Cabinet Office

The UK Cyber Security Strategy

Report on progress – December 2012

Forward Plans

We are at the end of the first year of meeting the objectives outlined in the National Cyber Security Strategy. A great deal has already been accomplished in our aim of making the UK one of the safest places to do business online, and delivering the four Strategy objectives:

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

The past year has seen activity across a wide range of areas and with many partners, generating increasing momentum across the Cyber Programme. Vital groundwork has been laid. Key enabling structures and capabilities have been introduced or enhanced. Plans are in place to build on these initial investments, accelerating delivery of the National Cyber Security Strategy.

This document gives an outline of these plans, which focus on: improving cyber awareness and risk management amongst UK business; bolstering cyber security research, skills and education; tackling cyber crime in order to maintain the confidence needed to do business on the Internet; further deepening our national sovereign capability to detect and defeat high-end threats; ensuring robust and resilient UK systems and networks; and helping to shape international dialogue to create and support an open, secure and vibrant cyberspace.

We will maintain this fast pace, assessing our progress and re-prioritising as necessary in response to an ever-changing technological and threat environment.

Further work to meet the objectives of the Strategy will be outlined in future reports.

Objective 1: Making the UK one of the most secure places in the world to do business in cyberspace

Working in partnership with the private sector to improve cyber security in the UK is central to our approach. The private sector drives innovation and investment in this area, but by the same token they own most of the networks which are at risk, and suffer much of the damage caused by cyber threats.

Much work has been done already in reaching out to the private sector in order to raise awareness of the threat and to encourage business to embed effective cyber security risk management practices. We will build on this in the following areas:

- We will continue to work with businesses and their representative groups and trade associations to deliver the messages set out in the Cyber Security Guidance for Business booklet that we launched in September, ensuring these messages reach the largest possible audience. As an example of this sort of outreach, a GCHQ/industry event is being held in December which explores how businesses can build the business case for investing in improving cyber security. This will involve a threat briefing from GCHQ as well as examples of successful businesses cases that have got board level buy-in on spending to improve cyber security measures.

- We will further expand the Centre for the Protection of the National Infrastructure's (CPNI) provision of bilateral cyber risk advice to reach more private companies of economic importance to the UK. Through CPNI we will also seek to build greater cyber security awareness within organisations that supply professional services to those who operate our key networks and infrastructure.

- We will also provide targeted information and advice for SMEs, including producing a version of the guidance suitable for SMEs, with supporting activity to reach out to this audience in partnership with industry and through existing channels such as Get Safe Online and Action Fraud.

- We will embed cyber security best practice requirements in future contracts for Defence and Security procurements.

- We will take forward research through CPNI's work programme with the University of Oxford, with the aim of developing advice and guidance to help reduce the risk of cyber attacks facilitated or instigated by company insiders.

As is made clear in the UK Cyber Security Strategy, awareness raising in isolation is unlikely to lead to the scale of sustained behaviour change needed to address adequately the cyber threat faced by businesses. We also need to develop and spread best practice, encourage the right market structures and provide incentives to ensure that managing cyber risk is recognised as integral to good business practice. We want

boards, customers and investors to think about cyber security issues when they are making purchasing or investment decisions. We want the market to identify and reward good practice. To this end we will:

- Work with, amongst others, the Institute of Chartered Secretaries and Administrators, the Audit Committee Institute (Audit Chairs), the Association of General Counsel, Company Secretaries of the FTSE 100, and the International Corporate Governance Network to establish cyber security as a significant business risk requiring the attention of company boards. These organisations are in a unique position to influence board room behaviour. We will work with them and other risk and audit professionals to ensure the message is getting through.

- Introduce an annual Information Security Breaches Survey from next year. Building on previous bi-annual surveys, this will provide us with an important indicator of how the private sector is responding to cyber security threats, and will allow firms to benchmark their own performance against that of their peers in order to drive up industry standards.

- Support the development of industry-led organisational standards for cyber security, to clarify what good cyber security practice looks like and to enable firms who attain such a standard to make this a differentiator in the marketplace. Government will develop and make public in early 2013 a “meta-standard”, characterising what it believes a robust organisational standard should include, and will look to endorse and support the first standard coming to market which meets these criteria.

- Extend ‘kite marking’ of cyber security products and services to stimulate the market by guiding potential purchasers to those that have been assessed by Government to meet rigorous standards. This activity will build on the Cyber Incident Response pilot launched by CESG and CPNI in November, which accredited four companies as reaching the required standards to provide certain cyber security services. We hope to develop this to become a sustainable scheme covering the full cyber incident lifecycle (identify, respond and improve). Key to this will be helping to nurture and grow industry capability in this space so more companies can join the scheme.

- Alongside this, we will also draw on Government’s own procurement expertise to provide information for businesses on issues to consider when moving data and services to the Cloud, so that they can make better-informed decisions on how to do this securely.

- GCHQ will also promote and develop its Commercial Product Assurance scheme, which gives institutions confidence that the security features of the products they buy to manage their cyber risks are effective. The first product assured under the scheme has already saved HMRC £2.4m. To manage information risks in the digital age, Government will be making much greater use of exactly these sorts of commercially assured products in future. To this end, we are reshaping and modernising some of our information security and classification policies to provide for this.

Greater awareness of cyber risks and better understanding of how to manage them will create significant opportunities for the UK cyber security sector. To ensure that business can take advantage of these, we will:

- Launch a 'Cyber Growth Partnership', in conjunction with Intellect UK (which represents the UK technology industry and has over 850 members). Central to this will be a high level group which will identify how to support the growth of the UK Cyber security industry, with an emphasis on increasing exports.

- Increase the proportion of Government cyber security contracts going to SMEs. In line with Government targets, at least 25% of GCHQ's procurement budget is to be spent through SMEs to gain access to the vibrant innovation of these firms. GCHQ will provide advice and information to encourage and support them in adopting appropriate standards to protect government information.

- Encourage innovative cyber security solutions. As part of Government's commitment to support smaller firms, GCHQ and other Government agencies launched the 'Finding the Threat' call to SMEs for innovative ideas to a set of security and intelligence challenges. The launch event attracted over 500 attendees, over half of whom were new to the sector. This was the most successful call of its kind ever held which indicates the level of interest in this market.

Cyber crime continues to grow and has the potential to undermine confidence in the Internet, both in the UK and internationally. To ensure the UK is a safe environment in which people and industry feel secure to do business on the internet, it is essential that the law enforcement community, supported by the intelligence agencies, has the ability, skills and resources to respond. They will continue to work with business, and will engage international law enforcement partners to identify, prevent, disrupt and investigate cyber crime. Our priorities in the coming months are to:

- Establish the National Cyber Crime Unit (NCCU) as an integral part of the new National Crime Agency. Bringing together the existing national law enforcement capabilities on cyber in one place will deliver a substantial enhancement to our ability to counter cyber crime. The National Crime Agency will be in place by October 2013, and we will expand joint SOCA Cyber and Police Central eCrime Unit operations before then, ensuring that the lessons learned from these inform the development of the NCCU.

- Continue to build better information sharing mechanisms between law enforcement and industry, including through the UK Cyber Information Sharing Partnership (see below), improving our capability to share information on cyber crime threats in real time.

- Further strengthen specialist law enforcement and prosecutors' skills and increase mainstream law enforcement awareness of, and capability to tackle, cyber crime.

- Build on co-operation between the UK and international law enforcement agencies, including more joint operations.

- Launch an enhanced reporting tool for Action Fraud, as the UK's central reporting hub for cyber fraud, which will make it easier for businesses to report repeat cases.

Objective 2: Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace

A significant proportion of the first year's Programme funds has been invested in strengthening GCHQ's ability to detect cyber attacks on UK interests. This has transformed our situational awareness in cyberspace. The next phase of investment will see GCHQ further increasing its ability to respond to the threat, to protect the UK's national and economic security interests.

The Government will also take steps to increase the security of its own computer networks with the next phase of projects delivered to ensure the security of information across public services via the PSN (Public Sector Network).

Learning from the processes developed for and tested at the Olympics, we will strengthen the protection and resilience of the UK to cyber attack, improving our ability to respond to cyber attacks on both public- and privately-owned critical national infrastructure. London 2012 was the first truly digital games. Throughout the Games, Government worked hand in hand with private sector to combat/handle cyber threats. The Olympics provided a genuine test of our preparedness with potential threats successfully averted. We are building on the lessons learned in streamlining and improving incident response for future potential events. We plan to:

- In partnership with industry, move to establish a UK national CERT (Computer Emergency Response Team). This will build on and complement existing structures in Government to improve national co-ordination on incident response and provide a focal point for international sharing of technical information on cyber security.

- Following the successful information sharing pilot between government and businesses on cyber incidents, develop a permanent information sharing environment called CISP (Cyber Information Sharing Partnership) to be launched in January 2013. Initially, this will be open to companies within Critical National Infrastructure sectors, but we intend to make membership available more broadly, including to SMEs, in a second phase.

- Expand the Cyber Incident Response pilot launched by CESG and CPNI in November, which accredited four companies as reaching the required standard to provide certain cyber security services. Developing this pilot into a market-supporting tool will be a key goal of the Cyber Growth Partnership with industry.

- Work closely with key allies and like-minded partner countries on the development of cyber security policy, co-ordinating domestic action where we can to bring mutual enhancements to national security.

Objective 3: Helping shape an open, vibrant and stable cyberspace that supports open societies

The nature of the internet means that we cannot focus our efforts on the UK alone. International co-operation is crucial. Cyberspace knows no borders. Our overall priority is to promote the UK's vision of an open, vibrant, stable and secure cyberspace. This will help ensure that the economic and social benefits of cyberspace are protected and available for all. To do this we are working in partnership with other nations and organisations to help shape norms of behaviour for cyberspace while promoting the UK as a leader in cyberspace technology and policy. We will:

- continue to expand and strengthen the UK's bilateral and multilateral networks, and to develop international collaboration through the work of EU, NATO and other bodies.

- seize key opportunities in the year ahead to help safeguard the free and open future of the Internet and develop 'rules of the road' for cyberspace. These opportunities will include the Seoul Cyber Conference, the report of the UN Group of Government Experts on international security norms, OSCE (Organisation for Security and Co-operation in Europe) work on Confidence Building Measures and discussions on internet governance in the lead-up to the World Summit on the Information Society (WSIS). We will also play an active role in discussions on the new EU cyber Strategy.

- continue to work for transborder law enforcement co-operation on cyber crime. With more countries intending to sign up to the Budapest Convention on Cyber Crime in the coming year, UK law enforcement agencies will continue to expand partnership building and joint operations.

- work with other countries to build up their capacity to tackle cyber threats and bear down on safe havens for cyber criminals, including through the new Global Centre for Cyber Security Capacity Building announced by the Foreign Secretary in October 2012.

Objective 4: Building the UK's cyber security knowledge, skills and capability

Improving cyber security skills to meet increased demand for professionals in this area is critical if we are to maximise the business opportunities of the networked world and keep the UK at the forefront of innovation. We are making interventions across the education system to develop the skills at an early stage in the education of children and young people; and to ensure that we can develop the specialism that we need through our university system. Alongside this, we are actively encouraging the development of apprenticeship routes into security work and the cyber security profession. We are doing this through initiatives such as:

- Ensuring that all graduate software engineers have had adequate training in cyber security. We have partnered with the Institution of Engineering and Technology (IET) to support and fund the Trustworthy Software Initiative which aims to improve cyber security by making software more secure, dependable and reliable. As part of the initiative a module has been developed to educate students doing technical degree courses on the importance of trustworthy software. This material is currently being piloted at De Montfort

University, the University of Worcester and Queens University Belfast. The IET plans to expand the pilot next spring, with the objective of making this a mandatory component of Engineering Degrees accredited by the Institution by 2015.

- Creating two Centres of Doctoral Training. The Centres will call on a wide range of expertise to deliver multidisciplinary training and so help to provide the breadth of skills needed to underpin the work of the UK's next generation of doctoral-level cyber security experts. The two CDTs will deliver in total a minimum of 48 PhDs over their lifetime with the first cohort of students starting in October 2013. These are in addition to 30 GCHQ PhD Studentships also sponsored by the National Cyber Security Programme.

- Continuing to support Cyber Security Challenge UK which uses innovative approaches to recruit new and young talent into the cyber security field. Since its launch in 2010, they have had more than 10,000 registrations and received support from over 50 industry sponsors. In 2013, the initiative will introduce a new series of competitions for schools in partnership with universities and businesses.

- Actively identifying and developing talent in school and university age students. Within Government GCHQ and the other Intelligence Agencies will recruit up to 100 apprentices to be enrolled on a tailored two-year Foundation Degree course. We will work with industry to encourage firms to build up their own apprenticeship schemes.

To fill skills gaps now, as well as increasing the pipeline of future talent we also need to make it easier for people to move into this field in mid-career. To this end we are working with skills bodies to identify other professional formation routes and training opportunities. We are also:

- Moving forward with a programme to recruit 'Cyber Reservists' to the MoD. The Services will engage additional experts to support their work in defending against the growth in cyber threats. These will be supporting roles to the Joint Cyber Units across the full spectrum of cyber and information assurance capability. A series of events are being held with industry on how the scheme will work. A further announcement will be made spring 2013.

- Putting in place a scheme to certify cyber security training courses as part of the ongoing development of certification and professionalism in cyber security.

Underpinning this we are working with a range of partners across industry and academia to boost cyber security research in the UK and ensure we can continue to call on cutting edge ideas in this field. We are investing in the best UK cyber expertise to lead thought and strengthen capability, keeping the UK at the forefront of international research in in this strategically important area. To this end, we will:

- Extend the Academic Centres of Excellence in Cyber Security Research programme. The first eight[1] UK universities conducting world class research in the field of cyber security have been awarded "Academic Centre of Excellence in Cyber Security Research" status by GCHQ in partnership with the Engineering and Physical Sciences Research Council (EPSRC) and the Department for Business Innovation and Skills (BIS). The Centres of Excellence will benefit the UK by enhancing the UK's cyber knowledge base through original research; providing top quality graduates in the field of cyber security; supporting GCHQ's cyber defence mission; and driving up the level of innovation. A second call for applicants will close shortly, with the assessment scheduled for early in 2013.

- Establish a second Research Institute to look at Automated Program Analysis and Verification in spring 2013. The first Institute was formed at University College London in October 2012 and covers seven UK universities drawing on social scientists, mathematicians and computer scientists to develop the Science of Cyber Security.

- Launch a new multidisciplinary Academic Cyber Journal in 2013. This will provide a platform for publishing a broad range of cyber security research from both UK and international universities, fuelling innovation and growth in cyber security and other sectors.

We must also ensure that consumers are better informed of the potential risks and what they can do to protect themselves online. This is important not only in protecting people from online fraud and other crimes but also to ensure that people's unprotected home computers are not compromised to pose a threat to other systems and networks.

Much work has already happened including the National Fraud Authority's Devil in Your Details campaign on online fraud and the 2012 Get Safe Online Week. Going forward we will be extending this work in partnership with the private sector, to maximise the potential reach for messages and information:

- Government will be mainstreaming cyber security messages across the breadth of its communication with the citizen. For example, HMRC will be automatically alerting customers using out of date browsers and directing them to advice on the threat this might pose to their online security.

- From spring 2013 we will be rolling out a programme of public awareness drives, building on the work of GetSafeOnline.org and the National Fraud Authority. This programme will be delivered in partnership with the private sector and will aim at increasing cyber confidence and measurably improving the online safety of consumers and SMEs. We are working now to understand the online behaviour of different segments of consumers in order to prepare the ground for these campaigns and to ensure what we do is based on evidence on what works.

[1] University of Bristol, Lancaster University, Queen's University Belfast, University of Southampton, Imperial College London, University of Oxford, Royal Holloway University of London, University College London.

- To measure progress we will put in place a “Cyber Confidence tracker”, which will regularly track online safety perceptions and behaviours, providing both a benchmark and measurement of success for all awareness and behaviour change activities. This will inform the further development of campaign work to support awareness activity. The first tracking will have taken place by March 2013.

We have set out above key elements of our planned activity over the next 12 months in support of the National Cyber Security Strategy. We will regularly 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 making this country one of the best places in the world to do business online.