WRITTEN MINISTERIAL STATEMENT

CABINET OFFICE

3RD DECEMBER 2012

Minister for the Cabinet Office and Paymaster General: Progress on the UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World

---

On 25th November 2011, I published the UK Cyber Security Strategy. In the Strategy I committed to report back on progress after one year, in particular on the achievements of the National Cyber Security Programme for which my department has oversight. I am pleased to present this report to both Houses today.

The Strategy outlined how the Internet has changed and shaped our lives. A year on from its publication, this transformation continues at pace.

The UK has been proclaimed as the 'most internet-based major economy', with one recent study stating that the UK's Internet-related market is now worth £82 billion a year and rising[1]. The Internet provides a rich and fertile basis for industry, and small businesses in particular, to expand and grow.

However, as was pointed out in the Strategy last year, there exist real and growing threats to our interests in cyberspace; these threats have increased concurrently with the growth of the 'Internet economy'

Industry suffers at the hands of such threats. The 2012 PwC Information Security Breaches Survey found that 93% of large corporations and 76% of small businesses had a cyber security breach in the past year. With the cost for a security breach estimated between £110,000-250,000 for large businesses and £15,000-30,000 for smaller ones, these are losses which UK businesses can ill afford.

[1] AT Kearney: The Internet Economy in the United Kingdom

And we are not immune in Government. Attacks on government departments continue to increase.

The UK Cyber Security Strategy sets out our approach to tackling the threat. It clearly states four objectives for the UK:

- To tackle cyber crime and to be one of the most secure places in the world to do business in cyber space
- To be more resilient to cyber attacks and better able to protect our interests in cyberspace
- To have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies
- To have the cross-cutting knowledge, skills and capabilities the UK needs to underpin these other objectives.

These objectives are delivered through the National Cyber Security Programme which prioritises and co-ordinates work across Government and provides £650 million of new funding to improve the UK's cyber security capability.

We are making good progress against these objectives and I am pleased to be able to report on some notable achievements.

Combating the threats

Firstly, I would like to point to the work of GCHQ in addressing cyber threats. Its work underpins our ability to contend with the many challenges of the cyber age that threaten our national security. We have invested in new and unique capabilities for GCHQ to identify and analyse hostile cyber attacks in order to protect our core networks and services and support the UK's wider cyber security mission. I cannot reveal details of this work, but it has broadened and deepened our understanding of the threat, helping us prioritise and direct defensive efforts.

As part of this work, the MOD has established a tri-service Unit, hosted by GCHQ in Cheltenham. The Joint Cyber Unit training and skills requirements have been established and it is currently developing new tactics, techniques and plans to deliver military capabilities to confront high-end threats.

The Security Service has developed and enhanced its cyber structures, focusing on investigating cyber threats from hostile foreign intelligence agencies and terrorists, and working with UK victims. This informs the work of the Centre for the Protection of National Infrastructure (CPNI) which is helping organisations to improve their cyber security measures.

CPNI is actively influencing standards, researching vulnerabilities and focusing on the key technologies and systems of cyber infrastructure. As part of this work it has commissioned a major research programme from the University of Oxford with the aim of delivering advice,

guidance and products to help reduce the risk of cyber attacks mounted or facilitated with the help of company insiders.

In terms of protecting core Government systems, work is being done across the Public Sector Network to create a new security model for the sharing of services. This includes: a common and standardised approach to assurance - Single Sign-on - through an employee authentication hub; security monitoring; more effective policing of compliance; and greater network resilience.

2012 saw the UK hosting one of one the greatest sporting events of our time. The London Olympics was the first truly digital Games and, as such, we recognised the need to address potential cyber threats. We established unprecedented mechanisms for working hand in hand with sponsors and suppliers to the Games in combating and managing incidents. The lessons learned from the event are informing our cyber security national incident management plans as we go forward.

Tackling cyber crime

The Government has invested in strengthening law enforcement and prosecutors' capabilities to prevent, disrupt and investigate cyber crimes and bring those responsible to justice. The Police Central e-Crime Unit has trebled in size, three regional cyber policing teams have been established, and training on cyber crime for mainstream police officers has been designed. This is increasing the capacity of the police to tackle cyber crime in line with the Strategic Policing Requirement which was issued by the Home Secretary in July 2012. The Serious Organised Crime Agency (SOCA) has increased its cyber capability including the introduction of cyber overseas liaison officers and a number of posts dedicated to mainstreaming cyber and digital investigations across the organisation.

The Police Central e-Crime Unit has reported that it has exceeded its four year operations performance target of averting £504 million of harm within the first year of the National Cyber Security Programme alone – preventing £538 million of harm at a return on investment of £72 harm averted for every pound invested. In addition and in conjunction with partners, SOCA has repatriated over 2.3 million items of compromised data to the financial sector in the UK and internationally since November 2011 with an estimated prevention of potential economic loss of over £500 million. In addition, The Crown Prosecution Service in turn is devoting more resources to prosecuting cyber crime. As at the end of September 2012, the Department was prosecuting 29 'live' cyber crime cases.

Joint operations between the two units have now been initiated as a first step towards their coming together in 2013 to form the National Cyber Crime Unit of the new National Crime Agency. This will deliver the next step in transforming law enforcement capability to tackle cyber and cyber-enabled crimes.

National Cyber Security Programme funding has enhanced Action Fraud to be the UK's national reporting centre for fraud and financial internet crime, operating on a 24/7 basis. This enables reported incidents of crime to be developed into intelligence packages that national and local

agencies can use for targeted enforcement activity. Over 12 months, Action Fraud received 46,000 reports from the public of cyber-enabled crimes amounting to attempted levels of fraud of £292 million.

To further assist in tackling online fraud, HMRC has established a new Cyber Crime Team to enhance the Department's capability to tackle tax fraud by organised criminals. HMRC's enhanced anti phishing capabilities are now leading to the interception of five major threats a day and have helped the Department to shut down almost 1000 fraudulent web sites in the last 12 months.

Partnership with industry

Government cannot do this alone. We know that industry is the biggest victim of cyber crime and intellectual property theft through cyber crime is happening on an industrial scale. In the past year we have cast our net wide to work with industry, academia and ever wider across the public sector to promote awareness of the need to address cyber threats. We have produced and promoted a 'Cyber Security Guidance for Business' document for industry Chief Executives, which sets out how board members and senior executives should adopt a holistic risk management approach to cyber security in order to safeguard their most valuable assets, such as personal data, online services and intellectual property.

We have successfully completed a pilot government and industry information sharing initiative to provide a trusted environment for organisations to share information on current threats and managing incidents. This included around 160 companies across five sectors: Defence, Finance, Pharmaceuticals, Energy and Telecommunications. Although industry to government and government to industry information exchange worked well, most value was gained through the industry to industry engagement and this is informing how we take this work forward.

Education, skills and awareness

We have been actively raising awareness among industry and the public about the problem so that people take the simple steps to protect themselves and demand better cyber security in products and services. Working with industry, we have been raising awareness of cyber security threats amongst the general public through initiatives such as the recent Get Safe Online Week, which for the first time ran in conjunction with the EU and US and Canadian partners, as part of a drive to establish a global Cyber Security Month in October each year. The National Fraud Authority has also delivered targeted campaigns on online fraud, reminding people of the increasing threat of cyber crime. Over 4 million individuals were reached by the *Devils in Your Details* campaign in spring 2012. In evaluation afterwards two-thirds of those surveyed said they would change their behaviour as a consequence.

We are investing in skills and research so that we have the capability to keep pace with this problem in the future. The first eight UK universities conducting world class research in the field of cyber security have been awarded "Academic Centre of Excellence in Cyber Security Research" through the Engineering and Physical Sciences Research Council. In addition, a

new virtual Research Institute has been launched as a government/academia partnership. Its aim is to improve understanding of the science behind the growing cyber security threat. These initiatives help keep the UK at the forefront of international research in this field.

Meanwhile we have taken steps to improve cyber security skills among young people and to widen the pipeline of talent coming into this field. BIS has commissioned e-Skills UK to develop interactive learning materials on cyber security for GCSE students. One hundred and twenty schools have already signed up to use the materials as part of the Behind the Screen initiative. In November, GCHQ and the other Intelligence Agencies launched a new technical apprenticeship scheme which aims to identify and develop talent in school and university age students. They aim to recruit up to 100 apprentices who will be enrolled on a tailored two-year Foundation Degree course. We have also sponsored the Cyber Security Challenge UK in its work providing advice, support and guidance for anyone interested in a career in cyber security, and to create opportunities for employers and previously unidentified talent to come together. Since its launch in 2010, over 10,000 people have registered with the initiative.

Ensuring that those in the field of cyber security get the right training and education, GCHQ has established and is building on a set of certification schemes to improve the skills and availability of cyber security professionals. The Certification for Information Assurance Professionals scheme will help Government and Industry to recruit cyber security professionals with the right skills at the right level to the right jobs. It will also assist participants to build a career path and to have the opportunity to progress through re-assessment as skills and experience grow.

International efforts

The nature of the Internet means that we cannot focus our efforts on the UK alone. International co-operation is crucial. We have continued to promote the UK's vision of an open, vibrant and secure cyberspace internationally, for instance through our active contribution to the Budapest Cyber Conference, and to build up a wide network of international partnerships. We have strengthened relationships with traditional allies and have initiated discussions with a broad range of countries. We are also working with international partners to improve co-operation to tackle cyber crime through legislation and operational work, and have played a prominent role in international discussions on norms of behaviour and Confidence Building Measures in cyberspace. In October, the Foreign Secretary announced the establishment of a Cyber Capacity Building Fund for supporting cyber security internationally, part of which will create a new Global Centre for Cyber Security Capacity Building. This Centre will help to make UK expertise and technology in this field available to international partners.

Reflecting the global nature of the cyber crime threat, UK law enforcement agencies continue to work closely with their international partners, through partnership building and joint operations. SOCA continues to lead, with international partners, on the global representation of law enforcement interests to ICANN, the Internet domain name organisation. Collaboration with ICANN to amend the registrar's Accreditation Agreement has assisted law enforcement in crime prevention and detection. In April 2012, SOCA led a global day of action to tackle Automated

Vending Cart websites selling compromised financial data. Two arrests were made in the UK and seventy websites taken down world-wide, resulting in major disruption to organised crime groups' activities.

A fuller list of achievements from the first year of the Cyber Security Strategy and work on the National Cyber Security Programme can be found at www.cabinetoffice.gov.uk

Future plans

Looking forward, we are clear that there is still much work to do. We will continue the work that is underway, while regularly assessing it against priorities, and taking into account new and emerging threats.

We are reviewing our national approach to cyber incident management, particularly in the light of the successful Olympics response outlined above. Our intention is to move towards the establishment of a UK National CERT (Computer Emergency Response Team). This will build on and complement our existing CERT structures, improve national co-ordination of cyber incidents and act as a focus point for international sharing of technical information on cyber security.

In addition, a new Cyber Incident Response scheme, recently launched by CESG and CPNI in pilot form, will move to become fully operational in 2013. It is an HMG quality-assured service, provided by industry, that organisations can turn to for assistance when they have suffered a cyber security incident. The scheme will enable the UK's emerging cyber response industry to grow, bringing further benefit to the UK in terms of skills and business opportunities.

Working with the private sector to improve awareness of the need for better cyber security continues to be a priority. We are now focussing our efforts on making sure that the right incentives and structures are in place to change behaviour in a sustainable way. Government departments and agencies are working with professional and representative bodies to ensure the consideration of cyber security becomes an integral part of corporate governance and risk management processes. We are supporting the development of organisational standards for cyber security so consumers can identify those businesses with good cyber security practices.

Building on the successful 'Auburn' pilot project between government and businesses, we are developing a permanent information sharing environment called CISP (Cyber-security Information Sharing Partnership) to be launched in January 2013. This has been a joint industry/government design. 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.

We are constantly examining new ways to harness and attract the talents of the cyber security specialists that are needed for critical areas of work. To this end, the MOD is taking forward the development of a 'Cyber Reserve', allowing the Services to draw on the wider talent and skills of the nation in the cyber field. The exact composition is currently in development and a detailed announcement will follow in 2013.

On cyber crime, the Government will continue to work with the law enforcement community to enhance their capabilities, particularly through the creation of the National Cyber Crime Unit (NCCU), an integral part of the National Crime Agency which, subject to parliamentary approval, will be established in October 2013. The NCCU will bring together the capabilities of the Police Central e-Crime Unit and SOCA's cyber team to create an even more effective response to the most serious cyber criminals.

Alongside tackling the threat the Government is determined to help seize the business opportunity in cyber, promoting the UK cyber security industry both domestically and across the globe. To support this, we are today forging a new joint 'Cyber Growth Partnership' with Intellect, the organisation which represents the UK technology industry. 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.

To ensure the UK can continue to call on cutting-edge skills and research BIS and the Engineering and Physical Sciences Research Council (EPSRC) will fund two Centres of Doctoral Training (CDT). The Centres will call on a wide range of expertise to deliver multidisciplinary research 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.

We are also building cyber security into undergraduate university degrees. 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 on technical degree courses on why trustworthy software is important. 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; from 2015 education in cyber security will be a mandatory component of software engineering degrees accredited by the Institution.

On the international front, we will continue to expand and strengthen the UK's bilateral and multilateral networks. Key opportunities to shape the future of cyberspace in the year ahead 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.

Public awareness will be a priority: we need to warn people of the risks and what they can do to protect themselves while ensuring that confidence in the Internet is maintained. 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.

Meanwhile 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.

Conclusion

Further details on forward plans are available at www.cabinetoffice.gov.uk

One year after the Strategy's publication a great deal has already been accomplished in our aim of protecting UK interests in cyberspace and making the UK one of the safest places to do business online. This is not an issue for Government alone. Industry has the potential to lose the most by not rising to these challenges so together we must work to address cyber threats which could undermine our economic growth and prosperity.

The past year has created an increasing momentum across the UK at varying levels and across all sectors in addressing a wide range of cyber security threats. We look forward to maintaining this pace, continually assessing our progress as we go forward. I will report back on progress again a year from now.