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

Our vision is to help the nation spend wisely.

We apply the unique perspective of public audit to help Parliament and government drive lasting improvement in public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Amyas Morse, is an Officer of the House of Commons and leads the NAO, which employs some 860 staff. The C&AG certifies the accounts of all government departments and many other public sector bodies. He has statutory authority to examine and report to Parliament on whether departments and the bodies they fund have used their resources efficiently, effectively, and with economy. Our studies evaluate the value for money of public spending, nationally and locally. Our recommendations and reports on good practice help government improve public services, and our work led to audited savings of more than £1 billion in 2011.

National Audit Office

Cross-government

The UK cyber security strategy: Landscape review

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 11 February 2013

This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act

Amyas Morse
Comptroller and Auditor General
National Audit Office

5 February 2013

HC 890 London: The Stationery Office £16.00

This landscape review describes government's evolving approach to cyber security and describes the programme of work it has under way.

Printed in the UK for the Stationery Office Limited on behalf of the Controller of Her Majesty's Stationery Office

2540545 02/13 PRCS

Contents

Key facts 4

Introduction 5

Part One
The UK cyber security strategy 10

Part Two
Challenges for government 24

Annex
Assessing the value for money of cyber security 32

Appendix One
Our audit approach 36

Appendix Two
Our evidence base 38

Endnotes 40

The National Audit Office study team consisted of:
Veronica Marshall, Linda Mills, Jeremy Weingard and James Young, under the direction of Sally Howes

This report can be found on the National Audit Office website at www.nao.org.uk/cyber-security-2013

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

Tel: 020 7798 7400

Enquiries: www.nao.org.uk/contactus

Website: www.nao.org.uk

Twitter: @NAOorguk

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.

Part One

The UK cyber security strategy

1.1 In this part of our report, we describe the background to the 2011 UK cyber security strategy and its scope. We set out the government's spending and the progress it has made to date.

Evolution of the UK cyber security strategy

1.2 The government's 2011 strategy builds on ten-years' experience of seeking to protect government information, systems and networks (**Figure 1** on pages 12 and 13). In 2001, the Communications-Electronics Security Group (CESG) (within GCHQ) first recognised the importance of protecting the security of data. The group recommended the appointment of a central sponsor to determine policy on managing and securing government data.

1.3 By 2004, the government had published a national strategy for information assurance and established a network of Senior Information Risk Owners. They aimed to lead and foster a culture that valued and protected information.

1.4 Two serious losses of data in HM Revenue & Customs in 2007, and the Ministry of Defence in 2008, damaged the reputation of the government and demonstrated the importance of managing information risk. Reviews of these incidents found that information security had not been a management priority.

1.5 In 2009, the government recognised the emerging and significant risks of cyber threats and published its first cyber security strategy. The aim was to broaden its role beyond that of protecting government information and systems. It also wanted to work with industry and citizens to protect the wider UK economy and society from cyber threats. As part of its strategy, the government set up the Office of Cyber Security in the Cabinet Office.

1.6 In 2009, the government ranked cyber attacks on the UK below climate change, terrorism, failed states and the banking crisis as key risks to UK national security. By 2010, it had raised cyber attacks to one of the four top national risks, alongside international military crises, terrorism, and major incidents such as natural disasters or influenza pandemics.[19] In response to the rising risks of cyber attacks, in November 2010, the government announced an additional £650 million of funding for a four-year National Cyber Security Programme.[20] The Home Office transferred responsibility for cyber security in government to the Cabinet Office in 2011.

1.7 In November 2011, the government published a new cyber security strategy.[21] This set out how the government planned to deliver the National Cyber Security Programme through to 2015.

The new strategy

1.8 The strategy differs from the previous one. For example, the strategy places greater emphasis on the role and responsibilities of the public and industry in helping secure the UK against attacks. It also recognises that existing legislation and education at all levels should incorporate cyber security within mainstream activities.

1.9 The strategy sets out four key objectives. Six central departments and nine other government organisations (including those in the Intelligence and Security Agencies) are responsible for delivery as shown in **Figure 2** on page 14.

1.10 In the strategy, the government describes what success will look like for the UK.

- Individuals know how to protect themselves online.
- Businesses operate securely in cyberspace.
- It has a growing international market in cyber security products and services.
- It is recognised as a safe place to do business in cyberspace.
- Its law enforcement has been sharpened to tackle cybercrime.
- Its critical national infrastructure is protected against cyber attack.
- Its capabilities to detect and defeat attacks in cyberspace are stronger.
- Skills and capability, research and development and all levels of education effectively support cyber security.
- Working relationships with other countries, business and organisations around the world are strong and well established.

Governance

1.11 The strategy sets out how the government will deliver the 2010 National Cyber Security Programme. The Office of Cyber Security and Information Assurance (OCSIA), among other responsibilities, manages and coordinates the programme which the Minister for the Cabinet Office oversees as shown in **Figure 3** on page 15. Six Cyber Delivery Capability Groups manage activities at a working level and the Cyber Delivery Management Group, representing all 15 delivery partners, meets quarterly to review the programme and address cross-cutting issues. The programme is included within the governance arrangements for the government's Major Projects Portfolio and participates in annual Gateway reviews by the Efficiency and Reform Group to ensure that it follows best practice.

Figure 1

Information assurance and cyber security reports, events and key changes in strategic direction

The government's approach to cyber security has developed since 2001

	2001	2002	2003	2004	2005		2006	2007	2008	2009	2010	2011
	Information Assurance									**Cyber Security**		
Report	The Communications-Electronics Security Group (CESG) Review recommending Central Sponsor for Information Assurance			National Information Assurance Strategy				Updated National Information Assurance Strategy		First cyber security strategy Coleman Report: *Protecting government information* Data Handling Procedures in Government: *Final Report and Poynter Review of information security at HM Revenue & Customs*	The National Security Strategy: *A Strong Britain in an Age of Uncertainty* This outlines reappraisal of Britain's role in the world, the risks to our security and their implication for the UK The Strategic Defence and Security Review	UK cyber security strategy This sets out the objectives and tasks to be undertaken as part of the National Cyber Security Programme
Event	Increasing use of online services requires development of security measures. Outcome of CESG's review was to recommend a central sponsor for Information Assurance	E-envoy appointed as Central Sponsor for Information Assurance (CSIA) Central Sponsor for Information Assurance (CSIA) secretariat established		A network of Senior Information Risk Owner's (SIROs) across government established				HMRC loses disc containing Child Benefit data of 25 million people	Ministry of Defence loses personal records of around 600,000 people	The Office of Cyber Security formed in the Cabinet Office		Ministerial responsibility for cyber security moved from the Home Office to the Cabinet Office
Key changes in strategic direction		This new role provides focus for Information Assurance activity and development of a National Information Assurance strategy		This is the first framework for departments and public bodies, to help them understand ICT risks. It sets out government's approach to dealing with risks facing information systems				Single Information Assurance framework for the whole of the UK extended beyond confidentiality of information to cover availability, integrity, non-repudiation and authentication		Government responds to increasing risks of cyber threats by broadening its role beyond Information Assurance to cyber security Protection of government systems and critical infrastructure part of the strategy. Also recognition that cyber protection requires a multi-stakeholder approach and action at many levels	Cyber security elevated to one of the four key risks to UK national security Strategic Defence and Security Review announce £650 million of additional funding for National Cyber Security Programme	Cyber security strategy now includes how the UK will tackle cyber threats to promote economic growth and to protect national security and the UK's way of life

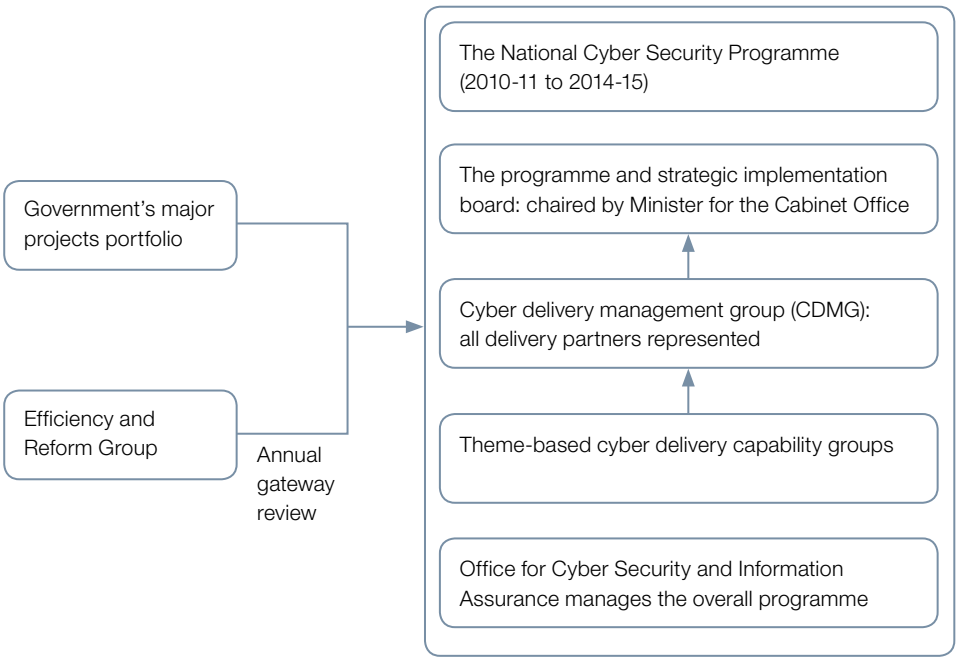
Sources: 1–6, 9–11 The Cabinet Office. 1. National Information Assurance Strategy, 2003; 2. Protecting our information system, 2004; 3. A National Information Assurance Strategy (revision), 2007; 4. Protecting Government Information; The Coleman Report, 2008; 5. Data Handling Procedures in Government: Final Report, 2008; 6. Cyber Security Strategy of the United Kingdom, 2009; 7. HMRC – Poynter Recommendations – ICO Audit, ICO, 2010; 8. Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, The Ministry of Defence, 2010; 9. Protecting government information, 2010; 10. The National Security Strategy "A Strong Britain in an Age of Uncertainty", 2010; 11.The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, 2011

Figure 2
Strategic objectives and responsibilities for the National Cyber Security Programme

Objective	Organisations	Responsibilities
1 To tackle cybercrime and make the UK one of the most secure places in the world to do business	Home Office, Serious Organised Crime Agency, Child Exploitation and Online Protection, Police Central e-crime Unit, police forces, National Fraud Authority	Tackling cybercrime: • Reducing online vulnerability • Restricting criminal activity online • Promoting effective partnerships
	Department for Business, Innovation and Skills, Technology Strategy Board, UK Trade and Investment	Making it safer to do business in cyberspace: • Increasing awareness and visibility of threats • Improving incident response • Protecting information and services • Fostering a culture that manages the risks • Promoting confidence in cyberspace
2 To make the UK more resilient to cyber attack and be better able to protect its interests in cyberspace	The Cabinet Office and the Intelligence and Security Agencies	Defending national infrastructure: • Strengthening defences in cyberspace • Improving resilience and diminishing the impact of cyber attacks • Countering terrorist use of the internet
	Ministry of Defence	Ensuring that the UK has the capability to protect UK interests in cyberspace: • Improving our ability to detect threats in cyberspace • Expanding our capability to deter and disrupt attacks on the UK
3 To help shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies	Department for Culture, Media and Sport	Helping to shape the development of cyberspace: • Promoting an open and interoperable cyberspace • Promoting our fundamental freedoms and rights
	Foreign and Commonwealth Office	Protecting our way of life: • Ensuring our security without compromising our values
4 To build the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives	Department for Business, Innovation and Skills	Extending knowledge: • Building a coherent research agenda • Understanding threats, vulnerabilities and risks
	Department for Business, Innovation and Skills	Enhancing skills: • Building a culture that understands the risks • Improving skills at all levels
	The Cabinet Office	Expanding capability: • Building technical capabilities • Increasing ability to respond to incidents

Source: UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, Cabinet Office, 2011

Figure 3
Governance of the National Cyber Security Programme



Source: National Audit Office

Funding

1.12 In 2010, the Office of Cyber Security allocated additional funding of £650 million to the National Cyber Security Programme. The government has published provisional allocations for this funding as set out in **Figure 4** overleaf and plans for future years are indicative. Only a portion of future spend has been committed, to allow flexibility to respond to developments in what is a fast-moving area. Allocations are agreed on an annual basis.

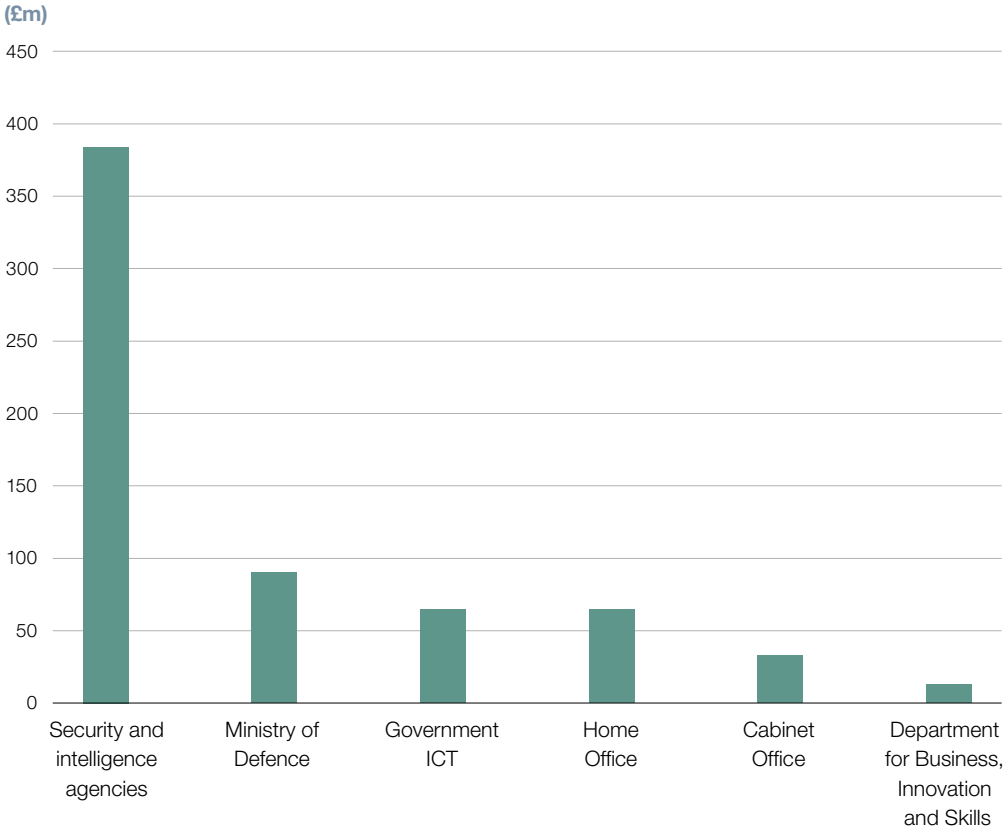
1.13 In addition to the £650 million of funding shown in Figure 4, departments and agencies are allocating funding from their operational budgets to cyber security. The figure of £650 million does therefore not include spending in support of cyber objectives that the National Cyber Security Programme does not fund. Such expenditure, however, is not always separately identified in departmental budgets and is not therefore readily quantified.

Figure 4

Breakdown of £650 million funding for the National Cyber Security Programme (2011-12 to 2014-15)

Funding has been allocated to six areas over the four years

£650 million			
2011-12 £105m	**2012-13** £155m	**2013-14** £180m	**2014-15** £210m



	Security and intelligence agencies	Ministry of Defence	Government ICT	Home Office	Cabinet Office	Department for Business, Innovation and Skills
£ million	384	90	65	65	33	13
Percentage	59%	14%	10%	10%	5%	2%

NOTES

1 Nominal values.

2 The funding shown for each department is the total amount allocated over the four years 2011-12 to 2014-15.

Source: UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, Cabinet Office, November 2011

Progress

1.14 The government reported progress after one year in December 2012.[22,23] **Figure 5** on pages 18 to 21 describes the government's progress against its strategic objectives and details of the government's plans. Activities are already beginning to deliver benefits. For example, the government has reported the following:

- in 2012, the Serious Organised Crime Agency (SOCA) took down 36 website domains that were selling compromised credit card and financial data. This was part of an international operation with the FBI and US Department of Justice. According to the SOCA this operation prevented international fraud estimated to be over £500 million; and
- in the past year, Action Fraud, managed by the National Fraud Authority, has received over 46,000 reports of cybercrime from the public. This amounted to fraud that would have cost £292 million.

Spending to date

1.15 We show outturn and forecast spending during the first two years of the National Cyber Security Programme in **Figure 6** on page 22. This is within the budget of £260 million allocated for 2011-12 and 2012-13 as shown in Figure 4. Spending has supported a broad range of cyber activities shown in Figure 5. In some areas, such as skills and awareness, the government will spend more in the next two years as initiatives expand. We can only comment on the unclassified part of the overall £650 million budget and are unable to show a breakdown of 'sovereign capability' spend in the Intelligence Agencies. However, developing this capability supports activity across all strands of the programme.

Figure 5
The government's progress and plans for cyber security (as at December 2012)

Progress

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

Tackling cybercrime

Action Fraud (managed by the National Fraud Authority) became the UK's national reporting centre for fraud and financially motivated cybercrime. It has received 46,000 reports of cyber-enabled crime amounting to £292 million of attempted fraud.

National Fraud Authority and industry partners delivered 'The Devil's in Your Details' cyber security awareness campaign that it claims reached over four million people.

The Police Central e-crime Unit has trebled in size and developed a framework for cyber specials (volunteer police officers with specialist cyber skills).

New regional cybercrime teams created in Yorkshire and the Humber, The North West and East Midlands.

The Home Office issued strategic policing requirements, which included major cyber incidents.

The Serious Organised Crime Agency increased its cyber capability to support international liaison and mainstreaming cyber investigations across the agency.

The Crown Prosecution Service enhanced its cybercrime prosecution capability. At end of September 2012, the service was prosecuting 29 'live' cybercrime cases.

The Crown Prosecution Service expanded its in-house cybercrime training programme.

The Police Central e-crime Unit, with other international agencies, suspended over 15,000 websites engaged in fraud.

The Serious Organised Crime Agency repatriated over 2.3 million items of compromised card payment details back to the financial sector in the UK, and internationally, since 2011, preventing potential economic loss of over £500 million.

The Serious Organised Crime Agency led a day of global action to tackle automated vending carts websites selling compromised financial data.

The Serious Organised Crime Agency and The Police Central e-crime Unit started joint operations as part of the transition to the new National Cyber Crime Unit.

The Foreign and Commonwealth Office contributed £100,000 to support a Council of Europe global project on cybercrime.

The Serious Organised Crime Agency worked with international partners such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Commonwealth cybercrime initiative on internet security.

HM Revenue & Customs established a cybercrime team to tackle tax fraud by organised criminals, which went live in time to protect the self-assessment filing peak.

Making the UK one of the most secure places in the world to do business

The Government Communications Headquarters (GCHQ), Centre for the Protection of National Infrastructure (CPNI), the Department for Business, Innovation and Skills, and OCSIA produced *Cyber Security Guidance for Business (the Ten Steps)*[1] aimed at providing advice to chief executives and board members.

CPNI expanded its scope to include companies not traditionally part of the critical national infrastructure.

The Department for Business, Innovation and Skills produced a report identifying growth potential of the UK cyber security sector.

A pilot joint public-private sector cyber threat information-sharing scheme, led by GCHQ completed.

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

GCHQ has invested in new capabilities to identify and analyse hostile cyber attacks on UK networks. This includes hosting the new Joint Cyber Unit in partnership with the Ministry of Defence to help counter cyber threats to the UK.

The Security Services developed additional capability to investigate cyber threats from foreign intelligence agencies and terrorists.

CPNI commissioned cyber security research to help enhance the advice it provides to industry on effective cyber protection.

The Cabinet Office and the security and intelligence agencies developed new ways of working to engage with business to protect the 2012 Olympic Games from cyber threats.

GCHQ and CPNI launched the cyber incident response pilot scheme to provide links to organisations certified to deal with cyber security attacks.

CPNI commissioned a major research programme with Oxford University to provide advice, guidance and products to reduce risk of cyber insider acts.

The government developed a new security model to protect the Public Services Network.

Plans

Objective 1: *continued*

Tackling cybercrime

To launch the national cybercrime unit in 2013 as part of the new National Crime Agency.

For government to continue to enable law enforcement and industry to cooperate and share information. The UK Cyber Information Sharing Partnership is an example of this.

For government to continue to build relationships with international law enforcement agencies to undertake more joint operations.

To enhance Action Fraud to make it easier for businesses to report repeat cases of fraud.

To launch a new Cybercrime Reduction Partnership between government, law enforcement, industry and academia.

Making the UK one of the most secure places in the world to do business

For the Department for Business, Innovation and Skills to work with businesses and their representatives to communicate messages from *Cyber Security Guidance for Business (the Ten Steps).*[1]

For CPNI to expand its cyber risk management advice to business.

For government to roll-out a programme of small and medium-sized business (and public) awareness drives in 2013. The Department for Business, Innovation and Skills to provide targeted information and advice for small and medium-sized enterprises using existing channels such as 'Get Safe Online' and 'Business in You'.

For government to mainstream cyber security messages across the breadth of its communication with business.

For defence and security procurements to embed cyber security best practice requirements in future contracts.

For CPNI to publish research with Oxford University to help reduce risk of cyber attacks by company insiders.

For government to continue to engage with institutional investors, professional and representational institutions and auditors to help company boards see cyber security as a significant business risk requiring action.

For an annual information security breaches survey to be introduced between 2013 and 2015 to enable organisations and sectors to benchmark performance against peers to drive up industry standards.

For the government to support development of industry-led cyber security standards and kitemarks for products and services. This will help clarify what good cyber security practice looks like and enable companies to differentiate themselves in the marketplace.

For the government to use its procurement frameworks to share information securely across supply chains.

GCHQ will promote and extend 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.

To launch a 'Cyber Growth Partnership' in conjunction with Intellect UK (which represents the UK technology industry and has over 850 members) to identify how to support the growth of the UK cyber security industry.

The government will increase the number of cyber security contracts going to small and medium-sized businesses. At least 25 per cent of GCHQ's procurement budget will be spent through small and medium-sized businesses.

To encourage smaller firms to innovate through initiatives such as the 'Finding the Threat', a call to small and medium-sized businesses requesting innovative ideas to address a set of security and intelligence challenges.

Objective 2: *continued*

For the government to increase security of its computer networks with the next phase of the Public Sector Network.

For lessons learned from the Olympics to be used to review and strengthen protection and resilience of the UK to cyber attack.

For the government to establish a UK national computer emergency response team in conjunction with industry. This will improve national coordination to respond to incidents and enable international sharing of technical information on cyber security.

For a government pilot information scheme, the Cyber Information Sharing Partnership, to be launched in 2013.

For the government to continue to work closely with key allies and like-minded partner countries on developing cyber security policy sharing information and coordinating responses.

Figure 5 *continued*
The government's progress and plans for cyber security (as at December 2012)

	Progress	Plans
Objective 3: To help shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies	The Foreign and Commonwealth Office organised 2011 and 2012 London Conferences on Cyberspace attended by 60 countries and worked with Hungary to deliver the Budapest Conference in October 2012. The Foreign and Commonwealth Office funded the new international Cyber Security Capacity Building Centre to tackle global cybercrime. The Cabinet Office and its industry partners delivered a 'Get Safe Online' week as part of the global 'Cyber Security Month' in October each year. The government worked with NATO and the EU to develop their emerging cyber strategies. Government departments and law enforcement agencies worked with international partners to encourage countries to sign up to the Budapest Convention on Cyber Crime.[2] Government departments played a prominent role in working with the UN Government Group of Experts and the Organisation for Security and Cooperation in Europe to improve cyber security.	**Objective 3:** *continued* For government to continue to expand and strengthen the UK's bilateral and multilateral networks, and to collaborate internationally through the work of the EU, NATO and other bodies. The government will continue to work with other international organisations and countries to develop the 'rules of the road' for cyberspace. The government will continue to work for trans-border law enforcement cooperation on cybercrime. With more countries intending to sign up to the Budapest Convention on Cybercrime in the coming year, UK law enforcement agencies will continue to expand partnership building and joint operations. For government to extend its advice and guidance to other countries to help them build capacity to tackle cyber threats and deny safe havens for cybercriminals through the new international Cyber Security Capacity Building Centre.
Objective 4: To build the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives	GCHQ launched a scheme to certify information assurance and cyber security professionals in the UK. GCHQ, in partnership with the Research Councils' global uncertainties programme and the Department for Business, Innovation and Skills awarded 'academic centre of excellence in cyber security research' status to eight UK universities and launched a research institute for the science of cyber security. GCHQ launched a programme to develop cyber security talent in schools and universities. The Department for Business, Innovation and Skills commissioned e-skills to produce cyber security learning materials as part of the 'Behind the Screen Pilot'. Schools can download this material. Joint public and private sector initiative 'Cyber Security Challenge UK' launched a new framework to enable people to move into cyber security mid-career. The government delivered 'Protecting Information' levels 1 to 3 and 'Fraud and Corruption' e-learning packages for the wider public sector. Cyber security training for the civil service, law enforcement and the military rolled out.	**Objective 4:** *continued* For the Department for Business, Innovation and Skills to continue to work with institutions to ensure undergraduates taking technical degree courses receive adequate training in cyber security. For the Department for Business, Innovation and Skills to launch two centres of doctoral training to fund 48 PhDs on multidisciplinary cyber topics. For GCHQ to sponsor 30 PhDs. For government to continue to identify and develop cyber security talent in school and university and support innovation through initiatives such as the 'Cyber Security Challenge UK'. For the Ministry of Defence to launch a 'Cyber Reservists' programme to recruit cyber security experts. For GCHQ to put in place a scheme to certify cyber security training courses to develop and certify professionalism in cyber security. For GCHQ, Engineering and Physical Sciences Research Council (EPSRC) and the Department for Business, Innovation and Skills to extend the Academic Centres of Excellence in Cyber Security Research Programme to other universities. This 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 increasing innovation. For a second Research Institute to be set up in 2013 to focus on automated program analysis and verification. For a new multidisciplinary academic cyber journal to be launched in 2013 to publish a broad range of cyber security research from both UK and international universities. For the government to mainstream cyber security messages across the breadth of communications with citizens. For the government to roll-out a programme of public awareness drives in 2013, building on 'Get Safe Online' and the work of the National Fraud Authority.

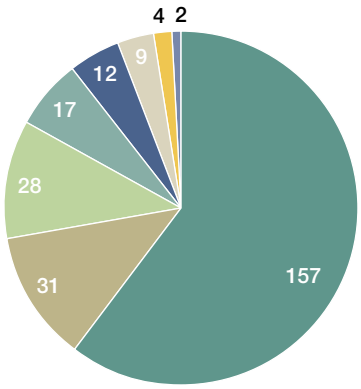
NOTES

1 *Cyber Security Guidance for Business*. September 2011 available at: www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive

2 Convention on Cybercrime, Budapest, 23 November 2001 available on the website of the Council of Europe.

Sources: Cabinet Office, Progress against the Objectives of the National Cyber Security Strategy – December 2012; Cabinet Office, The UK Cyber Security Strategy Report on Progress – December 2012: Forward Plans

Figure 6
Spending on the National Cyber Security Programme – includes actual spend in 2011-12 and forecast spend in 2012-13 (£ million)



- National sovereign capability to detect and defeat high end threats – Security and Intelligence Agencies
- Mainstreaming cyber throughout defence – Ministry of Defence
- Enforcing laws and combating cybercrime – Home Office
- Engaging with the private sector – Department for Business, Innovation and Skills
- Improving the resilience of the Public Sector Network – The Cabinet Office
- Coordinating programme, analysing trends and managing and responding to incidents – The Cabinet Office
- Education, skills and awareness – The Cabinet Office
- International engagement and capacity building – Foreign and Commonwealth Office

Source: Cabinet Office, Progress against the Objectives of the National Cyber Security Strategy – December 2012

International comparison

1.16 Many countries have developed cyber security strategies reflecting their national policy priorities, an assessment of cyber risks and their economic position.

1.17 We reviewed the cyber security strategies of nine countries to compare with the UK's strategic objectives. We found the UK's strategy to be unique in terms of the weight given by the UK government to promoting and securing commercial opportunity for UK business in the growing international cyber security market. What the UK shares with other countries is shown in **Figure 7**:

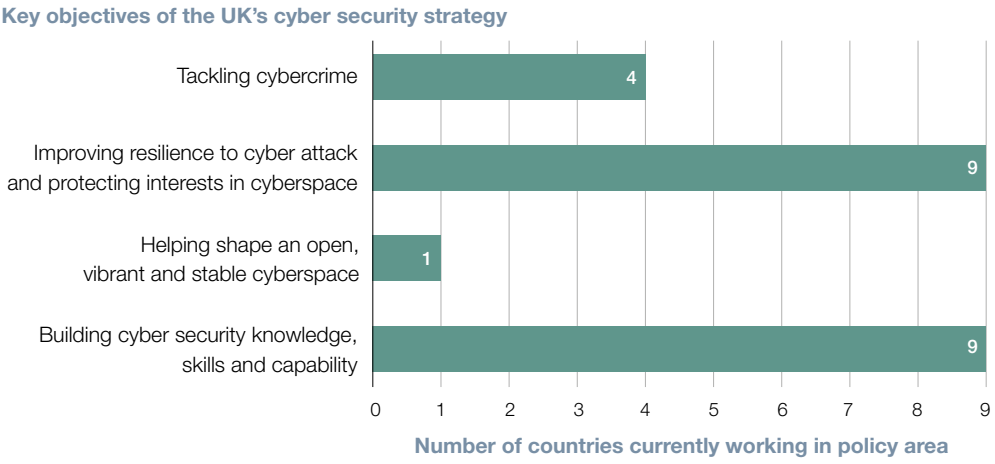
- four countries' strategies share the UK's focus on tackling cybercrime as an objective;
- all countries have stated objectives of working towards improving resilience to cyber attacks and protecting national security;

- only one other country, the USA, shares the UK's objective of helping to shape an open vibrant cyberspace to support open societies; and
- all countries aim to build cross-cutting knowledge and skills and capability in cyber security.

1.18 The UK therefore has one of the most wide-ranging cyber security strategies. Research by Booz Allen Hamilton and the Economist Intelligence Unit also shows that the UK leads other G20 countries in its ability to withstand cyber attacks and to develop a strong digital economy.[24] This is based on assessing each country's legal and regulatory frameworks, economic and social issues, technology infrastructure, and industry.

Figure 7
The number of countries of the nine reviewed that share the UK's cyber security objectives

Two of the UK's cyber security strategic objectives are common to the strategies of all nine of the countries we reviewed



NOTE

1 We reviewed the cyber security strategies of Australia, China, Estonia, France, Germany, India, Japan, Russia, and the USA.

Source: National Audit Office 2012

Part Two

Challenges for government

2.1 In this part, we describe six key challenges the government faces in implementing its cyber security strategy:

- influencing industry to protect and promote itself and UK plc;
- addressing the UK's current and future ICT and cyber security skills gap;
- increasing awareness so that people are not the weakest link;
- tackling cybercrime and enforcing the law at home and abroad;
- getting government to become more agile and joined-up; and
- demonstrating value for money.

Influencing industry

Forming effective partnerships with industry to reach a common understanding of risks and share the costs of protecting UK plc

2.2 The UK 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. The cost of cybercrime is also significant and estimated to cost the UK, mainly industry, between £18 billion to £27 billion a year.[25,26,27]

2.3 At risk of cyber attack is the UK's economy including the nation's critical national infrastructure. This infrastructure includes the networks, computer systems and electronic data that underpin government, emergency services, communications, utilities, financial services, food, health, and transportation. These services are essential to daily life, owned mostly by the private sector and their protection from cyber attacks is crucial.

2.4 The government has recognised that it needs to work in partnership with industry. It considers, for example, that cyber security is not well understood at board level and executives have difficulty assessing the impact of cyber security risks.[28] For this reason, GCHQ, the Department for Business, Innovation and Skills, CPNI and the Cabinet Office published advice for boards in September 2012 on the risks of cyber security and how to mitigate them.

2.5 Identifying how much investment the UK needs can be difficult as information on cyber threats is often unreliable. Reporting cyber attacks is not mandatory for public or private sector organisations. Many incidents go unreported, as news of them could damage corporate reputation and customers could lose confidence in using online services. For example, Sony's share price fell by 5 per cent in 2011 when the personal details of 77 million of its online PlayStation customers were stolen.

2.6 To advise industry and counter the lack of accurate threat information, the government has launched a number of new initiatives. For example, CPNI and the Communications-Electronics Security Group (CESG) inform industry on cyber threats and advise on cyber security. In November 2012, the government launched the Cyber Security Incident Response Service, which provides access to quality assured industry and government expertise for organisations after a cyber attack. While aimed at public sector organisations, the government also expects that the service will benefit the private sector. Figure 5 shows more initiatives.

2.7 The government has recognised the need to develop cyber security standards to help it, industry and citizens make informed choices about security products and services. It is working with the British Standards Institute to encourage the development of industry-led standards, kitemarks and best practice advice on cyber security. This covers products, processes and principles for cyber security. The government is also considering incorporating cyber security standards in its procurement frameworks to help secure its supply chain.[29]

2.8 The government considers that developing industry-led standards would help promote the UK as a safe place for internet trade and commerce and assist UK businesses to promote their products or services within both domestic and overseas markets.

2.9 Those we interviewed from government, academia and industry were generally positive about how government is working with industry and providing help and guidance. Many observed that the government advice released so far targets larger businesses. The government is aware of this and of the need to get its message across to small and medium-sized businesses too. It is tailoring its guidance accordingly. The Department for Business, Innovation and Skills will include messages on cyber as part of its mainstream communications with small and medium-sized businesses. The government has said it intends to target these businesses as part of the public awareness campaign it is planning for 2013.

2.10 Most interviewees thought that the introduction of industry-led cyber security standards to be beneficial, especially to the citizen and small and medium-sized businesses, but many considered that progress on standards was too slow. The government agrees and to encourage faster progress, ministers announced in December 2012, that the government will develop and make public in early 2013 a 'meta-standard', characterising what it believes a robust organisational standard should include. The government has said it will look to endorse and support the first standard coming to market that meets these criteria.

2.11 Interviewees also highlighted the risk supply chains posed and suggested that government and large companies make sure that their suppliers implement minimum standards for managing cyber risks. The Ministry of Defence has been working with its suppliers to develop such requirements for companies bidding for defence contracts. A number of interviewees suggested that larger businesses could help small and medium-sized businesses, particularly where there was an existing relationship such as a supply chain. The Department for Business, Innovation and Skills is working with the Confederation of British Industry and others to encourage this.

Addressing the UK's current and future ICT and cyber security skills gap

Ensuring the UK has enough skilled people and the right research and development to plug the immediate skills gap and address longer-term needs in the public and private sector

2.12 According to the government, the number of ICT and cyber security professionals in the UK has not increased in line with the growth of the internet.[30] This shortage of ICT skills hampers the UK's ability to protect itself in cyberspace and promote the use of the internet both now and in the future. The skills the UK needs to design and implement cyber security policy are not only technical, there is also a need for psychologists; law enforcers; corporate strategists and risk managers. Other professionals such as lawyers and accountants also need to understand cyber security in order to assess, manage and mitigate the business risk of cyber threats.

2.13 In April 2012, the Minister for Business, Innovation and Skills referred to 'a decade long' decline in ICT and computer science in schools and universities.[31] The government's special representative to business for cyber security also commented on the lack of younger people working in the area of cyber security. In 2011, the Committee of Public Accounts raised concerns about cyber security skills in government and recommended that the government needed to employ more people with these skills. Attracting and retaining talent is also a concern. In 2012, the Intelligence and Security Committee highlighted GCHQ's inability to retain internet specialists in the face of competition from the private sector.[32]

2.14 In 2012, the government established a Research Institute in the Science of Cyber Security and awarded 'Academic Centre of Excellence in Cyber Security Research' status to eight UK universities to boost research and to expand the UK's cyber skills base. We describe the government's activities in this area in Figure 5.

2.15 Interviews with government, academia and business representatives confirmed that the UK lacks technical skills and that the current pipeline of graduates and practitioners would not meet demand. A number of government departments commented that the UK depended on a small number of highly skilled people to participate in developing international technical standards. The government has introduced a range of initiatives aimed at broadening the pipeline as summarised in Figure 5.

2.16 Interviewees were concerned about a lack of promotion of science and technology subjects at school resulting in the reported lower uptake of computer science and technology courses by UK students. Those we interviewed from academia considered that it could take up to 20 years to address the skills gap at all levels of education. The government is working to address this and has said that it intends to overhaul ICT teaching in schools to make it genuinely about computer science rather than office skills. It expects cyber security to be a strong strand of the future GCSE computer science syllabus.

Increasing awareness so that people are not the weakest link

Raising awareness of online risks and individual responsibilities right across the UK so that people are not the weakest link for the security of their families or their employers

2.17 Cyber attacks exploit vulnerabilities in human behaviour and lack of awareness of risk. If people are not aware of threats and of how to stay safe online, they can put themselves, their children, their employers or even the nation at risk.

2.18 In 2011, 77 per cent of UK households, 19 million in total, had internet access compared to 73 per cent in 2010.[33] Twenty-one per cent of UK internet users, however, do not think they have sufficient skills to protect their personal data.[34] GCHQ estimates that 80 per cent of cyber attacks could be prevented through simple computer and network 'hygiene', such as using 'strong' passwords,[35] but in 2012, the top three passwords were password, 123456 and 12345678.[36] In 2011, the Science and Technology Committee reported that the most common form of cyber threat experienced by people was malicious software (malware) followed by online credit card fraud and social network profile hacking.[37]

2.19 The increased use of social media and unsupervised child access to the internet is also leading to greater child exploitation according to the Child Exploitation and Online Protection Agency. It has reported receiving 1,300 reports of child exploitation on average each month, 263 per cent more than two years ago.[38]

2.20 As more public and private sector services move online, the government has recognised the risk of a lack of public awareness and the need for behavioural change. It has already allocated £6 million to public education, including the public-private sector initiative 'Get Safe Online'. The government launched this initiative in 2005 to provide advice to small and medium-sized businesses and the public on internet security ranging from prevention of email frauds to how to protect networks. The programme also sponsored the 'Devil's in Your Details' campaign in spring 2012, run by the National Fraud Authority, which estimated that the campaign reached over four million individuals. Two-thirds of those surveyed said they would change their behaviour as a result. The government intends to roll-out from spring 2013, a significantly expanded programme of public awareness drives, building on the work of 'Get Safe Online' and the National Fraud Authority.

2.21 Many of our interviewees highlighted the need for better targeting of public awareness campaigns to address the needs of different users, particularly those from lower socio-economic groups and those less competent with ICT. On behalf of the National Cyber Security Programme, the National Fraud Authority has carried out a market segmentation exercise to ensure that the next stage of public awareness work is properly grounded in an understanding of what works for different groups.

Tackling cybercrime and enforcing the law at home and abroad

Enabling the police and encouraging the judiciary to make greater use of existing laws in the UK to deal with cybercrime and continuing to influence the international community for increased cooperation

2.22 Criminals use the internet for a variety of crimes including fraud, identity theft, theft of financial information and corporate intellectual property and child exploitation. Many criminals view the internet as a profitable and low-risk channel for committing crime and because it is borderless they can base themselves in countries that are unlikely to prosecute them.

2.23 In the UK, the government is working to ensure that law enforcement agencies and the judiciary use existing legislation to tackle cybercrime and protect the public. Such laws include Conspiracy to Defraud, the Data Protection Act 1998 and the Computer Misuse Act 1990. Courts are also able to monitor or restrict the computer use of cyber criminals.

2.24 Figure 5 sets out other actions government is taking which includes implementing a new national cybercrime capability. This will bring together work of the e-crime unit in the Serious Organised Crime Agency and the Police Central e-crime Unit. The new unit will deal with the most serious national-level cybercrime and provide cybercrime support to other police forces.

2.25 The internet is borderless so many cyber attacks on the UK come from overseas. The government is working to tackle this. For example, it is seeking to influence the international community through its involvement in cyber security conferences, including in London and Budapest in 2011 and 2012, and by providing cyber security advice to other countries. It is also working with other countries to cooperate more on law enforcement to catch cybercriminals and with internet governing bodies and internet service providers to improve internet security. However, we found that this work relies on a small number of highly skilled people. The government told us they were working to broaden and make efficient use of the available pool of talent, for example through apprenticeship schemes and the use of special police officers and reservists (Figure 5).

2.26 Most of our interviewees from government, academia and industry said that existing legislation was adequate to tackle cybercrime, although government needs to ensure that current legislation remains applicable in the face of increasing technology change and rapidly evolving cyber threats. The Draft Communications Bill divided opinion: some interviewees doubted it would have much impact on serious organised crime, while others said it was essential for fighting cyber criminals and protecting the UK. In December 2012, the Joint Committee on the Draft Communications Data Bill published its report and concluded that the draft bill needed to be 'significantly amended' to deliver only necessary data that law enforcement required.[39]

2.27 The formation of a specialist cybercrime capability was welcomed by everyone. However, they also stressed the need for government to do more to increase public awareness of safe behaviour on the internet. The government has said it intends to roll-out a significantly expanded programme of public awareness drives from spring 2013. This will be delivered in partnership with the private sector. The aim is to increase cyber confidence and measurably improve the online safety of consumers and small and medium-sized enterprises. There were different views on the role of the internet service providers: some considered that they should be responsible for providing greater protection for their customers while others said it should be left for customers to decide.

Getting government to become more agile and joined-up

Keeping pace with the evolving threats facing the UK and being able to respond in a fully joined-up and agile way – especially when resources are stretched and skills are in short supply

2.28 Successfully implementing this strategy with such broad aims, requires many government organisations to work together effectively, many for the first time. Given the increasing threat from cyberspace, these organisations need to develop roles and relationships among themselves and with industry quickly.

2.29 Cyber threats are continuously evolving and the pace of technology change is rapid, so the government needs to be agile to adapt to this dynamic environment. This will mean a culture change for many departments and being more open, sharing information, working with others and communicating in different ways, including on related cross-government strategies such as those on digital, transparency and ICT.

2.30 Those we interviewed from academia and industry were positive about government efforts to work with industry on cyber security as it demonstrated a more joined-up approach. Many acknowledged the progress government had made during 2012 in working together across departmental and agency boundaries to coordinate activities and messages about cyber security. Nevertheless, it was emphasised that efforts to coordinate and strengthen leadership should continue to be a priority. For example, several people spoke about the need to for all government websites to provide links to the 'Get Safe Online' website as the single source of cyber advice and information.

2.31 Interviewees also stated that the government needed to demonstrate the progress it was making in applying the cyber advice and guidance, it gives to business, to improving the protection of its own systems and data. This was considered necessary for government to maintain its leadership role and engagement with business and the public.

Assessing value for money

Having strong management and decision-making in place to demonstrate success and provide accountability across many different organisations delivering a broad range of activities

2.32 For the government to protect and promote the UK in cyberspace, it needs to be able to measure and demonstrate the success of its strategy. However, demonstrating the optimal use of resources on cyber security may not be easy in terms of measuring outcomes when the desired result is for nothing to happen. In addition, if cyber attacks do not occur, it does not necessarily follow that it was because of programme investment or activity.

2.33 Although it is difficult, the government has demonstrated it is possible to measure value for money from similar activities to cyber security delivered by different organisations such as those related to counterterrorism. For example, in this case the government has stated that it intends to assess the progress of its counterterrorism strategy, known as CONTEST, against a set of performance indicators, complemented by evaluating specific programmes.[40]

2.34 OCSIA has identified the benefits of the National Cyber Security Strategy and has work under way to measure them. The approach taken is to develop a logical relationship between strategic objective and strategic benefit, activities under way, deliverables committed and measurable benefits. The strategic benefits build on government's description of what success of the strategy will look like in 2015, as shown in paragraph 1.10. Measurable benefits are being designed to meet four criteria: accurate, reliable, credible and readily available from public or government sources, at low cost. A pragmatic process is also being agreed for benefit owners to forecast and report on benefits realisation through the established governance structure (Figure 3) so that the Cyber Delivery Management Group can focus on red or amber rated benefits.

2.35 To support government efforts in demonstrating its success, we set out our thinking on an approach assessing the value for money of the cyber security strategy in the Annex.

Annex

Assessing the value for money of cyber security

1 This annex sets out roles and responsibilities in relation to measuring and demonstrating value for money. We set out the key steps the government should consider in seeking to achieve this; discuss some of the particular challenges in assessing the value for money of the government's cyber security strategy; and make some observations on government's progress to date.

Value for money and the role of government and the NAO

2 The HM Treasury publication, *Managing Public Money*, states "government departments are responsible for efficiency, economy, effectiveness and prudence in the administration of public resources, to deliver value for money. This means departments ensuring that procurement, projects and processes are systematically evaluated and assessed to provide confidence about suitability, effectiveness, prudence, quality, good value and avoidance of error and other waste."[41]

3 *Managing Public Money* also explains that the C&AG's role is to examine and report to Parliament on the delivery of value for money by government through assessing the economy, efficiency and effectiveness with which government deploys public money in selected areas of public business.[42] We, in common with the Treasury, define good value for money as "*the optimal use of resources to achieve the intended outcomes*".

Key steps in establishing value for money

4 We have set out the following key steps for establishing value for money. This draws on HM Treasury guidance on evaluation for Central Government in the Magenta Book[43] and our own analytical framework for assessing value for money. It also draws on our experience of how similar cross-departmental strategies, for example on counterterrorism and on tackling problem drug use, have been, or are being, evaluated.

- **Define what good looks like.** The first step is to define what will constitute success, in terms of outputs and outcomes, and at which points in time. Although the definition of value for money above refers to the 'optimal' use of resources, in practice this will be interpreted differently in light of the particular circumstances.

- **Identify and collect the data and evidence required, including on resources.** This requires clarity on the 'logic chain' of the intervention or strategy – how the inputs, activities and outputs will link together to deliver the desired outcomes. It is particularly important to agree a robust process for collecting reliable and timely information on expenditure, both for project management and accountability purposes.
- **Decide comparators and evaluate performance.** The third key step is to consider the range of possible comparators or benchmarks against which success will be assessed, and establish the evaluation arrangements accordingly. The first step above will have established the 'internal' benchmark for assessing success. But progress and success can also be assessed relative to:
    - baseline performance before the intervention or strategy;
    - what is happening in other (similar) countries; and
    - counterfactual scenarios that try to establish what would have happened without the intervention of strategy, perhaps by modelling.[44]

Assessing the value for money of cyber security

5 We recognise that there are some challenges in establishing the value for money of cross-government strategies such as the cyber security strategy, where success depends on many disparate players and factors outside the control of the government.

6 On the value side, there is the conceptual problem that success will be in terms of events not happening. If cyber attacks do not occur, it will be difficult to establish the extent to which that was due to the success of the strategy and its implementation rather than because of other factors. Assessing how different components of the strategy have contributed to the overall success of it is also a challenge. Moreover, even if the contribution of the strategy and its components can be identified, there is then the challenge of assigning a value to that outcome, to set against the cost of the strategy.

7 On the cost side, the challenges are more practical than conceptual. First, the majority of spend is classified. Second, the non-classified expenditure is channelled through many different organisations for many different types of activities. Third, to the extent that existing financial and management reporting systems do not generate the required information on expenditure, effective reporting arrangements will have to be put in place.

Some observations

8 To establish the value for money of the cyber security strategy, there are precedents and similar examples, which can be drawn upon, as well as government guidance such as the *Magenta Book*. We would highlight two instances, related to counterterrorism and preventing drug use:

- On counterterrorism, the government has stated that it intends to assess the progress of CONTEST, its counterterrorism strategy against a set of performance indicators, complemented by evaluating specific programmes.[45]
- On the drugs strategy, the Committee of Public Accounts recommended that the Home Office should publish annual reports on progress against the strategy's action plan, setting out expenditure on each measure, the outputs and outcomes delivered, and progress towards targets.[46] *Estimating the crime reduction benefits of drug treatment and recovery*, was published by the National Treatment Agency in May 2012 to address the Committee's recommendation.[47]

9 Our own work on regulation in the UK also provides examples of measuring performance in a similar area. In our report on Ofcom we developed a 'sphere-of-influence' model to recognise that Ofcom has more direct control over some areas (for example, its own management and use of resources) than others (such as complaints from consumers).[48] In the case of cyber security, government similarly has different levels of influence. For example it has more control over UK law enforcement than the activity of the private sector or other countries.

10 In terms of the three key steps outlined in paragraph 4, we have noted some progress already made by the cyber strategy, and some areas, which require further attention.

- **Define what good looks like.** The government has articulated what success will look like at the end of the programme for the UK, as shown in paragraph 1.10. For example, it has defined high-level outcomes such as individuals knowing how to protect themselves from crime online; businesses operating securely in cyberspace; and the UK having a growing international market in cyber security products and services. The next step will be to identify potential comparative measures of good performance against which to judge whether these success factors have been met. As noted in paragraph 2.34, the government has this work in hand.

- **Identify and collect the data and evidence required, including on resources.** In its strategy, the government set out the activities to be delivered and committed to reporting progress against these activities on an annual basis. In December 2012, the government reported on progress against the objectives of the strategy including work completed and spend to date. It also reported on its forward plans for implementing the strategy. Given the cross-government nature of the strategy, it will also be important for the government to provide an assessment of the success of joined-up working.
- **Decide comparators and evaluate performance.** The government has articulated its 'internal' comparator, in terms of intended outcomes, outputs and activities. The next step is to consider other potential comparators and benchmarks, and the evaluation approach more generally. In the case of its counterterrorism strategy, the government aims to commission a small number of evaluations of key programmes, focusing on those which are judged most important to its mission on counterterrorism and which attract the greatest investment. The Department for Culture, Media and Sport has also developed an evaluation approach for the Olympics, which will integrate a number of separate evaluations of different aspects of the overall programme.[49]

Appendix One

Our audit approach

1 This landscape report examined the government's implementation of the UK cyber security strategy, which it published in November 2011. This was an early review of the strategy as the government will not implement it in full until 2015. We examined:

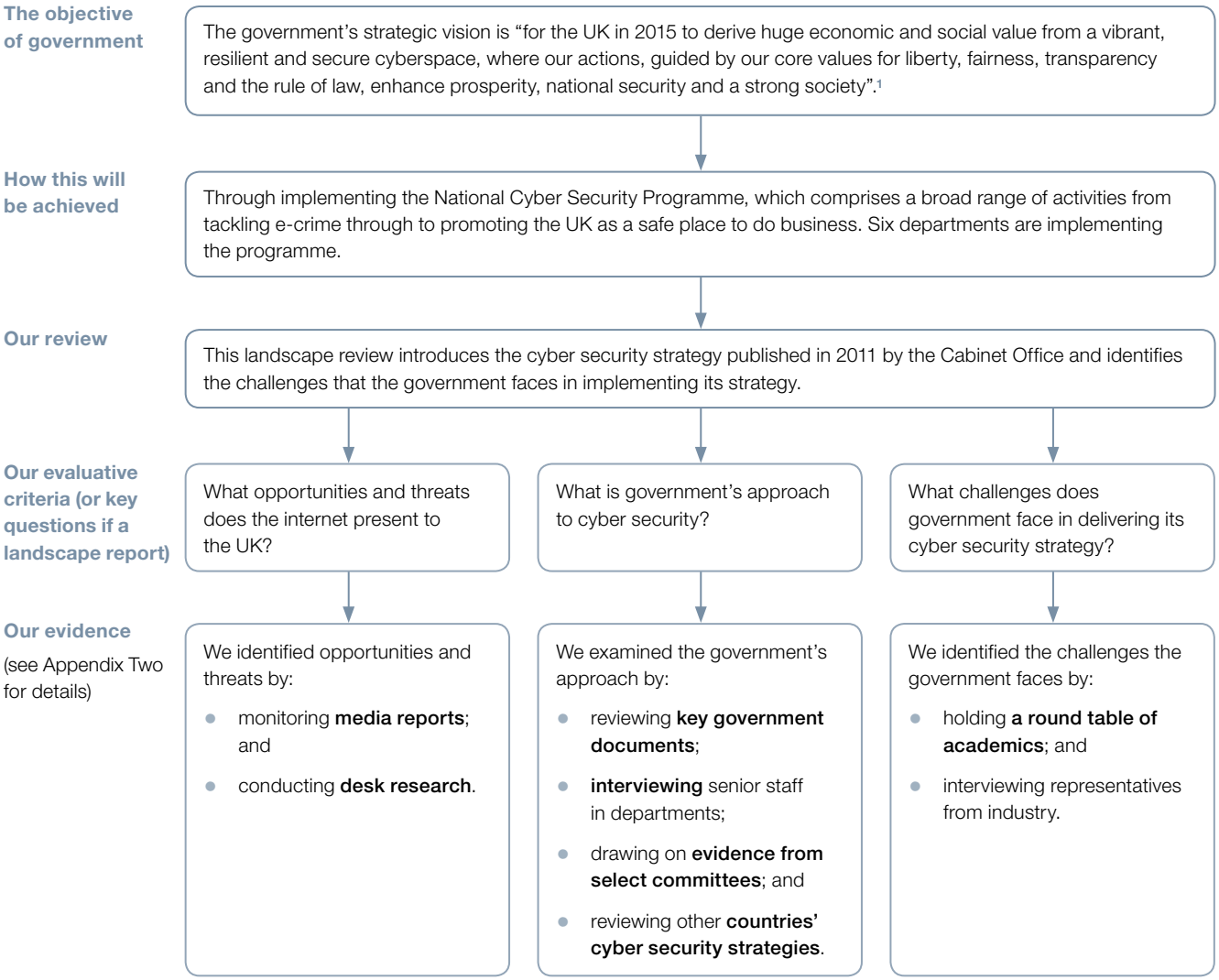
- the rationale for the government developing an approach to cyber security given the current opportunities and threats;
- the details of the strategy and the progress that the government is making in implementing the strategy; and
- the challenges the government faces in delivering the strategy.

2 We have also set out in an annex guidance for government on measuring the value for money of its cyber security programme.

3 Given the sensitivities of this area, we did not set evaluative criteria for judging the success of the strategy as it is at an early stage. Our report is a landscape review and does not conclude on the value for money of the strategy.

4 Our audit approach is summarised in **Figure 8**. We describe our evidence base in Appendix Two.

Figure 8
Our audit approach



NOTE

1 Cabinet Office, *UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. November 2011.

Appendix Two

Our evidence base

1 Our review of the UK's Cyber Security Strategy was completed following our analysis of evidence collected between July and October 2012.

2 Our audit approach is outlined in Appendix One.

3 To support our review we appointed Deloitte, one of our Strategic Partners, to prepare an early draft of a report, which provided a basis for our interviews with government during fieldwork. We then developed this report based on the evidence we collected.

4 We examined why cyber security is important to the UK.

- We monitored **the media on a daily basis** to keep up to date with cyber-related incidents such as attacks on organisations and individuals; and also announcements from government on the progress in delivering the strategy, including for example its launch of new initiatives to address cyber security.
- We conducted **desk research** of both UK and international reports from government and private sector on the digital economy, the growth of the internet and on cyber attacks, to identify the opportunities and threats the internet presents to the UK.

5 We examined the government's approach to cyber security and in particular the details of the UK Cyber Security Strategy published in November 2011 and progress to date.

- We reviewed **key government documents** including the National UK Cyber Security Strategies in 2009 and 2011.
- We interviewed **senior staff in eight departments and agencies** with responsibilities for delivering elements of the strategy to understand their roles and responsibilities; details of the activities for which they were responsible; and the challenges they faced in delivering the activities.
- We drew on **evidence from select committees**, which had previously examined elements of the government's approach to cyber security, including the Intelligence and Security Committee; the Defence Select Committee; and the Committee of Public Accounts.

- We reviewed **the cyber security strategies of other countries** including USA, and Australia as well as the reviews from the Supreme Audit Institutions in each of those countries to identify lessons on delivering similar strategies.

6 We identified the challenges government faces in implementing the strategy:

- We held **a round table of academics** from eight universities, who are experts in cyber security. We discussed their response to the government's strategy and asked them to identify the key challenges the government faced in delivering the strategy.
- We interviewed six **representatives from industry** including from the banking, defence and security, and ICT sectors.
- We also drew on the evidence from our interviews with **senior staff in eight departments and agencies.**

Endnotes

1 Boston Consulting Group, *The $4.2 Trillion Opportunity*, March 2012.

2 Boston Consulting Group, *The Connected World*, January 2012.

3 Cabinet Office. *UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*. November 2011.

4 See endnote 1.

5 Kaspersky Security Bulletin, Statistics 2011.

6 Lord Mayor's annual defence and security lecture, *The Olympics and Beyond,* June 2012, available at: www.mi5.gov.uk

7 Foreign Secretary speech, *Budapest Conference on Cyberspace*, October 2012, available at: ukingermany.fco.gov.uk

8 Detica and the Cabinet Office, *The Cost of Cyber Crime*, February 2011.

9 Cambridge University, *Measuring the Cost of Cyber Crime*, June 2012.

10 Available at: www.number10.gov.uk/news/cyber-security-strategy

11 See endnote 3.

12 House of Lords European Union Committee, *Protecting Europe against large-scale cyber-attacks*, Fifth Report, 9 March 2010.

13 House of Commons Science and Technology Committee, *Malware and cybercrime*, Twelfth Report of Session 2010–2012, HC 1537, 2 February 2012.

14 House of Commons Defence Select Committee, *Defence and Cyber-Security*, Sixth Report of Session 2012-13, HC 106, 9 January 2013.

15 Intelligence and Security Committee, *Annual Report 2011-12*, July 2012.

16 HC Committee of Public Accounts, *Information and Communications Technology in government*, Fortieth report of Session 2010–2012, HC 1050, June 2011.

17 HC Committee of Public Accounts, *Preparations for the roll-out of smart meters*, Sixty-third Report of Session 2010–2012, HC 1617, January 2012.

18 Cabinet Office, *Progress against the Objectives of the National Cyber Security Strategy*, December 2012.

19 HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Cm 7593, October 2010.

20 HM Government, *Securing Britain in an Age of Uncertainty: Strategic Defence and Security Review*, Cm 7948, October 2010.

21 See endnote 3.

22 Cabinet Office, *Progress against the Objectives of the National Cyber Security Strategy*, December 2012, available at: www.cabinetoffice.gov.uk

23 Cabinet Office, *The UK Cyber Security Strategy Report on progress – December 2012. Forward Plans*, available at: www.cabinetoffice.gov.uk

24 Booz Allen Hamilton and the Economist Intelligence Unit, *The Cyber Power Index 2012*, January 2012, available at: www.cyberhub.com

25 See endnote 9.

26 See endnote 8.

27 PricewaterhouseCoopers, *Global Economic Crime Survey 2011 – UK report*, November 2011.

28 Department for Business, Innovation and Skills Press Release, *The UK's most senior business leaders are getting new advice on how to better tackle the growing cyber threats to their companies*, 5 September 2012, available at: news.bis.gov.uk

29 Cabinet Office, *Government ICT Strategy*, March 2011.

30 Speech by Minister Chloe Smith at the Cyber Security Summit on 6 November 2012.

31 Business Technology, *Getting serious about security*, 8 April 2012.

32 See endnote 15.

33 ONS, *Internet Access – Households and Individuals, 2011*, August 2011.

34 See endnote 33.

35 See endnote 15.

36 SplashData Press Release, *Worst Passwords of 2012 – and How to Fix Them*, 23 October 2012, available at: www.splashdata.com

37 See endnote 13.

38 Ofcom, *Children and Parents: Media Use and Attitudes Report*, 23 October 2012.

39 House of Lords, House of Commons, Joint Committee on the Draft Communications Data Bill, *Draft Communications Data Bill*, Session 2012-13, HL Paper 79, HC 479, December 2012.

40 HM Government, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, Cm 8123, July 2011.

41 HM Treasury, *Managing Public Money,* May 2012.

42 See endnote 41.

43 HM Treasury, *Magenta Book: Guidance for Evaluation*, April 2011.

44 The Magenta Book provides extensive guidance on different approaches to, and techniques of, evaluation.

45 See endnote 40.

46 HC Committee of Public Accounts, *Tackling problem drug use*, Thirtieth Report of Session 2009-10, HC 456, April 2010.

47 The National Treatment Agency for Substance Misuse, *Estimating the crime reduction benefits of drug treatment and recovery*, May 2012.

48 Comptroller and Auditor General, *Ofcom – The effectiveness of converged regulation*, Session 2010-11, HC 490, National Audit Office, November 2010.

49 The Department for Culture, Media and Sport, *London 2012 meta-evaluation*, available at: www.culture.gov.uk/what_we_do/research_and_statistics/7605.aspx

Design and Production by
NAO Communications
DP Ref: 10057-001

This report has been printed on Evolution Digital Satin and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.

National Audit Office

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, telephone, fax and email
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/general enquiries: 0870 600 5522
Order through the Parliamentary Hotline
Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Houses of Parliament Shop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/general enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

TSO@Blackwell and other accredited agents

£16.00

ISBN 978-0-10-298128-5

9 780102 981285