Cabinet Office

The UK Cyber Security Strategy

Report on Progress and Forward Plans

December 2014

The UK Cyber Security Strategy

Report on progress and forward plans – December 2014

The Government first published its National Cyber Security Strategy in 2011. The objectives set out in that Strategy continue to guide our work today. Those objectives are:

- to make the UK one of the most secure places in the world to do business in cyberspace;
- to make the UK more resilient to cyber attack and better able to protect our interests in cyberspace;
- to help shape an open, vibrant and stable cyberspace that supports open societies;
- to build the UK's cyber security knowledge, skills and capability.

To deliver these objectives, the Government is working through the National Cyber Security Programme to:

- further deepen our national sovereign capability to detect and defeat high-end threats;
- ensure law enforcement has the skills and capabilities needed to tackle cyber crime and maintain the confidence needed to do business on the Internet;
- ensure critical UK systems and networks are robust and resilient;
- improve cyber awareness and risk management amongst UK business;
- ensure members of the public know what they can do to protect themselves, and are demanding good cyber security in the products and services they consume;
- bolster cyber security research and education, so we have the skilled people and knowhow we need to keep pace with this fast-moving issue into the medium-term; and
- work with international partners to bear down on havens for cyber crime and build capacity, and to help shape international dialogue to promote an open, secure and vibrant cyberspace.

This work is supported by the National Cyber Security Programme (NCSP), which with dedicated funding of £860 million over five years has supported a wide range of projects to develop cyber security capabilities and stimulate the UK's cyber security market. A breakdown of NCSP spend is provided at the end of this document.

This report summarises progress over the last 12 months and sets out our plans for the year ahead.

OBJECTIVE 1: MAKING THE UK ONE OF THE MOST SECURE PLACES IN THE WORLD TO DO BUSINESS IN CYBERSPACE

Raising industry awareness and providing guidance

Government has been working to raise businesses' awareness of the threat from cyber crime and espionage and encourage firms to embed effective cyber security risk management practices.

As a centrepiece of this campaign, two years ago Government published its '10 Steps to Cyber Security' guidance for business. An updated version, highlighting supporting initiatives that have started since the original launch, will be published early next year: the Government working with trade associations, professional bodies, and accountants and auditors will continue to ensure its messages reach the largest possible audience.

To support this material, the Government has been working to develop case studies which provide an independent, authoritative overview of the most common types of attack. These will be published alongside the refreshed '10 Steps' guidance.

Use of the '10 Steps' guidance has been backed by a Cyber Security Governance Health Check for FTSE350 companies**.** This year saw the second such Health Check. Carried out by BIS in partnership with the audit community, the Health Check assesses how the boards of top UK companies are managing cyber risks and enables them to benchmark themselves against their peers and competitors. Companies are receiving data from the latest round during December 2014 and the full results will be published in the New Year.

The Government's general guidance to business has been supported by specific products aimed at sectors judged particularly at risk, or who have a special role to play in spreading awareness. This year BIS published cyber security guidance for the corporate finance sector in partnership with the Institute for Chartered Accountants in England & Wales (ICAEW). The guidance helps tackle cyber threats around mergers & acquisitions, buyouts and venture capital. BIS is also working in partnership with the legal and accountancy sectors to improve cyber security awareness. To support this in October 2014 BIS, the ICAEW and the Law Society announced a new online training course to help lawyers and accountants protect themselves, their clients and the sensitive information they hold on their clients' behalf.

The Department for Business, Innovation and Skills also launched Cyber Security Guidance for Non-Executive Directors (NEDs) in December 2014. NEDs are the 'critical friends' who sit on company boards and offer advice from an external perspective based on their own expertise so are in a good position to advise companies on cyber security and encourage good management of cyber risks. This work complements the ‘10 Steps’ guidance and supports BIS’s wider work to improve cyber risk management in company boardrooms.

For small and medium sized businesses the Government has developed and launched a free online training course called 'Responsible for Information'. The course helps employees and small business owners understand information security and associated risks, and provides an introduction to protection against fraud and cyber crime.

Cyber Security Guidance for Businesses	
The 10 Steps to Cyber Security	Guidance for Chief Executives and board members on safeguarding their most valuable assets, including personal data, online services and intellectual property
Small businesses: what you need to know about cyber security	Guidance based on The 10 Steps, tailored for micro, small and medium-sized enterprises
Responsible for Information	E-learning for micro, small and medium sized businesses; FREE to access and role-based for employees, Information Asset Owners and Directors or business owners
Cyber Security for Legal and Accountancy Professionals	E-learning to help lawyers and accountants protect themselves, their clients and the sensitive information they hold on their clients’ behalf.
Cyber Security for Non-Executive Directors (NEDs)	Guidance to support NEDs who can advise companies on cyber security and encourage good management of cyber risks
Cyber Security in Corporate Finance	Guidance led by industry to help tackle cyber threats around mergers & acquisitions, buyouts and venture capital

The Government has continued a partnership with Universities and the Higher Education sector to improve awareness and encourage research and innovation to improve cyber security. BIS worked with Universities UK to carry out a Cyber Security Governance Health Check for higher education institutions. Nearly 50% of UUK members participated in the Health Check and have now received a personalised benchmark report identifying the areas they need to address. UUK will be releasing a summary report later this year.

To help business gauge the potential impact of cyber attacks BIS publishes the annual Information Security Breaches Survey to assess the level of information security breaches affecting UK businesses and raise awareness of the need for industry to take action. The survey provides valuable insight to help guide businesses and inform Government policy. In 2014 81% of large organisations and 60% of small organisations reported a breach. Although the overall number of breaches has gone down since 2013, the reported cost and severity of those breaches has increased significantly. For small organisations the worst breaches cost between £65,000 and £115,000 on average and for large organisations between £600,000 and £1.15 million.

To ensure that businesses who have had their awareness raised and want to take action know where to turn for advice and services, GCHQ has certified firms working in Cyber Incident Response and provided guidance on Bring Your Own Device security policy. GCHQ has also been enabling industry to deliver a broader supply of assured cyber security products to defend against cyber attack through Commercial Product Assurance (CPA), for example publishing a set of security characteristics for domestic equipment required for the GB Smart Metering Programme.

In June 2014 the Government launched Publicly Available Specification 754 (PAS 754) which sets out the processes which organisations can apply to help them identify and employ trustworthy software. Sponsored by CPNI and BIS, and developed by BSI, PAS 754 is the UK's first successful attempt at codifying what constitutes good software engineering.

Information-sharing

Information-sharing between firms on threats and mitigations can help them protect themselves better. To facilitate this Government in March 2013 launched the Cyber Security Information Sharing Partnership (CISP). CISP provides a platform for companies to share cyber threat information in real time. A fusion cell (composed of industry and government network defence analysts) examines the data and provides enriched information and advice to the CISP community. CISP now has 750 organisations as members, beating the target set for 2014 by 50%, with more firms joining each week. CERT-UK, which now hosts CISP, has broadened the variety of products to include Quarterly reports, technical case-studies and added beginners guides (for example to malware) focused at a small business audience.

CERT-UK, working with police Regional Organised Crime Units (ROCUs), has also begun a nationwide initiative to introduce Regional Cyber Information Sharing Partnerships (CISP fora). These aim to promote the sharing of cyber security information regionally to help local businesses to protect themselves from cyber crime. The East Midlands region has already launched fora. On the strength of that pilot we are currently establishing a second node in the South East (which launches in early 2015) with others to follow during the year. CISP fora established in the run up to the 2014 Commonwealth Games and NATO Summit will become permanent hosts for such information sharing in Scotland and Wales.

Government's own FTSE350 Health Check and independent surveys for example by the FT and Institute of Chartered Secretaries and Administrators show that awareness among businesses, especially large firms, is rising. The July 2014 FT Bellweather survey found that 69% of company boards now actively assess their vulnerability to cyber attacks, up from 44% in July 2013.

Help for smaller businesses

However there is more to do to spread the message to harder-to-reach small firms. An updated version of the '10 Steps' guidance aimed specifically at small and medium-sized enterprises will be published in January 2015. Government continues to develop and deliver marketing and awareness activity for small businesses, including working with industry to produce a cyber action plan for small businesses. This campaign aims to change the key behaviours which will help small firms stay safe online. BIS also worked with the Guardian Media Network to raise cyber security awareness and drive positive behaviour change amongst SMEs. Over 2.5 million online adverts were delivered to the target audience directing users to information and guidance.

> "Cyber crime poses a real and growing threat for small firms and it isn't something that should be ignored. Many small businesses will be taking steps to protect themselves but many others have not recognised the increasing threat and have neither adopted technologies nor strategies to defend against cyber crime. For those that don't, the cost of cyber crime can be a barrier for growth and in the worst cases, can put a firm out of business.
>
> While we welcome action from the government and the wider public sector, there are clear actions that businesses can take to educate and help themselves to counteract cyber crime. The FSB would strongly encourage them to do so"
>
> **John Allan, National Chairman, Federation of Small Businesses (FSB)**

To help smaller firms access the help they need BIS – in partnership with Innovate UK (formerly the Technology Strategy Board) – has been offering £5,000 cyber security Innovation Vouchers to SMEs to invest in improving their cyber security and enhancing their growth potential. 375 vouchers have been awarded since July 2013 with nearly £1 million invested so far.

Incentives for adoption of good practice; the role of insurance

Meanwhile, even among larger firms, the Government judges there is more to do before managing cyber risk is truly seen as integral to good business practice. We want boards, customers and investors to be thinking about cyber security issues when they make purchasing or investment decisions. We want the market to identify and reward good practice. The aim of Government action has been to help strengthen the incentives for this, by making it easier for firms who have made the effort to make that a differentiator for them in the marketplace, and by giving customers, investors, auditors and insurers the means to make judgements about how well firms are managing their risk.

To support this, in June 2014 GCHQ, BIS and Cabinet Office launched Cyber Essentials, a major new Government-backed and industry supported scheme to incentivise widespread adoption of basic security controls that will help to protect organisations against the commonest kind of internet attacks. The scheme is constructed to be affordable and practical for all firms, small as well as large. Certification comes with a badge which firms can use to help demonstrate their security credentials to customers and investors, and which insurers can take into account when considering firms for relevant insurance policies.

The scheme has generated significant interest, with over 30,000 views of the summary and associated documents. Since the launch 124 companies have been awarded the Cyber Essentials badge including high-profile organisations such as Barclays, Vodafone and the CBI, and more are going through the process. Many more are expressing support and the desire to encourage companies in their supply chains to use it. From October 2014, possession of Cyber Essentials accreditation has been mandatory for suppliers to Government in certain categories of procurement. This, along with the 50 certification bodies now in operation, will further drive adoption and contribute to increasing take-up during 2015.

> "Increasing awareness of the cyber security threat to business is an important issue to the CBI, so we are pleased to be one of the first organisations to take part in the Cyber Essentials scheme. Business leaders will benefit from the access to helpful and authoritative cyber security guidance. Encouraging firms to adopt this scheme is a positive step towards greater awareness of cyber security and more widespread action to manage the risks"
>
> **John Cridland, Director General, Confederation of British Industry**

CYBER
ESSENTIALS

More broadly Government and the insurance industry have committed to working together to develop the UK's cyber insurance market and drive improvements in cyber security risk management. Francis Maude, Minister for the Cabinet Office, and CEOs from the UK's largest insurers agreed joint objectives and a work plan at a summit in November co-hosted with the insurance broker and risk advisor Marsh. Marsh is now leading work with the insurance sector to deliver on these commitments and will present emerging conclusions in April 2015.

Exports and prosperity

Government is determined not only to tackle the risks to businesses from cyberspace but also to seize the opportunities for exports and prosperity which should follow if the UK can cement its reputation as a leader in cyber security policy and technology.

The UK cyber security sector is already worth over £6 billion and employs around 40,000 people. In 2013 cyber security exports from the UK grew by 22% on the previous year. The UK is on track to meet the Government's target of £2 billion of cyber security exports by 2016, increasing the UK's share of a growing global market.

To ensure we deliver and if possible exceed this target, Government and industry are working together in a joint Cyber Growth Partnership (CGP). The Partnership has appointed two small business representatives to drive innovation and growth in the UK cyber security sector. One of the representatives is helping to establish regional cyber security business 'clusters'. There are now 14 such clusters established or soon to be launched across the UK, following the lead of the flourishing Malvern cluster. The other representative leads the Cyber Connect initiative which is mapping the UK cyber security sector, and supporting and championing smaller UK cyber security companies domestically and internationally. These initiatives were announced as part of a UK-US summit on cyber security which

> "Since joining the Malvern Cyber Security Cluster at its inception in 2011 we have experienced a huge increase in demand for innovative cyber security products and we now export to over 60 countries. There are now over 70 small cyber company members benefiting from our local Cluster, with 13 other Clusters springing up throughout the country. The collaboration of promotion and ideas within these Clusters helps small companies like us to thrive, and the demand for British products from across the globe pays testament to the credibility and innovation of the British cyber industry."
>
> **Ian Whiting- CEO Titania**

also launched a £4 million Technology Strategy Board competition for UK cyber businesses to develop ideas to tackle cyber security threats.

The Partnership has also launched the Cyber Security Supplier to Government Scheme. The scheme enables companies which supply cyber security products and services to the UK Government to reference this fact publicly, for example when pursuing business overseas. There are 35 UK companies currently benefitting from the scheme. Working with the FCO, the Partnership has also delivered useable export guidance for UK companies working in cyber security to ensure they can export with confidence and responsibly while avoiding any potential risks to human rights.

As well as implementing joint Government/industry export campaign plans for the UK's key target markets, and promoting the UK's cyber security 'offer' overseas and domestically, the Partnership's workplan includes an initiative to boost cyber security skills by providing mentoring and training for recent computer science graduates to help them get into the cyber security profession (see under Objective 4 for more details).

One of the strengths of the UK's offer on cyber security remains the world-leading expertise provided by GCHQ. GCHQ is working to encourage and stimulate the cyber security sector in the UK, including by working with SMEs. Unclassified contracts worth around £1m have been awarded to SMEs who had not previously worked for GCHQ, and several of these initial contracts have led to further work. GCHQ is supporting plans to build a security and defence incubator in Bristol.

UK Cyber Security Business Clusters

Established or newly forming “clusters” in:

Bath

Cambridge

Exeter

London

Kent

Malvern

North East (Tyne & Wear)

Northern Ireland (Belfast)

North West (Lancaster)

Scotland (Edinburgh)

South Wales (Cardiff)

Sussex (Brighton)

Solent (Southampton)

Thames Valley (Reading)

The Department is also working with spin-off companies formed by their own staff. GCHQ has piloted an innovation centre in Gloucestershire where staff and cleared industry partners are free to conduct research, experimentation and code development in an unclassified environment. The experiment is likely to be expanded to include uncleared SMEs and start-ups. Looking further ahead, GCHQ may explore possibilities for expanding this pilot into a national network of such centres to conduct collaborative R & D with start-ups, SMEs and developers. GCHQ will host a summit for the UK cyber security industry – IA15 - in London in December 2015 to discuss how it can continue to help support innovation and high standards among UK suppliers.

Tackling cyber crime

Tackling cyber crime so that people feel safe online continues to be a top priority.

The National Cyber Crime Unit NCCU), part of the National Crime Agency (NCA), leads operations on serious cyber crime whether it originates in the UK or internationally. With NCSP funding the Unit continues to build its own cadre of specialist officers working on cyber, and to ensure that cyber is a key strand of the NCA's other work. Programme funding is also being used to enhance the broader digital investigation skills of NCA officers. 3519 NCA Officers have completed the e-learning digital awareness e-learning course (called "The Internet and You"). GCHQ is supporting the NCCU in helping it develop the skills and technology required to combat the most sophisticated cyber crime threats to the UK.

At the regional level the NCSP has funded the police to establish dedicated cyber units in each of the nine Regional Organised Crime Units (ROCUs) across England and Wales. There are currently over 85 operations being progressed with regional and national impact.

In London, Operation FALCON (Fraud and Linked Crime Online) has brought together the Metropolitan Police's fraud squad and the cyber crime unit to disrupt and arrest cyber criminals attacking London businesses. FALCON made 117 arrests from its inception in August through to October 2014.

Training in tackling cyber crime has also been delivered to mainstream police forces. The College of Policing has designed four e-learning modules on cyber crime aimed at police officers and staff, which give an introduction to cyber, digital and social media. Since they were rolled out in 2013, over 120,000 of these modules have been completed. The College and police forces have also been delivering a classroom-based course to police investigators which gives them understanding of how to exploit intelligence and evidential opportunities offered by technology, social networking and communications data. Together these initiatives are helping train up frontline police to be able to fight crime effectively in a digital age.

International co-operation on cyber crime; disruption of criminal networks

Many cyber criminals operate from outside UK jurisdiction. With NCSP funding the NCCU has been able to increase its overseas footprint in order to understand the global cyber crime threat, co-ordinate activity against priority threats, and develop relationships with international partners that can support transborder co-operation on prosecutions, including additional posts in Europol and Interpol.

The UK Government is working more generally to build international capacity to fight cyber crime. It has worked with the Organisation of American States to develop national cyber strategies in the Caribbean which will help those countries protect themselves as well as reducing threats to the UK. The UK Government also worked with the Council of Europe (CoE) to help establish a National Cyber Crime Centre in Romania, which acts as a co-ordinating body for all CoE capacity building activity relating to cyber crime and has also led cyber crime investigations. The Centre has enabled the CoE to manage the growing number of assistance requests and is now able to support countries worldwide in their efforts to tackle cyber crime, recently including Sri Lanka and South Africa.

Meanwhile the WeProtect Summit to tackle online Child Sexual Exploitation was hosted by the Prime Minister in London in December 2014. A Global Fund to support programmes to protect children has been launched to take forward the objectives from the Summit, which are: global action to identify and protect victims; global action to remove child sexual abuse material from the internet; action to strengthen co-operation across the world to track down perpetrators; and action to build global capacity to tackle sexual exploitation of children online.

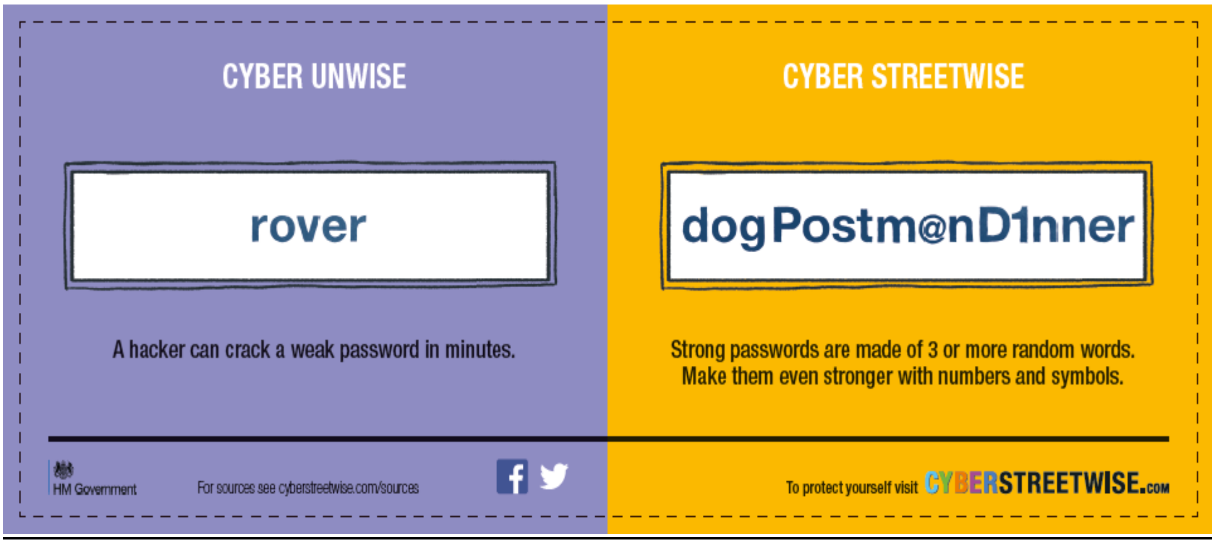
Where co-operation with other jurisdictions is difficult, or where prosecutions are not possible for other reasons, criminal activity can still be disrupted. Working with the FBI, GCHQ and other law enforcement partners as well as private industry the National Crime Agency has led for the UK on several major international operations on cyber crime. Backed by public messaging these can be highly effective in reducing UK firms' and citizens' exposure to cyber crime. For example in May 2014, the National Crime Agency (NCA) launched a major operation with international law enforcement and industry partners against two significant pieces of malware: Game Over Zeus (GOZeuS) and CryptoLocker. This resulted in over 3 million visits to HMG channels for advice on combating malware. The period from June to November 2014 showed a 70% reduction in GOZeus-infected UK computers.

Public awareness

As well as relentlessly pursuing and disrupting cyber criminals, the Government's strategy involves preventing crime through helping citizens and businesses get better protected. The Government is working to ensure that consumers are better informed of the potential risks and what they can do to reduce them, and demand better cyber security in the products and services they buy. Law enforcement has played its part in this wider effort by following up its operations with media campaigns aimed at highlighting the risks and signposting advice on responses.

Following the publication of the Internet Service Providers (ISPs) Guiding Principles in December 2013, the signatories formed a working group to co-ordinate and monitor progress made in these areas. BIS and law enforcement continue to work in partnership with ISPs to minimise and mitigate the internet cyber threats facing ISP customers. The ISPs have improved their security advice and support for customers and promoted the Government's cyber security awareness campaigns.

Cyber Streetwise launched in January 2014 with the goal of measurably improving cyber security amongst the public and small and medium sized businesses. A second phase of the campaign launched in October 2014 with a greater focus on. Since its launch it has driven over 600,000 unique visitors to the Cyber Streetwise website and the online films have attracted over 5 million views. The first phase improved take-up among more than 2 million adults of recognised cyber security activities such as using stronger passwords and checking signs for a secure website when shopping online.


CYBER UNWISE
rover
A hacker can crack a weak password in minutes.
CYBER STREETWISE
dogPostm@nD1nner
Strong passwords are made of 3 or more random words.
Make them even stronger with numbers and symbols.
HM Government
For sources see cyberstreetwise.com/sources
To protect yourself visit CYBERSTREETWISE.COM

> "Even businesses who don't sell online have much to gain by being cyber secure. Making themselves more attractive as an export and supply chain partner is a very achievable growth goal which is not open to businesses who disregard the issue of cyber security. Being a victim can severely impact a business's bottom line, but as Cyber Streetwise demonstrates, it doesn't need to cost the bottom line to implement."
>
> **Simon Whalley, Head of External Affairs at the London Chamber of Commerce and Industry**

OBJECTIVE 2: MAKING THE UK MORE RESILIENT TO CYBER ATTACK AND BETTER ABLE TO PROTECT OUR INTERESTS IN CYBERSPACE.

Detecting and defending against threats to our critical infrastructure

A significant proportion of NCSP funding has been invested in GCHQ's ability to detect and defend against the increasingly sophisticated cyber threats facing the UK. Much of this work is necessarily classified – details have been reported to the Parliamentary Intelligence & Security Committee.

The improved situational awareness this investment has delivered is being used to provide protection at pace and scale to key networks of national significance. In the coming year GCHQ will be expanding a programme to share timely and usable intelligence on hostile state and cyber crime activity with security-cleared personnel in Communications Service Providers (CSPs) so that they can use this awareness to take early action on the networks they manage and protect their customers.

Government Departments, supported by GCHQ and the Centre for the Protection of the National Infrastructure, continue to work with industry and industry regulators to ensure that the risks to the UK's critical national infrastructure are understood and that appropriate mitigations are in place.

The Secretary of State for Business hosted a 'summit of the regulators' in February 2014 to discuss the role of regulators in addressing cyber risks to the UK's critical national infrastructure. A communiqué from the summit set out the actions Government and regulators are jointly taking to ensure that our critical infrastructure remains robustly protected as threats evolve.

Resilience; the role of CERT-UK

In addition to this work on protection, the Government is also working with industry to ensure that critical services are resilient should a serious incident occur and that public authorities and infrastructure providers are ready to respond.

CERT-UK (the UK's national Computer Emergency Response Team) was launched in March 2014 and works with industry, academia and the public sector to enhance the UK's cyber resilience. CERT-UK oversees a programme of exercises to support critical sectors in preparing for the potential impact of a destructive cyber attack. It also works with other CERTs internationally to ensure the response to transborder incidents is prompt and co-ordinated and that the UK can benefit from international sharing of information on cyber security threats.

CERT-UK made an immediate impact providing information and advice on mitigation on the recently discovered Heartbleed and Shellshock vulnerabilities. CERT-UK provided information to Cyber security Information Sharing Partnership (CISP) members and issued alerts and advisories on its public website. Working with partners in industry, the police and the Scottish and Welsh Governments, CERT-UK successfully oversaw the safety of the digital infrastructure that supported the Commonwealth Games in Glasgow and the Wales NATO Summit.

Strengthening and protecting Government's systems

Meanwhile the Government continues to strengthen the protection and resilience of its own IT systems.

At the strategic level all Government department boards and the boards of key government agencies have incorporated cyber risk into their risk management regimes and report on this as part of their audited Statement of Internal Control. The National Archives' successful 'Responsible for Information' e-learning course for staff in the public sector has been completed by around 500,000 public servants and face-to-face training for more than 3600 staff has been delivered for those in critical roles.

The Government Digital Service completed the move this year of every local authority and council to the Public Services Network (PSN), the high-performance government IT network enabling secure collaboration between local authorities. The majority of central government departments and suppliers will also be moved to the PSN before the end of the financial year.

A new PSN compliance process is currently being piloted and will rolled out in 2015. It validates adherence to appropriate technical and security standards, ensuring that the PSN community can do business together safely, securely and efficiently.

Supported by National Cyber Security Programme funding, the Government Digital Service are working on GOV.UK Verify, which will be the way for members of the public to prove who they are when using digital government services. It will replace face-to-face and postal methods of verifying people's identity, so the process can be done securely online. During 2014, GOV.UK Verify has been testing the service with invited users of the HMRC's PAYE for employees service, DVLA's View Driving

Licence service and Defra’s CAP Information Service. Five identity verifiers have been appointed - Experian, Digidentity, Post Office, Verizon, and Mydex.

DWP has developed a comprehensive intelligence led cyber security capability to ensure its digital service programmes are secure. DWP and GCHQ experts continue to work together to ensure programmes are robust against interference or attempted fraud.

To ensure government finances are secure against cyber threats HMRC established a dedicated cyber security team in 2012. The team has been educating HMRC staff to identify suspicious behaviour, and deploying new technologies to enhance HMRC’s ability to identify and tackle cyber crime. The team has assisted in the prevention of fraud totalling more than £100 million this financial year.

HMRC has also deployed proactive technical measures to secure web domains that may otherwise be used by criminals to send fraudulent e-mails to customers for the purposes of delivering malware or stealing personal information. This is now in the process of being rolled out across all identified web domains. As a result, more than 94% of all fraudulent e-mails spoofing HMRC web domains are now being deleted by ISPs, preventing delivery to customers’ mailboxes. The department also takes down illegitimate phishing websites looking to steal data from taxpayers. To date this financial year, HMRC has responded to more than 75,000 phishing reports and taken down more than 4,000 illegal websites. Meanwhile HMRC provides cyber security advice to its customers on a daily basis via online guidance and Twitter – for example by raising awareness of phishing attacks using fake HMRC emails. Its cyber security pages have been viewed more than 400,000 times.

Cyber Security and Defence

The Government has continued to strengthen the cyber security of the armed forces and the military supply chain, and is mainstreaming cyber into Defence planning and operations. The Defence Cyber Protection Partnership (DCPP) was formed to improve cyber security within the defence supply chain, and continues to focus on best practice, awareness, and proportionate standards. The DCPP, which includes thirteen prime defence contractors and, representing smaller businesses, the trade associations ADS and techUK, has developed a framework that clearly identifies expected cyber standards. The Cyber Security Model for Defence will be officially implemented in 2015. Cyber Essentials is a basic building block for good cyber security practice across all organisations and as such will be an essential component of the new model. Suppliers are asked to achieve Cyber Essentials in preparation for this process.

OBJECTIVE 3: HELPING SHAPE AN OPEN, VIBRANT AND STABLE CYBERSPACE THAT SUPPORTS OPEN SOCIETIES

Cyberspace is borderless so our efforts to make the UK safer cannot focus on the UK alone. The UK's vision is for an internet that is vibrant, stable and secure while remaining open for the free flow of trade and ideas. The Government works with other countries to raise capacity, bear down on havens for cyber crime, and establish norms of responsible behaviour in cyberspace, while promoting the UK as a leader in cyber technology and policy.

Bilateral and multilateral networks

Over the coming year we will continue to expand and strengthen the UK's bilateral and multilateral networks, and to develop international collaboration through the work of the EU, NATO, the Commonwealth and other bodies. Bilateral relationships with the Republic of Korea, Israel, Singapore and Japan have been strengthened: Memoranda of Understanding were signed with the Republic of Korea and Israel in May and the Minister for the Cabinet Office further strengthened the relationship with Israel during a cyber- and digital-focused visit in November 2014; an inaugural bilateral cyber dialogue with Singapore was held in March this year; and cyber research and prosperity were key deliverables in State Visits by the Singaporean President and Japanese Prime Minister. A cyber dialogue with Japan is scheduled for later this month. to progress cyber security co-operation on the Olympics. A dialogue with India is planned for early 2015 to unlock cyber research, prosperity and security opportunities. An official dialogue and a think-tank led dialogue with China have allowed for improved bilateral understanding and engagement.

The UK successfully helped shape the EU cyber security strategy, providing a stronger basis for co-operation with other EU member states. In June 2014 the UK became a full member of the NATO Cooperative Cyber Defence Centre of Excellence. The centre, which is located in Tallinn, Estonia, is a NATO research and training facility dealing with education, consultation, lessons learned, research and development in the field of cyber security. In September 2014 the NATO Summit in Wales agreed the Enhanced NATO Policy on Cyber Defence. Concrete steps have been taken to protect NATO's own networks and make progress across the Alliance on a number of key policy priorities including prevention, detection, resilience, recovery and defence. A UK initiative for a NATO Industry Cyber Partnership (NICP) was agreed at the Summit and was highlighted in the Summit Declaration. The Declaration set out that 'technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives'.

The NCSP also funded the Commonwealth Telecommunications Organisation to develop and implement a national cyber governance model for the Commonwealth countries. Ratified this year, this is now in the process of being implemented by several Commonwealth members.

The future of cyberspace

The UK continues to help shape international debate about the future of cyberspace, including through the ‘London Process’ series of conferences on cyberspace which started in London in November 2011, and continued in Budapest in 2012 and Seoul in 2013. These have established the UK as a leading player in a broad range of cyber issues, particularly in international cyber security capacity building. The next conference will be in The Hague in April 2015 and will take this a step further and develop firm capacity building commitments from participating countries and companies. Such active engagement and profile for the UK in this debate boosts our wider economic and security objectives in cyber.

The 50th meeting of the Internet Corporation for Assigned Names and Numbers' (ICANN) was held in London in June 2014 and was well-attended, with a record-number of some 3000 participants. The UK hosted the second ever High Level Governmental Meeting during the week-long gathering and Ed Vaizey, Minister of State for Culture and the Digital Economy, made the keynote speech. The UK’s investment in this process is helping promote a model for governing the internet which remains open, accountable, transparent and secure.

Norms of behaviour

The UK Government continues to take a leading role in the development of norms of responsible state behaviour in cyberspace, in support of an open, resilient, secure and peaceful cyberspace. The UK participated in the UN Group of Governmental Experts (UNGGE) that agreed, in 2013, a consensus report making important progress in this area, in particular through the agreement that existing international law is applicable in cyberspace, and will be actively engaged in the new UNGGE that seeks to make further progress.

In addition, the UK will continue to contribute actively to discussions in the Organisation for Security and Cooperation in Europe (OSCE) on confidence building measures (CBMs) for cyberspace. OSCE participating States adopted the first regional CBMs for cyberspace in December 2013; the UK is implementing them and is engaged in discussions on developing further measures, in order to build understanding, confidence and cooperation between states.

Capacity building

The UK Government continues to work with other countries to build up their capacity and strengthen trans-border law enforcement co-operation on cyber crime. It works closely with global partners to ensure burden-sharing and effective co-operation.

Among other projects the UK co-funded the CyFy conference in India. Attended by well over 300 participants, and with speakers from over 12 countries representing government, business, academia and international organisations, the conference was India's biggest international cyber policy platform to date. The conference was successfully promoted dialogue on the future of the internet to a global audience. It also funds the Global Prosecutors E-network, which builds expertise and ability to interpret and use cyber crime legislation. The NCSP is funding selected Marshall, Chevening and Commonwealth scholars to attend a cyber policy course at Cranfield, engaging future international leaders with UK policy and positions.

The FCO continues to work with ICT4Peace to widen state participation on cyber security issues, so that countries which are not regular contributors can establish themselves on a global stage: this will broaden the debate and give countries the tools, skills and knowledge to engage at an international level. A workshop has been delivered in Latin America in conjunction with the OAS; a second workshop is planned in Africa in 2015.

The UK has also funded the Global Cyber Security Capacity Centre, part of Oxford University's Martin School. The Centre is a global thought leader in cyber security, and epitomises the best practice working model of government working with academia and industry to create the best policy. Oxford is developing the Capability Maturity Model, designed for identifying needs for capacity building, as well as developing global security capacity. A new Oxford Portal (www.sbs.ox.ac.uk/cybersecurity-capacity) will facilitate greater information exchange among researchers and consumers of research in cyber security, and act as a resource for UK and international partners.

OBJECTIVE 4: BUILDING THE UK'S CYBER SECURITY KNOWLEDGE, SKILLS AND CAPABILITY

Government's efforts to expand the UK's cyber security sector mean that more people with the right skills and education are needed to work in it. The National Cyber Security Programme has provided resources to seed initiatives across academia and the education sector to ensure we have a future workforce with cyber skills and expertise, as well as a basic understanding of cyber security among the public in general. Thanks to help from, among others, the Tech Partnership (formerly e-skills UK), Cyber Security Challenge, the British Computer Society, the Institution of Engineering and Technology and the Institute of Information Security Professionals, there are now interventions at every level of the education system from aged 11 to postgraduate.

Schools

In schools the NCSP has funded the development of cyber security learning and teaching materials at GCSE and A-level, with new Key Stage 3 (age 11-14) materials to be released to schools in 2015. This will guarantee that all schools will have access to resources to provide people leaving education with a basic understanding of cyber security before entering the workforce; it is hoped this will also motivate those with the aptitude to pursue a career in the field. In addition the NCSP has provided funding to support and accredit teacher professional development in cyber security in preparation for the recently implemented new school curriculum in computing and computer science.

Vocational training and apprenticeships

GCHQ already uses an apprenticeship scheme with success in its own business: Government is working with businesses and the Tech Partnership to help build a scheme across the wider economy and provide a new route into the sector for young people. So far these apprenticeships have helped to create nearly 200 new entry-level cyber security jobs, with more to come. Employers including CGI, Jeffries Investment Bank and Steria have recruited new cyber security apprentices for the first time. Seven training providers are developing courses to deliver the apprenticeship. In addition, the Tech Partnership has developed a new Cyber Intrusion Analyst Trailblazer Apprenticeship, providing training in this specialised and strategically important role. The first vacancies are expected in October 2015.

Government is part of a pilot scheme alongside BT, Cap Gemini, CGI and several smaller companies for a Cyber Higher Apprenticeship programme delivered by QA. A first cadre of apprentices have been recruited to work in DWP, CERT UK and HMRC. The apprentices are on a 13 week formal programme of training, which will lead to a structured pre-agreed progression route to a Foundation Degree. Subject to evaluation the scheme will be integrated into the Fast Track Apprenticeship scheme within the Civil Service in future years.

Higher education

For higher education the Government is working with academia, professional bodies, trade associations and industry to define a framework for the required learning outcomes in cyber security within computing science and related courses. From next year cyber security will be a mandatory subject of study in all undergraduate courses accredited by the British Computer Society and the Institution of Engineering & Technology.

The Higher Education Academy with BIS support and NCSP funding has provided four development fund grants totalling £153,000 for colleges and universities in Newcastle, Birmingham, London and Liverpool. The grants are to be used to create and showcase innovative approaches to improve cyber security teaching and learning in Higher Education. These are produced in partnership with companies including Barclays Bank and online retailers the Hut Group. This is the first development fund specifically aimed at supporting cyber security. Twenty applications were received from academic institutions, partnering with industry. These were reviewed by an independent panel of experts and the decision was taken to award grants to four of the applicants who showed the greatest willingness to innovate and secure industry collaboration. With NCSP funding and value-in-kind support from industry, the Cyber Growth Partnership and the Cyber Security Challenge have partnered to develop two projects aimed at providing computing graduates with the practical experience and range of business, communication and technical skills that they require, as follows:

> "It's vital for businesses and academics to share knowledge and ideas in how to generate the best research and results in cutting-edge services and products to meet rapidly changing demands. I think this initiative is a great step in this direction and we are very keen to support."
>
> **Stephen Robinson, Managing Director at Xyone Cyber Security on the new HEA grant on Cyber Security.**

- a mentoring scheme where existing cyber security professionals mentor students and recent graduates interested in a cyber career; and
- tailored 'cyber camps' for students and recent graduates, combining intensive exercises to strengthen technical, communication and business skills with the opportunity to gain an industry recognised foundation qualification.

Both will strengthen the skills of students and graduates from computing science and related disciplines, and promote career opportunities in businesses and the wider cyber security profession. This will help address the skills challenges faced by the cyber security sector, and support efforts to drive up employment rates among recent computer science graduates.

Postgraduate education

At postgraduate level GCHQ has certified six 'Master's degrees in General Cyber Security'. This work is an important first step towards recognising Academic Centres of Excellence in Cyber Security Education. Out of the 26 courses put forward from England, Scotland and Wales, six universities were judged to provide well-defined and appropriate content, delivered to the highest standard.

The Programme is also funding two Centres of Doctoral Training to provide an expanded pool of top-end skills at PhD level. The first cohort of students have entered their second year. The Centres will deliver 66 additional PhDs from 2017. In parallel GCHQ continues to expand its own PhD studentship programme with NCSP funds.

Broadening the pool of talent

NCSP funding has enabled investment in innovative initiatives to raise cyber skills and awareness and broaden the pool of available talent. A new Massive Open Online Course in cyber security, funded by the NCSP and run by the Open University, opened for registration this year. The course runs for an eight-week period, four times a year. As well as raising awareness amongst a mass audience the course aims to encourage those with an interest to take the subject further. 24,127 people enrolled for the first iteration.

Funded by the NCSP and industry sponsors, the Cyber Security Challenge runs cyber security competitions with the aim of encouraging a broader set of people to test their skills and consider a career in the field. 18,800 people have registered to take part in this year's competitions; this March, 40 finalists will compete in an ultimate set of tests co-designed by GCHQ, NCA, BT, Lockheed Martin, Juniper and Airbus.

The Challenge also runs a schools programme to introduce young people in secondary education to cyber security. Since its inception in 2013, over 800 schools have registered to take part and over 22,000 young people have used the learning resources. The Challenge has run two competitions a year for school age participants. The latest competition 'Cyber Games 3.0' was held at Warwick University on 10 December 2014.

To help teach young people about cyber security and encryption, students working on placement at GCHQ have developed a new, free-to-download app – 'Cryptoy' - that is aimed at exciting interest in cipher and coding for a new generation of cyber specialists. The app is being launched alongside publication of this report.

Cyber Security Knowledge, Skills and Capability	
Schools	Learning and teaching materials at GCSE and A-level, new Key Stage 3 (age 11-14) materials to be released in 2015; now interventions at every level of the education system
Training and apprenticeships	200 new entry-level cyber security jobs through the Tech Partnership and employers, to add to 120+ GCHQ apprentices, plus a Cyber Intrusion Analyst Trailblazer Apprenticeship in 2015
Higher Education	4 Higher Education Academies to receive NCSP teaching development grants in universities, a mentoring scheme and "Cyber Camps" for graduates and undergraduates
Postgraduates	GCHQ has certified six 'Master's degrees in General Cyber Security', plus 2 Centres of Doctoral Training to deliver 66 additional PhDs from 2017 on top of GCHQ's PhD programme
Wider educational support	Open University developed Massive Open Online Course 'Introduction to Cyber Security' – nearly 24,127 sign ups to the first offering, and a new App from GCHQ on coding, 'Cryptoy'
The Cyber Security Challenge	18,800 registered for the Masterclass competition; 800 schools participating in the Schools' competition; over 22,000 young people have used the learning resources

Cyber Reserves

As Government looks to increase its own cadre of cyber security specialists it is using innovative employment models to make sure it can tap into the right pool of talent. Recruitment for military Cyber Reserves began in October 2013 aimed at as wide a spectrum of society as possible. By adopting flexible recruitment criteria, based on talent, skills and expertise to meet cyber threats, the MOD is on track to have sufficient numbers of suitably skilled volunteers to fulfil its capability requirements by April 2016. In spring 2014 the first Cyber Reserve recruits completed their initial Single Service and Cyber induction process. The first three Cyber Reserve Induction Packages (CRIPs) have taken place. All MOD Cyber Units now have Cyber Reserves supporting them.

Professionalisation and careers

Meanwhile there are initiatives aimed at building a community of recognised, competent cyber security professionals and boosting cyber security professional training. The CESG Certified Professional (CCP) scheme sets the standard for the UK cyber security profession both in government and industry. CCP assesses candidates on how they apply their skills, knowledge and expertise in a working environment. At the end of September 2014, over 1040 cyber security professionals had been certified. This provides a firm foundation for the UK's emerging cyber security profession. There is a supporting initiative (the CESG Certified Training (CCT) scheme) to accredit high quality suppliers of training. Since launch in November 2014, eight training providers and 12 courses have been certified.

To increase awareness of cyber security careers for HE students we have funded cyber security careers resources on the Graduate Prospects careers website. A follow-on scheme from November 2014 is targeting all students with IT, engineering and STEM interests, drawing attention to current and emerging opportunities for skills development and recruitment.

The Government has also funded CREST (the Council of Registered Ethical Security Testers) to develop online resources illustrating routes towards a wide range of cyber security roles. These resources will now be brought together in a cutting-edge virtual cyber security careers hub which will showcase different cyber security careers, learning pathways, training and skills development opportunities and specific job opportunities.

The public sector at large is involved in wider initiatives to grow the pipeline of talented individuals coming into the profession. Government has invested in training its own workforce to ensure that it has better general cyber awareness and the specific cyber skills it needs, as detailed above under objective 2.

Research

Government is working to develop the community of cutting-edge cyber security research carried out in the UK. 11 UK universities now have the status of 'Academic Centres of Excellence' in recognition of the high standard of their cyber research.

Three Research Institutes founded with NCSP funds – one on the science of cyber security, one on automated programme verification, and one on trustworthy industrial control systems - are facilitating collaboration between leading researchers. Amongst other successes, researchers at University College London involved in the Research Institute on Automated Programme Analysis have developed with Google, Mozilla and others a new system which protects the privacy of users when using web applications that combine data from different websites.

The UK has also launched joint-funded research collaborations with Israel and Singapore. The call for proposals with Israel was heavily oversubscribed; the successful applications will be announced shortly. Areas of collaboration with

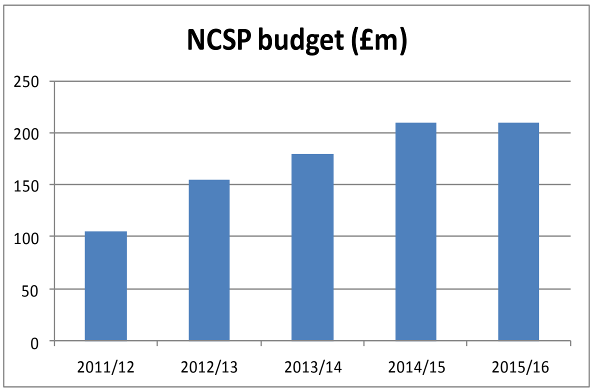
Singapore are being identified and the invitation for proposals will be issued in spring 2015.

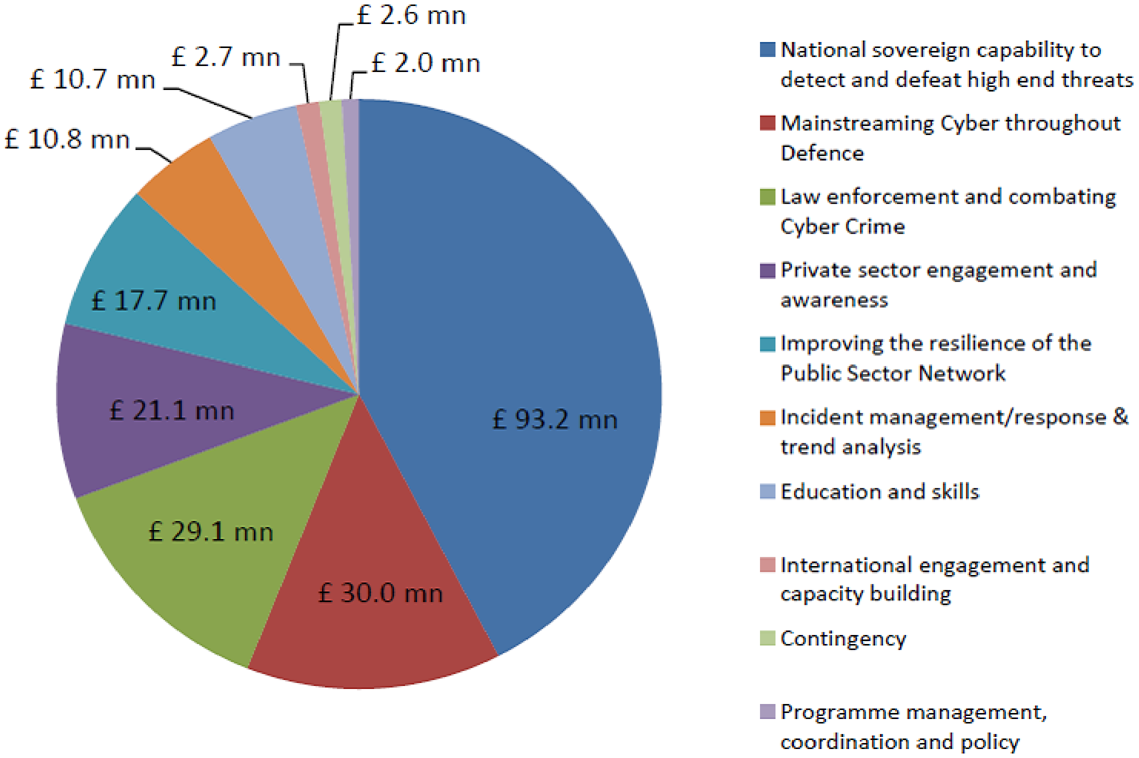
CONCLUSION

We have set out above key elements of existing and planned activity in support of the National Cyber Security Strategy. In a year's time we will again review progress against the aims and objectives of the Strategy, learning lessons and responding to new threats and challenges, with the aim of protecting UK interests in cyberspace and maintaining this country's reputation as one of the best places in the world to do business online.

NATIONAL CYBER SECURITY FUNDING

The allocation of NCSP funding for 2014/15 is set out below. These figures do not include spending in support of cyber objectives funded outside the NCSP. The chart demonstrates the spread of spend across the full range of cyber security activity. The spend on 'sovereign capabilities', not broken down here, supports activity across the Programme.


NCSP budget (£m)
2011/12
2012/13
2013/14
2014/15
2015/16


£ 2.6 mn
£ 2.7 mn
£ 2.0 mn
£ 10.7 mn
£ 10.8 mn
£ 17.7 mn
£ 21.1 mn
£ 93.2 mn
£ 29.1 mn
£ 30.0 mn
National sovereign capability to detect and defeat high end threats
Mainstreaming Cyber throughout Defence
Law enforcement and combating Cyber Crime
Private sector engagement and awareness
Improving the resilience of the Public Sector Network
Incident management/response & trend analysis
Education and skills
International engagement and capacity building
Contingency
Programme management, coordination and policy