National Audit Office

REPORT BY THE
COMPTROLLER AND
AUDITOR GENERAL

HC 890
SESSION 2012-13

12 FEBRUARY 2013

Cross-government

The UK cyber security strategy: Landscape review

Key facts

Opportunities

3bn
people will be using the internet worldwide by 2016

£121bn
value of the UK's internet-based economy in 2010

8%
proportion of UK GDP accounted for by UK internet economy, a greater share than for any other G20 country

No.1
UK ranked against other G20 countries based on its ability to withstand cyber attacks and develop strong digital economy

Threats

44m
cyber attacks in 2011 in the UK

£18bn–£27bn
estimated annual cost to UK of cybercrime

80%
of cyber attacks could be prevented through simple computer and network 'hygiene'

Cyber attacks ranked as one of top four UK national risks in 2010

The UK cyber security strategy and programme

Additional funding of £650 million to protect and promote

2011-12	2012-13	2013-14	2014-15
£105 million	**£155 million**	**£180 million**	**£210 million**
November 2011 – The Cabinet Office publishes UK cyber security strategy: *Protecting and promoting the UK in a digital world*	December 2012 – The Cabinet Office reports progress after one year of the UK cyber security strategy, sets out plans and commits to report back on progress in 2013		

Fifteen government organisations working together on four objectives

1 To tackle cybercrime and make the UK one of the most secure places in the world to do business

2 To make the UK more resilient to cyber attack and be better able to protect its interests in cyberspace

3 To help shape an open, stable and vibrant cyberspace that the UK public can use safely and that supports open societies

4 To build the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives

Introduction

1 The growth of the internet, or cyberspace, has impacted profoundly on everyday life and the global economy. By enabling people to exchange knowledge and ideas all over the world, the internet has contributed to a more open society and greater freedom of speech. It has transformed the conduct of business and opened up new markets. The internet is also making governments more accountable and transparent and is changing the way they deliver public services.

2 If the internet were a national economy in its own right, it would be the fifth largest in the world.[1] The internet has evolved from initial experiments to link computer systems in the US in the 1960s, to the global interconnected network of systems and information that it is today. Commercial investment and technical innovation have driven these changes. International governments have intervened little. Nobody controls the internet, centrally or globally. Although no one person owns it, 80 per cent of the internet lies in the private sector. It is impossible to predict how people will use the internet in the future. With digital information growing, combined with new technologies, government, industry and citizens are likely to depend increasingly on the internet. Approximately three billion people will be using the internet by 2016.[2] However, the internet was not designed with security in mind.

An open internet

3 An open internet that is safe for everyone to use and that supports economic growth is central to the government's vision:

> "… for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values for liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society."[3]

4 The UK currently has one of the world's largest internet-based economies, valued at £121 billion in 2010. This is equivalent to 8 per cent of the UK's GDP, which is a greater share than for any other G20 country.[4] A secure internet is therefore vital for the UK's economic prosperity and to support government plans to make all public services digital.

Threats to the internet

5 Although providing opportunities, the internet also poses new and growing threats. As the internet is borderless and nobody polices it, legitimate users of the internet are vulnerable to attack. One report estimated that the UK suffered around 44 million cyber attacks in 2011, compared with one billion attacks across the world, although we must treat data on such events with caution.[5]

6 The government has recognised the existing and evolving threats to the internet and is focusing on:

- serious organised crime using the internet to steal personal or financial data to commit fraud, steal corporate intellectual property, or launder money;
- political activists hacking and using the internet to steal information or damage computer systems to serve political agendas; and
- state supported espionage and attacks on critical national infrastructure.

7 In June 2012, the head of MI5 warned that malicious activity in cyberspace had increased.[6] The Foreign Secretary recently announced that the computer systems supporting the London 2012 Olympics and Paralympics were attacked every day during the Games. Effective cyber security protected the Games against these threats and ensured services were not disrupted.[7]

8 Cyber attacks are easy and cheap to perpetrate compared with traditional crime, and attackers can easily evade prosecution by being in countries that will not arrest them. Consequently, tackling crime using the internet is a major challenge.

9 Serious organised crime has developed an internet-based black market for criminals, which sells stolen identity information and software products to launch cyber attacks as well as technical support for cybercrime.

10 The threat to cyber security is persistent and constantly evolving. The covert nature of the threats, however, means people can underestimate the risk to business, government and the citizen. Cybercrime currently costs the UK somewhere between £18 billion and £27 billion a year.[8,9] Consequently, business, government and the public must be aware of it and be able to resist the threat of cyber attack.

Government's response to cyber threats

11 In line with its vision for an open and trusted internet, the government raised cyber security as one of the four top risks for UK national security in 2010. It also recognised the opportunities that cyberspace presented to the UK. In the 2010 Comprehensive Spending Review, announced in October 2010, it therefore committed an additional £650 million of funding from 2011-12 to 2014-15 to a cross-government cyber security programme. The government already spends significant amounts on cyber security through the Single Intelligence Vote and in departments to secure their information, networks and systems. However, this departmental spending is highly disaggregated and the Cabinet Office does not have full insight into the total level of expenditure. The purpose of the additional £650 million was to enable different parts of government to work together to boost UK cyber defences and to promote the UK's strong international position.

12 In launching the government's 2011 UK cyber security strategy, the Prime Minister said:

> "While the internet is undoubtedly a force for social and political good, as well as crucial to the growth of our economy, we need to protect against the threats to our security. This strategy not only deals with the threat from terrorists to our national security, but also with the criminals who threaten our prosperity as well as blight the lives of many ordinary people through cybercrime. Cyber security is a top priority for government and we will continue to work closely with the police, security services, international partners and the private sector to ensure that the UK remains one of the most secure places in the world to do business."[10]

13 The strategy sets out what is at stake as follows:

> "Cyberspace has now grown to become a domain where strategic advantage – industrial or military – can be won or lost. It underpins the complex systems used by commerce (for example, banking, the delivery of food and the provision of utilities such as power and water) and the military. The growing use of cyberspace means that its disruption can affect nations' ability to function effectively in a crisis."[11]

14 The strategy addresses not only the technical aspects of cyber security (protecting systems, networks and information) but as importantly, it seeks to change the attitudes and behaviours of business, government and the public so that everyone uses the internet safely.

Parliament's increasing interest in cyber security

15 Parliament has shown an increasing interest in cyber security. In 2010, the House of Lords EU Committee reported that the UK was reasonably well-placed to deal with cyber attacks and was 'a leader in the EU, with developed practices that set benchmarks for others to adopt'.[12]

16 In 2012 and 2013, the following committees reported:

- The Science and Technology Committee called for government to do more to help the public understand how to stay safe online;[13]
- The Defence Select Committee published a report on cyber security in relation to the Ministry of Defence and the Armed Forces;[14]
- The Intelligence and Security Committee praised work on the defence and security of computer networks, but were concerned that delays in developing national capabilities will give the UK's enemies an advantage, given the rapid rise in cyber threats;[15] and
- The Home Affairs Select Committee held an inquiry into cybercrime.

17 The Committee of Public Accounts has not examined cyber security specifically, although it did point to a lack of detail on cyber security plans in the government's 2011 ICT strategy, given the government's aim to move more services online.[16] In March 2012, it also raised concerns about cyber security in the government's plans for smart electric and gas meters, which will enable suppliers to collect meter readings over the internet.[17]

Purpose of this landscape report

18 An effective UK response to cyber threats is essential for future economic prosperity, making public services digital by default, and maintaining the values and freedom of an open society. This landscape review describes government's evolving approach to cyber security and describes the programme of work it has under way. It sets the scene in an area likely to interest the Committee of Public Accounts. It does not conclude on the value for money of the government's cyber security strategy at this early stage.

- Part One describes the cyber security strategy published in 2011 by the Cabinet Office. It describes what 15 different parts of government are doing together to deliver the strategy and explains how the unclassified part of the £650 million budget is being spent.
- Part Two identifies the challenges that government faces in delivering its strategy.

Our approach

19 This report draws on our work as auditors of central government, past government publications, research from think tanks and data from the Cabinet Office. We interviewed lead officials, industry representatives, academics and citizens' groups during July to October 2012 and held a round table with leading cyber academics. We have also drawn on the Cabinet Office's progress report published in December 2012.[18] We explain our methodology in Appendix One.