GOV.UK

1. Home (https://www.gov.uk/)

Written statement to Parliament

UK Cyber Security Strategy: statement on progress 2 years on

Francis Maude delivered this written ministerial statement on progress against the objectives set out in the UK Cyber Security Strategy.

Published 12 December 2013
Last updated 12 December 2013 — see all updates

From:
Cabinet Office (https://www.gov.uk/government/organisations/cabinet-office) and The Rt Hon Lord Maude of Horsham (https://www.gov.uk/government/people/francis-maude)

This was published under the 2010 to 2015 Conservative and Liberal Democrat coalition government

Delivered on:
12 December 2013

Last December, I placed the first of my annual reports before Parliament on progress on the UK Cyber Security Strategy. I am pleased to present a second report to both Houses today.

The Cyber Security Strategy (https://www.gov.uk/government/publications/cyber-security-strategy), published in November 2011, set out the government's vision of "a vibrant, resilient and secure cyberspace", providing a framework to guide our actions to "enhance prosperity, national security and a strong society".

Read about our achievements and our plan for the future. (https://www.gov.uk/government/publications/national-cyber-security-strategy-2-years-on)

To support the Strategy we put in place a National Cyber Security Programme (NCSP) backed by £650 million of funding to 2015. This year we increased that investment with a further £210 million in 2015 to 2016. This funding will build on existing projects and also support new investment, enabling the UK to retain its emerging reputation as a leader in the field of cyber security.

The strategy set out 4 clear 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

These objectives continue to drive our work and are as relevant today as they were in 2011 even in the face of a rapidly changing technological and threat landscape. In this report, I will highlight significant areas of progress, new announcements and our forward plans.

Making cyberspace safer for UK business

Our partnership with industry continues to advance and bear fruit to mutual benefit. In March this year, I launched the Cyber Security Information Sharing Partnership (CISP) which we funded through the NCSP. It provides a trusted platform in which the security services, law enforcement authorities and industry exchange information on threats and mitigations in real time. The partnership already includes more than 250 companies. In November this year, the CISP supported the financial sector's 'Waking Shark II' exercise in conjunction with the Bank of England which tested the financial sector's ability to respond to a cyber attack. Going forward, we plan to expand its partnership by doubling the number of members to 500 by the end of 2014.

The Department for Business, Innovation and Skills (BIS) has also worked with partners to deliver a 'Cyber Governance Health Check' for FTSE350 companies and cyber security guidance for small businesses, both of which help companies to identify and tackle cyber risks. In addition, they have also been working closely with industry to develop an agreed 'Organisational Standard'.

Last month, the Minister of State for Universities and Science announced details of this new standard which will not only give companies a clear baseline to aim for in addressing cyber security risks to their company but will enable them to advertise the fact that they meet a certain set of criteria on cyber security. This provides them with an obvious competitive advantage in a marketplace that increasingly demands better cyber security from suppliers. To reinforce this and give the standard a kick-start, we will be mandating its use in government procurement. Its adoption will be subject to proportionality and relevance, particularly in relation to SMEs, as this is not designed to impose costs on business but rather to boost cyber security while improving the security of the government's supply chain.

In concert with this, BIS has developed a new Cyber Security Suppliers Scheme as part of the work being done in conjunction with techUK and the cyber security sector through the new Cyber Growth Partnership. The scheme provides UK companies with a means of demonstrating, via a public list, that they are a supplier of cyber security products and services to the UK government. We want to help UK companies capitalise on a growing market in cyber security products and services, and we are setting a target for future export growth. The target, the first of its kind, has been set at £2 billion worth of annual cyber sales by 2016, a significant increase on the 2012 export sales figure of £850 million.

Tackling cyber crime

The launch of the National Crime Agency (NCA) in October saw the establishment of the new National Cyber Crime Unit (NCCU). The NCCU brings together the skills and expertise of its precursors, SOCA Cyber and the Police Central e-Crime Unit, into a world-leading organisation dedicated to fighting the most serious cyber criminals.

The NCCU has already had significant successes. Just in the past month, it issued an urgent alert to inform internet users of a risk of infection linked to a mass email spamming event aimed at millions of consumers. In addition, NCCU delivered a quick response to a threat to a bank that enabled security measures to be put in place and prevented approximately £14 million from potentially being extracted from accounts. Working closely with the Metropolitan Police, 6 suspects were also sentenced to a total of 28.5 years after being convicted of stealing thousands of pounds from job hunters using fake online adverts for companies. The group defrauded UK financial institutions for many years and stole personal data from thousands of members of the public. We look forward to the NCA developing its capabilities further over the coming year to provide a relentless law enforcement response to cyber crime.

Meanwhile government departments have also taken action to prevent cyber fraud. A dedicated Cyber Crime Capability in HMRC has provided specialist advice to approximately 20 criminal cases, resulting in an overall Revenue Loss Prevented of more than £40 million and more than 2,300 fraudulent websites have been shut down since January 2011.

Making the UK more resilient in cyberspace

Improving our resilience to and diminishing the impact of cyber attacks is vital. Much of our national infrastructure is owned and operated by the private sector and over the past year, the Centre for the Protection of the National Infrastructure (CPNI) has further extended its range of guidance and products to help companies protect their networks from cyber threats. CPNI's Cyber Risk Advisory Service provides in-depth support to senior executives and boards of the UK's most critical firms.

The safety of industrial control systems is an important element of infrastructure protection. Helping build our capability in this important area, in conjunction with the EPSRC, we are establishing a new Research Institute in Trustworthy Industrial Control Systems. This is the third such Institute to be established with the aid of NCSP funding. Based at Imperial College, the Institute will broaden our understanding of the threats to these control systems and find ways to enhance their security.

The MoD continues to mainstream cyber throughout our defence forces. In May this year, the MoD stood up Joint Forces Cyber Group to deliver Defence's cyber capability. The group includes the Joint Cyber Units (JCUs) at Cheltenham and Corsham, with the new Joint Cyber Unit (Reserve) which we announced last year. Recruitment for the Joint Cyber Unit (Reserve) commenced in October 2013 with a high number of applications received following the Defence Secretary's announcement in September 2013. The MoD continues to develop new tactics, techniques and plans to delivery military capabilities to confront high-end threats.

An open and secure cyberspace

Complementing these domestic efforts, we have been pursuing an international agenda for an open, stable and secure cyberspace, as set out by the Foreign Secretary at the London Cyber Conference in 2011 (https://www.gov.uk/government/news/foreign-secretary-to-host-london-conference-on-cyberspace-1-2-november). This has been advanced through subsequent conferences in Budapest in 2012 and Seoul this October, where over 85 countries were represented. In Seoul, we succeeded in getting agreement on a clear statement of the importance of maintaining an open Internet for economic progress.

We are working in partnership with a whole host of nations and organisations including the G8, the UN, NATO, and the EU to help shape norms of behaviour for cyberspace whilst promoting the UK as a leader in cyberspace technology and policy. And we are investing in capacity and cooperation internationally by establishing a Cyber Capacity Building Fund. Through this we have supported the creation of the Global Cyber Security Capacity Centre at Oxford University this year. The Fund is already helping the UK to tackle cyber threats at source, with the arrest in June 2013 of a major Global e-fraud network following UK training of partners in South East Asia.

Cyber security is a long term project, so we are investing for the future with a new engagement process in which Chevening, Commonwealth and Marshall scholars from Africa, Asia, and America by selecting a number of these students to attend the annual Academic Centres of Excellence in Cyber Research Conference in December and to enrol in an international cyber policy course at Cranfield University. Through this initiative, we aim to help ensure that future cadres of global leaders will have a good understanding of cyber security issues.

Education and skills

We know that our efforts to expand the UK's cyber security sector mean that we need more people with the right skills and education to support this. The National Cyber Security Programme is working with business, academia and the education sector to ensure we have a future workforce with cyber skills and expertise, as well as a basic understanding and awareness of cyber security among the public in general.

We are addressing skills at every level and have funded development of cyber security learning and teaching materials at GCSE and A-level, with further materials to be released to schools in January 2014. We are also funding initiatives at university level for graduates and post graduate students, as well as internship and apprenticeship initiatives, such as the one being run by GCHQ to attract technically-minded people.

To promote research in cyber security, we have:

- set up 11 Universities as Academic Centres of Excellence in Cyber Security Research
- established 3 new Research Institutes in the Science of Cyber Security
- set up 2 cyber security Centres for Doctoral Training to ensure the UK gains the high-end cyber security skills needed to tackle current and future cyber challenges

For the future, with NCSP funding, the Open University is developing a Massive Open Online Course (MOOC) in cyber security, to be run for the first time in summer 2014. The course is free and has a potential reach of 200,000 students world-wide. Through this initiative, we have a unique opportunity to raise awareness of cyber security to a mass audience of students, not just those in courses involving it, with an ultimate aim of bringing more students into the field.

Throughout 2012 to 2013 we have continued to fund work by the Cyber Security Challenge across the UK which runs innovative competitions to seek out talented, young people and motivate them into entering the field of cyber security. We have also funded a new Schools programme for the CSC which enabled them to run a pilot for which 562 schools have already signed up. For the coming year, we will be giving them a further £100,000 to roll out this pilot nationally.

We are also investing in public sector skills. For example, the National Archives are ensuring that staff across the public sector are trained in protecting information and have worked with National Fraud Authority to produce the e-learning course 'Responsible for Information', which has been taken by nearly 70,000 central government staff since July 2013. It is widely available across the public sector and we will be adapting it for an SME audience in early 2014.

However we also need to cast our net wider to ensure that people across the UK have a better understanding of potential threats and are better equipped with the necessary protection to go about their business online with confidence. To this end, BIS has been working with the UK's Internet Service Providers (ISPs) on a set of guiding principles for ISPs (https://www.gov.uk/government/publications/cyber-security-guiding-principles) to improve the online security of their customers. The principles, being launched today, set out that at a minimum, ISPs will provide cyber security information to their customers, or signpost to information elsewhere. ISPs will assist and empower their customers to protect themselves by offering tools and security solutions, or indicate where solutions can be accessed. If their customer does experience a problem, ISPs will support them by providing clear information about how to report the incident. They will also inform them of a potential compromise, in line with company policy, and explore ways to bring potential issues to the attention of customers. This is an important step in not only protecting people online but in helping to minimise the number and impact of cyber attacks in the UK.

Lastly, we are investing in a major campaign to increase awareness of cyber security amongst both the general public and small businesses. The campaign, led by the Home Office and backed by £4 million of funding from the NCSP, is to be launched next month. It is being supported by a broad range of organisations, including Facebook, BT, a number of anti-virus companies such as Sophos, banks and financial organisations as well as community and trade organisations. These organisations are providing financial and in-kind benefits worth around £2.3 million, which will extend the breadth and reach of the campaign and help to improve our nation`s cyber health.

Conclusion

We are in a much better place than 2 years ago when we launched the Strategy. This reflects the collective effort of numerous government departments and agencies, and powerful partnerships with industry, academia and international counterparts. Today I have also placed before Parliament a list of achievements over the past year, as well as a document which outlines our forward plans, priorities and some key initiatives we will be taking forward over the next 12 months.

There is still much work to be done, but our progress to date has put us in a strong position for the future.

Published 12 December 2013
Last updated 12 December 2013 + show all updates

1. 12 December 2013 Added link to policy reports.
2. 12 December 2013 First published.

Related content

Collection

- Cyber Security Strategy: progress so far (https://www.gov.uk/government/collections/cyber-security-strategy-progress-so-far--2)

Policy

- Cyber security (https://www.gov.uk/government/policies/cyber-security)