000 as a result of social media activity.
- Digital assets were amplified by Santander, Lloyd's, Barclays Bank, Tesco, Get Safe Online, and Action Fraud.

Supporting organisations

The vast majority of organisations in the UK rely on digital technology to function. Good cyber security helps them take full advantage of the opportunities that technology brings.

The NCSC has worked with DCMS to identify priority sectors to tailor support. It has developed effective partnerships across 14 economic sectors as well as in education, charities and voluntary organisations. Since the NCSC launched, it has built trusted relationships, produced actionable guidance and innovative self-help tools to raise cyber security resilience across the sectors it serves.

Small and medium-sized organisations

Managing cyber security can feel daunting if you run a small business or are responsible for IT systems in charities, clubs and schools. The NCSC aims to help people feel confident in protecting their organisations.

Small Business Guide

The NCSC Small Business Guide provides five quick and easy steps that can significantly reduce the chances of businesses becoming victims of cyber crime. The guide, and accompanying action list, has been distributed around the country, reaching hundreds of thousands of small and medium-sized enterprises (SMEs). New guidance was launched this year to help small businesses prepare their response and plan their recovery from a cyber incident as quickly as possible.

"We are increasingly seeing the Cyber Essentials scheme being used successfully as a scaffold for the smallest of organisations to implement basic cyber security controls. The assessment questions are a structured way for small companies to become more educated and question their IT providers on security controls, helping to protect their business."

Dr Emma Philpott MBE, CEO, The IASME Consortium Ltd

Cyber Essentials

Helping organisations to protect themselves from the most common internet-based cyber threats, Cyber Essentials is available to all UK organisations, of any size and from any sector, that want to demonstrate their commitment to cyber security.

As part of DCMS and the NCSC's ongoing commitment to the scheme, improvements continue to be made. As well as ensuring that there is consistency in the way the scheme is operated, the NCSC wants to ensure that Certification Bodies and Assessors are all working to the same standard and have a clear and consistent minimum level of cyber security competence. The NCSC has awarded a five-year contract to the IASME Consortium Ltd to be its new Cyber Essentials partner from April 2020.

Currently, there is no automatic expiry date on certificates. For companies that are using Cyber Essentials to provide confidence in the security of their supply chain, this is not helpful. To support this and improve the process, from 2020, certificates will be issued with a 12-month expiry date.

"The NCSC's guidance for businesses to protect themselves has received positive engagement, and we anticipate it can reach and positively influence a wide portion of our business and commercial customer base."

Robert Mitchell, Content Manager, Commercial & Private Banking Digital Services, NatWest

"At ASOS we decided to incorporate the 'Exercise in a Box' content into our data security incident rehearsals. We found that the structure of the desktop exercises and simulation really helped to bring the rehearsals to life as well as encourage discussion and feedback."

George Mudie, Chief Information Security Officer, ASOS

Exercise in a Box

Exercise in a Box is an online tool which allows organisations to find out how resilient they are to a cyber attack, and to evaluate their readiness to respond. The tool was originally designed for SMEs, local government and emergency services, but high demand has seen many larger organisations using the tool to determine their own resilience.

Ciaran Martin, NCSC CEO, says: "Large or small, private or public sector, getting your organisation to practice what happens in a cyber attack helps you to spot the gaps in your fitness regime and shows where you might need to change up a gear."

Steve, one of the NCSC's experts who helped design the concept, says that exercising is one of the best ways for a business to find out how they would react to an incident.

"There are plenty of commercial products that offer exercises for companies, but they can be very expensive. We designed this to be a free tool because we wanted SMEs to get used to the concept of exercising.

"Any company can do these exercises on their own and know they are doing it in a safe environment. It's much better to practice beforehand rather than waiting for the real event.

"You don't have to be technically-minded to use this product. It's all done in a language that can be readily understood, with lots of supporting material and resources.

"We've been really impressed with how popular these exercises have been, not only in the UK, but around the world. We are now looking to evolve the concept for bigger businesses and the public sector."

www.ncsc.gov.uk/information/exercise-in-a-box

How to set up your own basic security logging system

Logging is an important tool for any organisation to keep track of and capture the kind of data that's central to understanding and recovering from a cyber breach.

This can be everything from logins to emails to firewall updates – all of which are considered security events. These logs provide a detailed record of all security events which can be used to manage cyber attacks and prevent them from happening in the future.

The newly launched open source project, Logging Made Easy (LME), is a self-install tutorial for small organisations to gain a basic level of centralised security and provide them with the tools they need to detect and protect themselves against cyber attacks.

"We know that small charities and voluntary organisations face real risks from cyber crime. By working in close partnership with NAVCA and its network of members, the NCSC has demonstrated a commitment to delivering cyber security protection to thousands of small voluntary organisations, working to support communities and people in need the length and breadth of the country."

Jane Ide, CEO, National Association of Voluntary and Community Action (NAVCA)

Charities

A government survey found that many of the UK's 180,000 charities had experienced cyber breaches, including viruses, phishing emails, ransomware attacks and identity theft.

While criminals may pursue financial gain, charities have also been attacked by hackers motivated by a personal or political agenda.

One UK charity lost £13,000 after its CEO's email account was hacked, and a fraudulent message sent to its financial manager with instructions to release the funds. Often such crimes go unreported because of a charity's fear of reputational damage.

In response to this, the NCSC has developed an educational programme designed to put the charity sector on a much stronger footing in cyberspace. The programme features a series of simple steps to protect organisations from attack, saving reputation, funds and data from falling into the hands of criminals.

Charities often prefer to seek advice from the bodies that represent them, so a partnership has been made with NAVCA which supports 145,000 charities and voluntary groups in England. A successful programme has been developed to train volunteers to deliver cyber safety awareness sessions for charities and voluntary groups within local communities.

The pilot showed a clear need for these sessions, with 96% of participants having felt that their increased awareness of cyber safety would improve their organisation.

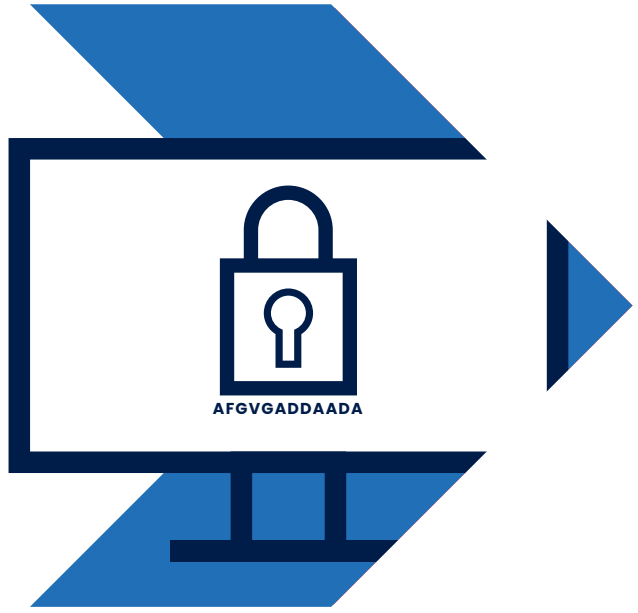
Top Tips for Staff

The NCSC's e-learning video, Top Tips for Staff, has proved immensely popular with small businesses and individuals, as a free, easily accessible guide to keeping safe online.

The 30-minute video, aimed at a non-technical audience, covers four key areas: protection against phishing, the importance of strong passwords, securing devices and reporting incidents when things go wrong.

The NCSC's Jack says: "The tips can be used by anyone, from large companies to people working on their own from home. It's highlighting the message to organisations that their first line of security is their staff.

"The advice has been taken up by many smaller businesses and charities which may not have their own IT departments or the resources to train employees in cyber security, attracting 1,500 hits per month to the NCSC website."



Schools and colleges

In partnership with the education sector, the NCSC has produced the first dedicated piece of research on cyber security in schools.

The NCSC spoke to over 430 schools across the UK, with 92% stating that they would welcome more cyber security training for teachers and staff. In response, the NCSC is developing a dedicated cyber security training package for schools.

Before this package is launched, the NCSC has created information cards that contain basic cyber hygiene messages for all staff working in the sector, which will be sent directly to over 10,000 schools across the country.

By increasing its engagement with schools and colleges, the NCSC has improved its understanding of the sector's cyber vulnerabilities. The NCSC has built links with the Association of Colleges and other umbrella bodies, and is helping the sector to improve its cyber resilience through existing NCSC products and services, including a webinar which is available to all senior college leaders through an industry portal.

Large organisations

Cyber Security Toolkit for Boards

Boards are pivotal in improving the cyber security of their organisations. The Board Toolkit has been created by the NCSC to encourage essential discussions about cyber security to take place between the Board and their technical experts, helping to raise the maturity, readiness and resilience of the UK's largest organisations against cyber threats.

New regulations, such as GDPR, mean that board members have a responsibility to ensure good cyber security protects their organisation's resilience in a complex digital world.

The NCSC's Katie says that while those on a board may have the confidence to ask the right questions on accounting or health and safety matters, they often don't have the same confidence on cyber security issues.

"The Board Toolkit gives organisations a starting point to examine this topic. They may want to put cyber security on the agenda, but are looking for a good place to start. This toolkit provides an introduction to a wide range of subjects in a digestible format.

"Board members can ask any questions, knowing they will receive an engaging and informed discussion with technical experts that will enable them to take positive action."

www.ncsc.gov.uk/collection/board-toolkit

"A common issue in the UK boardroom has been that cyber security is delegated to the IT department and does not gain attention as a priority until a breach has occurred. Given that a cyber attack is no longer an 'if' but a 'when', board members need help with guidance on what to protect and how to go about it. The Toolkit is a practical resource for board members and their CISOs to help identify best practice and better understand how to discuss cyber investment decisions in the boardroom."

Jacqueline de Rojas, President, techUK

Supply chain contracts

Most organisations rely upon suppliers to deliver products, systems, and services. But supply chains can be large and complex, involving many different parties. Effectively securing the supply chain can be hard, because vulnerabilities can be inherent or introduced and exploited at any point in the supply chain, in some cases causing wide-spread damage.

To combat this risk, the NCSC is introducing support to help companies protect themselves as part of their supply chain contracts, putting processes in writing to ensure that any cyber threat in their supply chains have as little negative impact as possible.

Supplier Check

The NCSC is piloting an initiative called Supplier Check, with critical suppliers to government. The product scans a company's external footprint to identify and highlight vulnerabilities, which can then be discussed with the supplier to raise their level of cyber security.

Universities

The NCSC has continued to engage with universities and research institutes, supporting them to defend themselves against and respond to cyber incidents.

Consultation conducted with universities will form the basis of Trusted Research, advice being jointly produced by the Centre for the Protection of National Infrastructure (CPNI) and the NCSC.

Trusted Research is designed to help the UK's world-leading research and innovation sector get the most out of international scientific collaboration, whilst protecting intellectual property, sensitive research and personal information.

The NCSC is now funding academics at Academic Excellence in Cyber Security Research (ACE-CSR) universities to undertake research projects to identify the specific cyber security challenges facing their own and others' institutions.

www.ncsc.gov.uk/report/the-cyber-threat-to-universities

Major Events Guide

The NCSC's Major Events Guide outlines how to incorporate Cyber Risk Management processes into event planning. The guide is designed for organisations running large scale sporting events, but steps and processes outlined can also be incorporated into general event planning.

www.ncsc.gov.uk/guidance/cyber-security-for-major-events

Commercial Assurance Services: Harnessing industry

Partnerships are vital to the NCSC. This is particularly true for Commercial Assurance Services, where the NCSC aims to increase its reach by harnessing industry.

The NCSC has embarked on an ambitious service transformation to simplify operations, enhance partnerships and extend its offering to meet the needs of new customers, as well as improving services for existing users.

A wide range of the NCSC's specialists work in technical, educational, legal, commercial, and engagement roles to make sure its industry partners – currently more than 180 organisations – meet required standards. These NCSC-assured products and services help provide people with confidence and trust in their choices.

Vulnerability Assessment is a critical service that keeps us all safe in our professional and personal lives. The NCSC's "CHECK" companies test systems and networks that are relied upon every day, looking for flaws that developers can fix before systems go live.

In the last year, these assured industry partners have raised over 2,000 reports detailing the vulnerabilities they have identified to keep the UK cyber safe.

Responding to Cyber Incidents is a critical service when problems arise. The NCSC's Incident Response experts work with its trusted industry partners to assist in identifying the root cause of incidents and assist in recovery and clean-up, ensuring that the most comprehensive lessons are shared along the way. The NCSC has involved the Information Commissioners Office, enriching dialogues with industry and helping to set the direction for the Cyber Incident Response service as it looks to enhance, improve and expand to meet new needs.

Commercial Assurance Services in numbers

12
Gas & Electricity Smart Meter products assured

39
Quality audits of industry partners carried out

40
Vulnerability Assessment partners

14,234
Cyber Essential Certificates issued

39% **increase on the previous year**

16
Industry partner events hosted, with

325
representatives from industry

253
Cyber Professional Certifications issued

19
cyber security training courses certified

Case study: Smart Meters

The NCSC has played a pivotal role in supporting the government's objective, which requires all 13 million UK households to be offered a Smart Meter.

It has worked with industry partners and BEIS, to certify 12 new gas and electricity meter products. In addition, the NCSC's industry partners have assured a further six communication products that transmit data from the meter in homes back to the utility provider.

"As always, the NCSC's technical insights continue to provide huge value in assessing current and future requirements, whilst their pragmatism and flexibility has been crucial in enabling us to continually review and improve the assurance processes where required."

Daryl Flack, Smart Metering Implementation Programme, BEIS

Cyber security communities

Cyber Security Information Sharing Partnership

The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative, set up to exchange cyber threat information in real time, in a confidential and dynamic environment, reducing impact on UK business.

Through CiSP, members are provided with a secure environment to engage with industry and government counterparts, supplying early warning of cyber threats, and helping them learn from experiences and successes of other users.

There are currently 15,571 registered CiSP members. The NCSC estimates this comprises 5,500 organisations from 22 sectors.

Industry 100

Industry 100 is the NCSC's principal initiative to facilitate close collaboration with the best and most diverse minds from outside the organisation. It brings together public and private sector talent to challenge thinking, test innovative ideas and enable greater understanding of cyber security.

In the last 12 months, 72 additional secondees, from more than 56 organisations, have worked across the NCSC in short-term placements, such as threat operations, capability development, and across engagement teams. From engaging with CyberFirst students and launching products to better alert their sectors to emerging threats, to developing systems which allow real-time detection of adversaries, the secondees have made invaluable contributions to the NCSC, their organisations and the wider cyber security community.

Law Enforcement and Regional Organised Crime Units

Managed by the National Police Chiefs' Council, Regional Organised Crime Units (ROCUs) are trusted partners of the NCSC that form the Cyber PROTECT Network and the wider National Crime Agency-led Team Cyber UK network. The ROCUs network is made up of more than 100 officers and staff across the country, helping to make the NCSC's advice as accessible as possible for communities to protect themselves against cyber crime. The network also enables large-scale mitigation work to be carried out across UK law enforcement.

The regional Cyber PROTECT teams were central to the launch of Exercise in a Box, helping the NCSC to reach local businesses, providing them with a practical way to test their cyber preparedness. The network worked with the Foundation for Social Improvement to raise awareness of the Small Charity Guide and support organisations in making improvements to their cyber security.

On a day-to-day basis, the network uses the NCSC's advice and guidance as the foundation for supporting victims of cyber crime, to help them recover and prevent repeat victimisation.

"The NCSC provides us with an up to date PROTECT framework containing current threat data, mitigation advice and interactive services to help keep the businesses and residents of Yorkshire and Humberside safe from the ever-evolving threats posed by cyber criminals."

DCI Tim Ingle on behalf of York and the Humber ROCU

CYBERUK 2019

Hosted in Scotland for the first time, CYBERUK 2019 reached nearly 3,000 delegates across industry, government and academia. The event delivered a wide range of content through demonstrations, talks and interactive workshops with world-leading experts.

Providing a dynamic forum for the UK's cyber security community, CYBERUK 2019 facilitated national and international conversations to deepen understanding, challenge thinking, create debate and foster collaboration in cyber security.

Working closely with partners, a strong Scottish presence was facilitated through speakers and exhibiting companies. The Scottish government ran a Cyber Week in Glasgow to coincide with CYBERUK 2019 and now plans to run this annually, ensuring a lasting legacy.

The event also encouraged Scotland's young people to consider a role in cyber security, inspiring the next generation of industry experts. Local schools were invited to visit the exhibition at CYBERUK 2019, to hear from the NCSC and industry experts, and develop their skills in 'cyber games', through code-breaking challenges, cipher decryption, and lessons in Minecraft and Python.

The NCSC will be hosting CYBERUK 2020 in Wales.

CYBERUK 2019 at the Scottish Event Campus, Glasgow

Paul Chichester, NCSC Director of Operations welcomes delegates

Highlights

- **2,767** delegates
- **240+** speakers
- **159** sponsors and exhibitors
- **21** countries represented
- **22** 'Spotlight Stage' lightning talks
- **48** audience-centred stream sessions
- **17** interactive workshops
- **Five Eyes** panel discussion on global cyber issues
- **9** Scottish SMEs showcased in the exhibition's 'Scotland Street'
- **81** children attended from Glasgow schools
- **1,800+** pieces of media coverage
- **8,187** uses of #CYBERUK19 on social media
- **92%** of delegates rated the event overall as good or excellent

"CYBERUK 2019 was a great opportunity to hear from key influencers in the industry and learn from their experience and best practice. It was a privilege to host the event in Glasgow and was a testament to Scotland's commitment to cyber security. To have all these varied stands, speakers and organisations come together is a fantastic opportunity to network and build relationships."

Kirstie Steele, Cyber Resilience Unit, Scottish Government

"CYBERUK is exactly what you can expect from a conference led by the NCSC, which continues to focus on high leverage and high impact activities. Their innovation is setting the bar for cyber security efforts across the Five Eyes, and we are grateful for the partnership."

Rob Joyce, former Senior Cyber Security Advisor, National Security Agency

6 Cyber capability for the future:

How we work with people

The NCSC uses industry and academic expertise to nurture the UK's cyber security capability. It helps to build the UK's talent pipeline, promote innovation and develop the country's cyber security research, ensuring a secure, resilient and prosperous economy by providing people and organisations with the cyber security skills they need.

People

Working with industry, government and academia, the NCSC strives to support the next generation of students, researchers and cyber security professionals at a time of rapid change, to help them develop the skills they need to have a rewarding career in cyber security.

CyberFirst

CyberFirst aims to identify and nurture young talent, engaging students from all backgrounds and regions, helping them to explore their passion for technology and providing them with the necessary skills and knowledge to put it into practice.

CyberFirst Bursaries

Now in its fourth year, the CyberFirst Bursary is continuing to provide financial support, cyber security training and work experience to over 750 UK undergraduates, helping young people kick start their career in cyber.

Each year hundreds of carefully selected and highly talented students are provided with a bursary of £4,000 for each year of their undergraduate study. They return each summer to spend a minimum of eight weeks learning key cyber security skills in either the CyberFirst Academy or placements with more than 70 industry and 14 government members of CyberFirst.

To date, 56 Bursary students have graduated from the CyberFirst programme and have moved into full time cyber security roles with companies and government departments, including; BAE Systems, Barclays, IBM, Netcraft, Encipher Ltd, Lockheed Martin, DSTL, HMGCC, MET Police, the MoD, GCHQ and at the NCSC.

Since 2017, the NCSC has seen a 181% increase in the number of industry partners supporting this scheme.

CyberFirst pathway

CyberFirst
Girls Competition

The CyberFirst Girls Competition inspires the next generation of young women to consider a career in cyber security. This free, nationwide contest is open to girls in Year 8 in England and Wales, Year 9 in NI and S2 in Scotland.

CyberFirst
Defenders

A free five-day residential and non-residential course aimed at 14 to 15 year-olds, helping to increase awareness of cyber security, whilst also equipping them with relevant practical skills they can apply in their own life.

CyberFirst
Advanced

A free five-day residential and non-residential course aimed at 16 to 17 year-olds, to hone the skills and behaviours they need to enter the cyber security or computing workplace for real.

CyberFirst
Bursaries

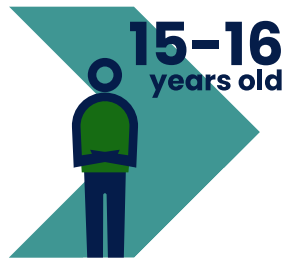
A CyberFirst Bursary offers undergraduates £4,000 per year financial assistance and paid cyber security training each summer to help kick start their career in cyber.

CyberFirst
Adventurers

A free one-day non-residential course aimed at 11 to 14 year-olds. The course consists of four themed modules offering interactive, hands on, self-guided, exploratory learning.

Cyber
Discovery

Cyber Discovery is the government's free, online, extracurricular programme developing the cyber security skills of teenagers across the country. For students aged 13 to 18, the NCSC is seeking problem solvers, code crackers and, most importantly, those who never give up.



CyberFirst
Futures

A free five-day residential and non-residential course aimed at 15 to 16 year-olds, to explore advanced cyber security threats to devices, apps and software, and discover ways to prevent them.

CyberFirst
Degree Apprenticeships

A CyberFirst Degree Apprenticeship allows undergraduates to earn whilst they learn, ready for a job with GCHQ.

For more information visit:
www.cyberfirst.ncsc.gov.uk

"The CyberFirst Bursary scheme has been the best thing I've ever done in my life and has opened so many doors for me. I've had the opportunity to meet new people, make new connections and gain new skills."

Tia, CyberFirst Bursary student, Scotland

"We have benefitted tremendously from six CyberFirst Bursary students in the last four years. They have been amazing students, whose ability to absorb ideas and deliver results at pace is a joy and huge benefit to us all."

Martin Huddleston,
Head of Cyber, APMG

"CyberFirst has given us access to a wealth of budding cyber talent. By giving students the skills and investment they need to live and work securely online, CyberFirst is totally aligned with our own mission to make society a safer place. It's through initiatives like this that we will ensure the industry achieves ongoing sustainable growth, and we look forward to strengthening our partnership in the coming years."

Colin Gillingham, Director of Professional Services, NCC Group

CyberFirst Courses

The CyberFirst Courses are carefully designed to bring out every student's potential. Open to 11 to 17 year-olds, students are encouraged to understand how everyday technology works and importantly, how to protect it. This year, courses took place in Paisley, Cardiff and Belfast, as well as Newcastle, Southampton, Warwick, Gloucester and London.

All CyberFirst summer courses have been credit rated by the Scottish Qualification Authority (SQA) and have been independently certified as a GCHQ Certified course, which is a fantastic endorsement of the course content, quality and delivery.

Joanna's CyberFirst journey

Joanna reached the final of the CyberFirst Girls Competition at the age of 12, before going on to complete the CyberFirst Adventurers, Defenders, Futures and Advanced courses. She is now considering a CyberFirst apprenticeship.

"Before the CyberFirst Girls Competition, I didn't really know much about GCHQ and the kind of jobs that were available. I had an interest in computers, but I wasn't sure where to go next. After taking part in the finals of the competition, I realised I had a love of information gathering and evaluation. The competition sparked a passion that has led me to want to pursue a career in intelligence/data analysis.

"After the competition I was invited to join the CyberFirst courses, which excited me as I wanted to find out more about technology and how it can be used to protect us. During the course, we were told about the CyberFirst apprenticeship and bursary, and what our next steps could be if we were interested in a career in cyber security. I'm now hoping to apply for the apprenticeship when I finish sixth form. I probably would have never found out about this area of work if it wasn't for the CyberFirst Girls Competition!"

90%
of CyberFirst
Defenders, Advanced and Futures students would like to pursue a career in cyber security, with 936 students hoping to attend additional CyberFirst programmes

809
students
aged 11 to 14 years-old, took part in Cyber Adventurers courses, 50 of whom attended the course at the NCSC's headquarters

A further
1,100
free places
were taken up by 15 to 17 year-olds on CyberFirst Defenders, Futures and Advanced courses

Cyber First

705
young women
who took part in the CyberFirst Girls Competition, enjoyed free places on CyberFirst Defenders courses

Overall, course applications increased by 29%
with a 47% increase in the number of female applicants

CyberFirst Girls Competition

The CyberFirst Girls Competition is part of the NSCS's efforts to get more girls into cyber security. It provides a fun but challenging environment to inspire the next generation of young women to consider a career in the industry.

With the largest and most diverse set of participants, the CyberFirst Girls Competition 2019 was the most successful to date. Nearly 12,000 girls from 841 schools entered from all corners of the UK – from Jersey to Caithness, Essex to Londonderry – with double the number of schools participating from Scotland and Wales.

After an online round of codebreaking challenges, the top 10 schools competed in a face-to-face Grand Final in Edinburgh. The winning team saved the day for a fictitious company facing a cyber incident, developing skills in networking, cryptography, logic and coding along the way.

Following the competition, 98% said they would like to learn more about cyber security.

"We were delighted to work with the NCSC to bring this course to our bright and engaged young students. Women are very underrepresented in the global cyber industry but, here at TIGHS, we have exceptionally talented girls who can help make our country the safest place to live and do business online. Let's get them excited about computing, early."

Asia Ali, Assistant Principal of Tauheedul Islam Girls' High School, Blackburn

"The competition has helped me learn lots of new things that I had never heard of before. It opened my eyes to what cyber security is really like, and what it takes to become a cyber security professional. There aren't many girls in cyber security, so it is important to encourage more to get involved."

Erinna, The Queen's School, Chester

Cyber Schools Hub at Newent Community School

Cyber Schools Hubs

The last 12 months have seen the first full academic year of Cyber Schools Hubs, created to develop a model for engaging with schools on cyber security. The project currently supports schools across Gloucestershire in a variety of ways, from sharing technical equipment and lesson plans, to funding educational visits and linking with industry supporters.

Schools have set up extra-curricular cyber-related clubs, augmenting the learning and inspiring the students. Newent Community School, for example, organised a Dragons' Den-style event, developing ideas for wearable technology. They are now looking to run a regular wearable tech lunchtime club to build upon the interest now generated amongst students.

Wyedean School welcomed 200 Year 5 children for a full day of Computer Science and cyber security, and Cleeve School ran a Hacking Skills day, providing an opportunity for students to use the new hacking servers gifted to the project.

Organisations from across the UK are now actively involved in supporting participating schools, from hosting visits, delivering events, providing facilities for schools to use and offering work placements.

"Cyber Club has helped my confidence in computing lessons. It has given me access to technology and equipment that I have never experienced. Attending Cyber Club has made me consider Computer Science as a job in the future, as well as helping me develop my problem-solving skills in everyday life."

Sam, Year 8 student

Cyber Schools Hubs statistics

26
participating schools

250
extra teaching hours of computer science activities delivered across four schools

120
crates of educational equipment such as specialised computers, robots and games, shared by schools around the county

19
organisations voluntarily participating in the project

"The Cyber Schools Hub project is instrumental in enabling our delivery of successful and impactful sessions with talented young people who are incredibly passionate about the topic and are willing to learn how to practice their skills legally and safely. Through the opportunities provided by the Cyber Schools Hub, we have also significantly broadened our own understanding into why more young people are becoming interested in cyber and the opportunities available for them in a variety of exciting careers."

Representative, South West Regional Organised Crime Unit

Certified Degrees

The NCSC Certified Degree community has continued to grow, with seven certified undergraduate degrees and 24 certified postgraduate degrees. Universities across the UK, from Bristol to Dundee, Pontypridd to Belfast, now offer certified degrees. This year also saw the publication of a new standard to certify Degree Apprenticeships in Cyber Security, based on the Institute for Apprenticeships and Technical Education's recently published Cyber Security Technical Professional standard.

"Gaining certification has led to a continual increase in student numbers."

Dr Rich Macfarlane, Edinburgh Napier University

Cyber Security Body of Knowledge

Cyber security encompasses a wide range of disciplines, but its relative youth means it lacks the coherence found in more mature STEM fields. In response to this, the NCSC set up the Cyber Security Body of Knowledge, with the long-term aim of contributing to the development of the cyber security profession. The project's purpose is to codify the cyber security knowledge which underpins the profession. The project focuses on providing learning pathways, professional development and careers information for the people of the UK.

Apart from giving structure to the core knowledge, topics and reference texts, the project will enable the UK to focus learning pathways, professional development and careers information. The NCSC has been working with the cyber security community to identify key knowledge areas. To date, the project has issued 19 knowledge areas for review, with 14 published as version 1.0, including Human Factors, Adversarial Behaviours and Software Security.

Research

Working with partners in government, industry and academia, the NCSC identifies and supports excellence in cyber security research and encourages industry investment. By continuing to work with external partners, the NCSC is helping to put the UK at the forefront of internationally leading cyber security research.

Cyber security for the 2020s

The NCSC conducts research into new technologies and pioneers innovative approaches to keeping the UK safe online. Research is essential to ensure the mission continues to be successful in the long-term. Research activities span the full range of NCSC interests, from new ways of protecting citizens to its classified research into defending critical systems from highly motivated attackers.
It is important to recognise that just as current research will drive the NCSC's future work, its current successes are built on years of research and development, in-house as well as in academia and industry.

Academic Centres of Excellence in Cyber Security Research (ACE-CSR)

Academic Centres of Excellence in Cyber Security Research (ACE-CSR) are at the forefront of cyber security research in the UK and showcase the UK's research capabilities on the global stage. The NCSC and the Engineering and Physical Sciences Research Council recently welcomed De Montfort University and Northumbria University to the ACE-CSR community, bringing the total number of universities recognised to 19.

Cardiff University has been recognised as an ACE-CSR since 2018.

Peter Burnap, Professor of Data Science and Cyber Security at Cardiff University believes the awards act as a magnet for research excellence in the UK and are "a great bridge in the process of turning research into technological products and services."

He says: "The role of academic institutions is to drive innovations forward and at Cardiff, we decided to work with the local community to see what industry viewed as some of the cyber security challenges for them.

"We started work with Airbus to translate our research into products and services now being used by the company, as well as their industry partners such as Rolls-Royce and BT. Over 10 years we have developed a strong narrative of converting research into practical applications.

"The NCSC needs a lot of information and the academic world holds a great deal of that, so it's an ideal link.

"The NCSC is driving the ideas that come from the academic community into the research councils for funding prioritisation, in a process that is helping to maintain the UK's status as world-leader in cyber security."

Research Institutes

The NCSC is now supporting four successful academic Research Institutes, to develop cyber security capability in strategically important areas. Each one is focusing community effort in its respective area and encouraging interaction between academia and industry.

- Research Institute in Science of Cyber Security
- Research Institute in Verified Trustworthy Software Systems
- Research Institute in Trustworthy Interconnected Cyber-physical Systems
- Research Institute in Secure Hardware and Embedded Systems

The Research Institute academics are increasingly providing their expertise into relevant government policy activity. Examples include the UK Research and Innovation-managed 'Digital Security by Design' challenge advisory board and assisting the DCMS and the NCSC with developing the Institute of Technology Code of Practice.

CISSE UK

The Colloquium for Information Systems Security Education (CISSE) is an academic-led organisation, which brings together all those from government, industry and academia who care about cyber security education from primary to tertiary level.

In the last 12 months, the NCSC has supported the creation of CISSE UK, the first official, chartered foreign chapter of CISSE.

Quality

Commercial Assurance Services: Cyber training and education

The work the NCSC does to set the standards for training and education for cyber professionals has far reaching impact, by touching the lives of everyone who comes into contact with it. It works closely with accreditation and exam institute, APMG, to assure the validity of its cyber training courses.

The NCSC works with examining bodies to certify cyber professionals, guaranteeing a standard of professional that delivers cyber services or products to organisations across the country.

Cyber security awareness training sessions at the NCSC's London headquarters

Innovation

The NCSC aims to develop the UK's cyber security ecosystem by transforming innovative ideas into real world solutions.

Cyber Accelerator

The NCSC Cyber Accelerator supports the growth of start-up cyber companies which are bringing new security products to market. It aims to support the emerging cyber security industry within the UK, encouraging skills, jobs and growth.

The third cohort of the NCSC Cyber Accelerator has created 30 jobs, won 18 trials, proof of concept and contracts and raised more than £15 million in funding.

"Taking part in the programme was very important to challenge us and build our credibility. The team was very encouraging, and to have access to their technical expertise was invaluable. It's been a brilliant experience for us to be mentored and assisted by the NCSC."

Simonetta d'Ottaviano,
Co-Founder and CEO, Nettoken

Cyber Accelerator case study: Nettoken

Simonetta d'Ottaviano is CEO of Nettoken, an identity management platform designed to encourage awareness of an individual's expanding digital footprint, helping improve their personal security. The platform keeps track of all of a subscriber's online accounts, making everything accessible from a single control panel.

"The average internet user is signed up to around 150 active accounts, putting them at high risk of cybercrime," says Simonetta, who co-founded the firm with Charlotte Slingsby and Ela Neagu while completing her master's in engineering.

"We realised that most cyber security products are designed for businesses and we wanted to look at it from an individual's point of view."

They designed a management platform for a user's digital identity; a way of organising multiple online accounts, which also acts as a single password manager.

"Nettoken provides an overview of all the services that you may have signed up for, whether it was to book a flight or create a new Wifi access. It acts as a manager which puts them into groups, your shopping accounts in one, utilities and financial accounts in another."

She explains: "We wanted to create a usable tool that has cyber security embedded, without the user having to worry too much about it."

The service is already proving popular and the company is aiming to soon reach 5,000 paying customers.

Simonetta believes Nettoken has benefited greatly from being included in the NCSC Cyber Accelerator programme.

"Taking part in the programme was very important to challenge us and build our credibility. The team was very encouraging, and to have access to their technical expertise was invaluable. It's been a brilliant experience for us to be mentored and assisted by the NCSC."

Cyber Accelerator case study: LuJam

Five years ago, Tim Moran set up LuJam Cyber to combat a major challenge in cyber security, encouraging SMEs to understand that whatever their size, they are not immune to attacks.

Last year, 31% of all SMEs suffered from hostile incidents and, as Tim states, "The worst thing is that the majority of these attacks were preventable. Many of these companies are relying on a firewall and antivirus alone, often because other forms of protection are too expensive."

Tim recognised that SMEs require similar levels of security to larger enterprises but delivered in a way that is easy for a business owner to use and understand, without needing to be an IT specialist. After attracting investors to match a £250,000 grant won from Innovate UK – as well as selling his house to raise more capital along the way – Bristol-based LuJam launched a subscription service offering customers full protection against the latest cyber threats for all of their devices.

"Following extensive trials, we were ready to provide companies with cyber security software at a competitive price. Our goal is to help Managed Service Providers (MSPs) take their customers on a steady journey to improved cyber hygiene.

"Our service is powered by cloud analytics and network scanning that discovers IT assets, assesses risks, blocks bad connections and provides continuous monitoring."

LuJam spent nine months working with the NCSC, an experience Tim views as incredibly rewarding. After five years of development, the future looks bright for the company, which is now in trials with several major partners and investors.

Tim says: "Our solution is applicable anywhere in the world and we are already involved in a number of initiatives in Commonwealth countries. We've also started to explore much larger opportunities in cyber insurance, enterprise supply chains and enterprise homeworkers."

"We've been really encouraged by the positive experience we've gained with the NCSC. We firmly believe that all businesses should be encouraged to reach Cyber Essentials certification, with continuous monitoring of cyber security becoming best practice for all."

Tim Moran, Founder and CEO,
LuJam Cyber

CyberFirst Courses

Venue	Course
Beaufort School	Adventurers
Cardiff Metropolitan University	Adventurers, Defenders, Futures, Advanced
Energus Cumbria	Defenders, Futures, Advanced
Imperial College London	Defenders, Futures, Advanced
Lancaster University	Adventurers
NCSC headquarters, London	Adventurers
New Scotland Yard	Adventurers
Queen's University Belfast	Adventurers, Defenders, Futures, Advanced
RAF Benson	Defenders
RAF Lossiemouth	Defenders
Tauheedul Islam Girls' High School	Adventurers
University of Bristol	Advanced
University of Central Lancaster	Advanced
University of Gloucestershire	Adventurers Adventurers, Defenders,
University of Leicester	Adventurers
University of Kent	Defenders
University of Newcastle	Adventurers, Defenders, Futures, Advanced
University of Southampton	Futures, Advanced
University of Warwick	Defenders, Futures, Advanced
University of the West of England	Adventurers
University of the West of Scotland	Adventurers, Defenders, Futures, Advanced
University of Wrexham	Defenders

Research Institute – Host Universities

Research Institute in Science of Cyber Security – University College London
Research Institute in Verified Trustworthy Software Systems – Imperial College London
Research Institute in Trustworthy Interconnected Cyber-Physical Systems – Imperial College London
Research Institute in Secure Hardware and Embedded Systems – Queen's University Belfast

Academic Centres of Excellence in Cyber Security Research

University of Birmingham
University of Bristol
University of Cambridge
Cardiff University
De Montfort University
University of Edinburgh
Imperial College London
University of Kent
King's College London
Lancaster University
Newcastle University
Northumbria University
University of Oxford
Queen's University Belfast
Royal Holloway, University of London
University of Southampton
University of Surrey
University College London
University of Warwick

NCSC - Certified Degree Providers

University of Birmingham
Edinburgh Napier University
Imperial College London
Lancaster University
University of London International Academy
University of Oxford
Oxford Brookes University
Queen's University Belfast
Royal Holloway, University of London
Sheffield Hallam University
University of South Wales
University of Southampton
University of Surrey
University College London
University of Warwick
University of the West of England
University of York

7 Celebrating 100 years of GCHQ's cyber mission

The last century has seen GCHQ placed at the heart of the nation's security and it is committed to continuing to keep the UK safe for the next 100 years and beyond. This year saw a number of events take place to celebrate the milestone.

GCHQ 100 years

The Science Museum launches exhibition revealing GCHQ secrets

Coinciding with the centenary and in a first for a UK intelligence agency, GCHQ has launched a new exhibition which will take visitors through the history of secret communications. 'Top Secret: from Ciphers to Cyber Security', explores a century's worth of intelligence that underpin GCHQ's vital role.

Supported by funding from the National Cyber Security Programme, free tickets are available to book on the Science Museum's website. From July to September 2019, 80,000 people visited the exhibition. It runs in London until February 2020, moving to Manchester's Science and Industry Museum in October the same year.

Royal celebrations for GCHQ

Her Majesty The Queen visited the original top-secret home of GCHQ as part of the centenary celebrations for the UK's intelligence, security, and cyber agency (see image top right).

During The Queen's visit, she met with the 2018 CyberFirst Girls Competition winners from The Piggott School.

As part of the celebrations, His Royal Highness the Prince of Wales also visited GCHQ's Cheltenham headquarters, where he was introduced to the NCSC's Technical Director Dr. Ian Levy, as well as teachers and students from schools taking part in the Cyber Schools Hubs pilot. His Royal Highness also met a team from Girl Guiding South West England, who showed off their new set of Girl Guides' Cyber Skills badges, developed in conjunction with the NCSC.

"It is reassuring that with the founding of the National Cyber Security Centre, which has tackled over 1,500 significant cyber attacks since opening in 2016, the cyber security of this country is in safe hands."

His Royal Highness The Prince of Wales

The GCHQ Centenary Puzzle book II

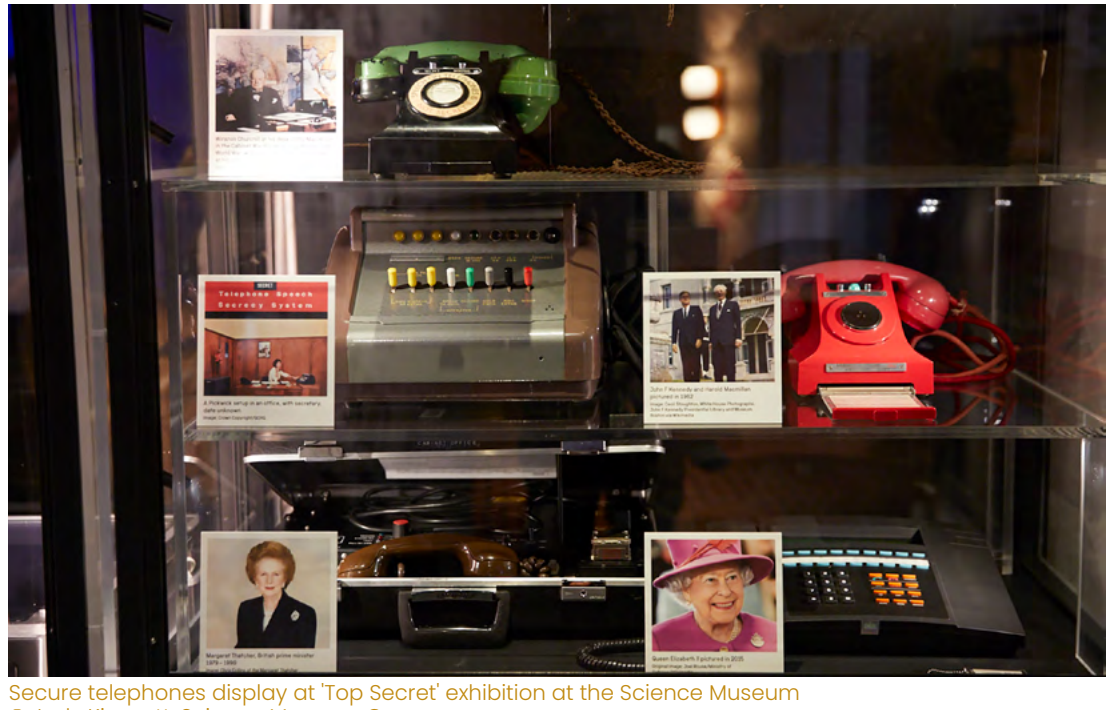
The NCSC contributed to the development of GCHQ's Puzzle Book II. It includes stories from the organisation's inception, all the way through to the opening of the NCSC and puzzle designs based on previous cyber competitions.

The proceeds from the sales of Puzzle Book II will be donated to Heads Together, which works to raise the profile of the importance of mental health.

"For the first time the public will be given a glimpse into our secret history of amazing intelligence, world-leading innovation, and most of all brilliant people. And – as the threats to the UK become more diverse and complex – it's a chance to encourage the next generation of recruits. Because at GCHQ we believe that with the right mix of minds, anything is possible."

Jeremy Fleming, Director, GCHQ

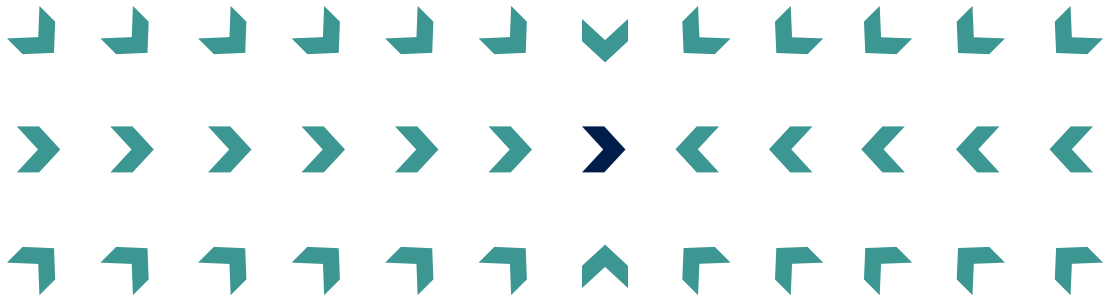
Her Majesty The Queen unveils an historic plaque at Watergate House, the 1919 birthplace of GCHQ



Secure telephones display at 'Top Secret' exhibition at the Science Museum
© Jody Kingzett, Science Museum Group

Can you find the secret message?

Decrypt at **ncsc.gov.uk/annual-review-2019**



ncsc.gov.uk/annual-review-2019

@NCSC

National Cyber Security Centre

@cyberhq

Designed and created by Agent Marketing Ltd.
agentmarketing.co.uk