National Audit Office

Report
by the Comptroller
and Auditor General

Cabinet Office

Update on the National Cyber Security Programme

HC 626 SESSION 2014-15 10 SEPTEMBER 2014

Our vision is to help the nation spend wisely.

Our public audit perspective helps Parliament hold government to account and improve public services.

The National Audit Office scrutinises public spending for Parliament and is independent of government. The Comptroller and Auditor General (C&AG), Sir Amyas Morse KCB, is an Officer of the House of Commons and leads the NAO, which employs some 820 employees. 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 £1.1 billion in 2013.

National Audit Office

Cabinet Office

Update on the National Cyber Security Programme

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 9 September 2014

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

Sir Amyas Morse KCB
Comptroller and Auditor General
National Audit Office

5 September 2014

HC 626 | £10.00

The government continues to make good progress in implementing the £860 million National Cyber Security Programme, which is helping to build capability, mitigate risk and change attitudes, as well as taking advantage of opportunities for economic growth.

Links to external websites were valid at the time of publication of this report. The National Audit Office is not responsible for the future validity of the links.

10510 09/14 NAO

Contents

The National Audit Office study team consisted of:
Gary Mogaji and Christopher Grant, under the direction of Tom McDonald.

This report can be found on the National Audit Office website at www.nao.org.uk

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/contact-us

Website: www.nao.org.uk

Twitter: @NAOorguk

Summary

The National Cyber Security Programme

1 The government's National Cyber Security Programme (the Programme) has a budget of £860 million and is running from April 2011 to March 2016. It has 4 objectives:

- Tackling cyber crime and making the United Kingdom one of the most secure places in the world to do business.
- Making the United Kingdom more resilient to cyber attack and better able to protect our interests in cyberspace.
- Helping to shape an open, vibrant and stable cyberspace which the United Kingdom public can use safely and that supports open societies.
- Building the United Kingdom's cross-cutting knowledge, skills and capability to underpin all our cyber security objectives.

2 A small programme team in the Office of Cyber Security and Information Assurance, in the Cabinet Office, manages the Programme. The team reports to the Deputy National Security Adviser, who is the Senior Responsible Owner for the Programme. The Cabinet Office allocates resources to delivery partners across the public, private and third sectors.

Background to our work

3 In November 2011, the government published the UK Cyber Security Strategy.[1] Since then, it has published 2 progress reviews, in December 2012 and December 2013, and several supporting documents. In February 2013, we published our landscape review of cyber security.[2] We described what different parts of government were doing to implement the Cyber Security Strategy and identified the challenges they faced in doing so.

4 Using our review, the Committee of Public Accounts held a hearing on 13 March 2013 on the subject of cyber security and took evidence from Cabinet Office officials. After the hearing, the Committee's Chair wrote to the Cabinet Office. The Chair noted 5 key challenges for government and asked us to give an update of the Programme after the government's next planned review. This report is our response.

[1] The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, November 2011, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[2] Comptroller and Auditor General, *The UK cyber security strategy: Landscape review*, Session 2012-13, HC 890, National Audit Office, February 2013, available at: www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

5 The evidence for this report is based on semi-structured interviews with Programme staff and delivery partners, financial analysis and document review, interviews with industry representatives, a round-table discussion with academics and a short survey of 34 stakeholders engaged with the Programme.[3]

Key findings

6 Overall, the government continues to make good progress in implementing the Programme, which is helping to build capability, mitigate risk and change attitudes, as well as taking advantage of opportunities for economic growth. But cyber threats continue to evolve and the government must increase the pace of change in some areas to meet its objectives. The government also needs to decide which initiatives should be mainstream activity across public sector organisations and which require the impetus and coordination that a successor programme might provide.

7 Findings in specific areas are as follows:

- The Programme's financial management and governance mechanisms are strong, and have improved over the Programme's life to date. The Programme is on track to spend its budget of £860 million by March 2016.
- The government has made good progress in improving its understanding of the most sophisticated threats to national security. This area scored the highest rating in our survey. However, there is a varied understanding of threats to wider public services.
- The government has made some progress in encouraging businesses and citizens to mitigate risks, particularly in getting larger companies to take action. It has had a limited impact with SMEs, where it has struggled to communicate guidance in a way that meets those businesses' needs.
- While UK cyber exports have increased by 22% between 2012 and 2013, progress in encouraging trade and exports in cyber products and services has been slow and is the area of poorest performance, scoring the lowest rating in our survey. The government's marketing strategy was delayed by 14 months and it has only recently agreed a methodology to measure progress towards the £2 billion export target announced at the end of 2013.
- The government has encouraged many education and training initiatives to stimulate the development of relevant skills but demand for those skills remains considerable.
- Cabinet Office is managing the Programme effectively but cannot yet demonstrate a clear link between the large number of individual outputs being delivered and an overall picture of benefits achieved. However, this challenge must be set against the inherent difficulty of measuring how safe the United Kingdom is in cyberspace.

[3] We asked those responding to our survey to rank performance in each area of the Programme with a score between 1 and 5, where 1 = very poor performance and 5 = excellent performance. Further detail on this survey is contained in Appendix One.

Part One

Financial management

1.1 Financial management of the National Cyber Security Programme (the Programme) is strong and has improved over the Programme's life to date. The Programme is on track to spend its allocated total of £860 million by March 2016.

Programme budgeting

1.2 In the 3 full financial years since the Programme started in 2011-12, it has spent £434.1 million. This spending has been allocated to the strands of work set out in **Figure 1**. As set out in **Figure 2** on page 8, the Cabinet Office has allocated a further £219.9 million in 2014-15 but expects to spend around £210 million once it has made further in-year decisions on the Programme.

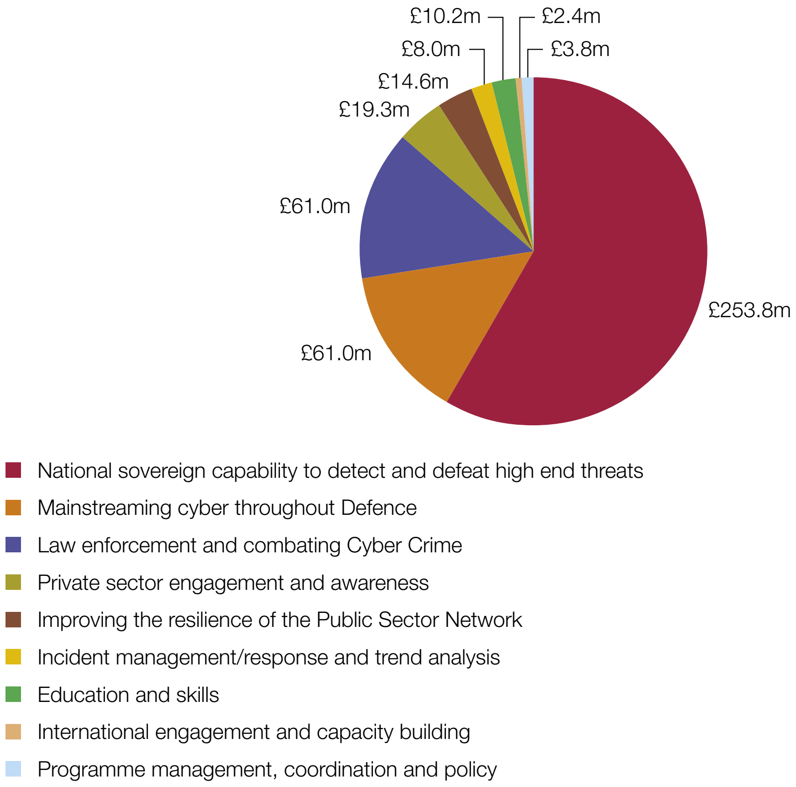
1.3 The Cabinet Office has managed its total budget of £860 million well, with annual expenditure kept within control totals. Annual budgets and actual expenditure by year are set out in **Figure 3** on page 8 which shows that expenditure is rising in line with planned budgets.

1.4 HM Treasury originally allocated £650 million for the Programme. In 2013, it allocated a further £210 million as part of the spending review it undertook that year, taking the total to £860 million. This additional investment was designed to provide funding for new and existing projects to 2015-16, but also demonstrated HM Treasury's confidence in the Cabinet Office's ability to allocate resources effectively.

1.5 In addition to the £860 million total Programme budget, departments and agencies continue to allocate funding from their operational budgets to cyber security. The figure of £860 million therefore does not include spending in support of cyber objectives that the National Cyber Security Programme does not fund. Due to the lack of cyber as a separately identifiable figure in departmental budgets and the difficulties in classifying cyber from general IT expenditure, there is no readily quantifiable measure of the whole of government's spend on cyber security.

Figure 1

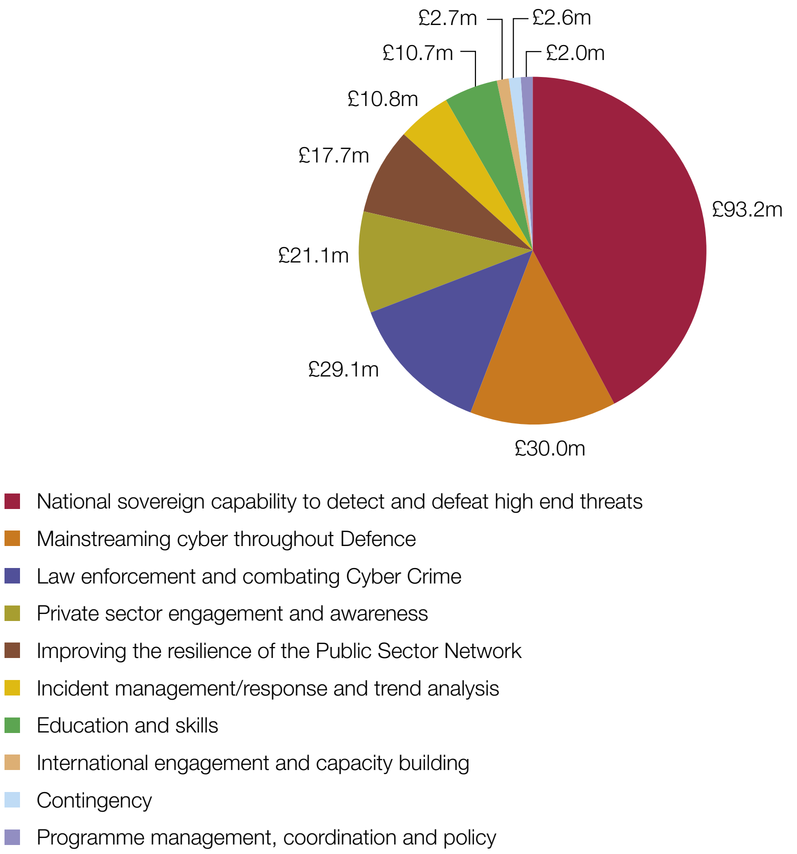
Total Programme expenditure for Years 1 to 3



Source: Cabinet Office

Figure 2

Proposed allocation of Programme expenditure for Year 4



Source: Cabinet Office

Figure 3

National Cyber Security Programme expenditure

Financial year	Budget (£m)	Actual expenditure to date (£m)
2011-12 (Year 1)	105	103.1
2012-13 (Year 2)	155	151.2
2013-14 (Year 3)	180	179.8
2014-15 (Year 4)	210	n/a
2015-16 (Year 5)	210	n/a
Totals	**860**	**434.1**

Source: Cabinet Office

1.6 HM Treasury reduced its original allocation for 2011-12 (Year 1) from £120 million to £105 million. It subsequently revised its allocation for 2012-13 from £140 million to £155 million, although the Programme only spent £151 million. These differences arose largely because of under-spending by delivery partners, some of which emerged late in the year.

1.7 Learning from this experience, the Cabinet Office worked closely with partners who were responsible for underspends and increased the level of over-programming to mitigate the effects of any future underspends. As a result, Year 3 expenditure was within 1% of the allocated budget.

Changes to allocations

1.8 Cabinet Office allocations to individual delivery partners have fluctuated over time, for the following reasons:

- Allocations within the Programme have evolved to reflect the maturity and effectiveness of projects. Initial allocations were based in part on delivery partners' sometimes limited ability to spend money effectively. Now that this has improved, the Cabinet Office has been able to tailor allocations more closely to objectives.
- The Cabinet Office has sometimes increased allocations once delivery partners have proved their ability to spend money effectively.

1.9 We heard from a wide range of delivery partners that the Cabinet Office controlled expenditure tightly, in some cases, more so than their own organisations' finance or approvals functions. They also noted that the Cabinet Office clearly linked approvals for further funding to the track record of results that each organisation had already delivered, creating clear expectations for delivery partners.

1.10 The Cabinet Office has not yet made any specific funding commitments beyond 2014-15. In prior years, the Cabinet Office has entered into multi-year commitments but wants to ensure that for 2015-16 that funds can be allocated flexibly to the highest priorities. It has invited delivery partners to indicate if the lack of multi-year commitments is constraining their delivery plans and, where this is the case, is prepared to provide approval in principle.

1.11 In the absence of agreed plans for the future of the Programme as a whole, the Cabinet Office has no plans for further expenditure beyond the expected allocations for 2015-16.

Part Two

Understanding the threat

2.1 The cyber threat is diverse and continues to evolve rapidly. Threats come from a range of actors including hostile states, state-sponsored organisations, serious organised crime groups and hacktivists, some of whom are developing their tactics and capabilities rapidly. The government has made good progress in improving its understanding of the most sophisticated threats to national security, but there is a varied picture of threat understanding across the public and private sectors.

Threat information

2.2 In 2013-14, the government spent £86.6 million on its technical capability to detect and defeat the most sophisticated threats. This equates to just under half the Programme's expenditure that year. Despite investment in capability to understand the threat, the latter is evolving rapidly and remains a source of considerable challenge. The government has established the Centre for Cyber Assessment to produce analysis of cyber threats, bringing together its understanding from a range of sources into one place.

2.3 In addition, GCHQ has invested in new technologies, skilled people and technical infrastructure that increase the government's ability to defend and protect the United Kingdom against these increasingly sophisticated threats. These capabilities support and inform a wide range of the government's work on cyber security, including tackling cyber crime and protecting critical national infrastructure.

2.4 From those interviewed, it is clear that there is a belief across all sectors – government, academia and industry – that there is a good understanding of the threat by central government, with an average rating of 3.7 out of 5 in our survey of stakeholders. But this understanding diminishes the further away organisations are from the centre. Stakeholders believe that central government departments unused to dealing with national security or fraud-related threats and NHS and local government organisations have a more varied, but limited understanding of the threat and they do not yet understand what would represent an appropriate level of threat protection.

2.5 In mitigation, the Cabinet Office has provided additional support to those departments at the greatest risk of fraud such as HM Revenue & Customs and Department for Work & Pensions. In addition, it has widened the number of central government departments participating in the Programme in 2014-15, allocating resources to new delivery partners such as the Department for Transport, the Department of Health and the Department for Environment, Food & Rural Affairs, to support their ability to understand and deal with threats. In addition, the majority of local authorities and public authorities have now met Public Services Network local connection standards, with 80% due to be on the Network by 2016.[4]

2.6 Levels of observed cyber crime continue to increase as enabling tools are more freely available to criminals. In addition, cyber capability is increasingly an enabler for a wider range of criminal activity. In response, the government placed a renewed focus on tackling cyber crime as part of its Serious and Organised Crime Strategy published in 2013.[5] Despite the establishment of the National Crime Agency's National Cyber Crime Unit and 9 Regional Organised Crime Units, these organisations do not yet have enough qualified personnel and technical capability to deal with such a fast-moving threat. In mitigation, the Programme is funding further recruitment, training and development of staff.

2.7 Rapid developments in the use of the internet and digital technology, such as the internet of things, smart cities, energy monitoring and distribution and transport applications, mean that the basic threshold for what needs protecting keeps on changing. As government increasingly delivers services through digital channels, its exposure to threats will increase accordingly.

Communication and coordination

2.8 The Cabinet Office has brought into being a number of organisations and initiatives designed to improve the communication and coordination of cyber security threat activity, of which 2 are likely to have the most effect on helping the United Kingdom to deal with the threat: the UK Cyber Emergency Response Team (the CERT) and the Cyber Information Sharing Partnership (CISP), which is now part of the CERT.

2.9 In March 2014, the Cabinet Office established the CERT to manage national cyber critical incidents and to act as the key point of contact between government, the private sector, academia and international counterparts. It is too early to judge the effectiveness of the CERT, but most stakeholders agree that it is in principle a good idea and that success will likely depend on building relationships with industry and other countries' CERTs. There is, however, some reluctance from many companies to share information about breaches, unless forced by regulators or legislation, because of the potential impact on their reputations.

[4] The Public Services Network is run by the Government Digital Service, with support from GCHQ. Its objective is to unify the provision of network infrastructure across the United Kingdom public sector into an interconnected network or networks to increase efficiency and reduce expenditure. The Network is also designed to improve security and governance arrangements.

[5] Serious and organised crime strategy, available at: www.gov.uk/government/publications/serious-organised-crime-strategy

2.10 The government's Cyber Information Sharing Partnership has a longer track record than the CERT, having been established in February 2013. It now has over 500 member organisations, with numbers continuing to grow at a steady rate. Both government and industry believe that there could be many more members actively involved and that this would increase its reach and effectiveness. Supporting this view, the 2014 InfoSec survey found that 67% of information security professionals thought intelligence was not shared effectively between government and industry.[6]

2.11 Alongside these 2 organisations, the government as a whole has now begun to make progress in understanding the threat from cyber-related fraud. This is because, until recently, the police, the Action Fraud organisation and other organisations receiving fraud reports were unable to gather an integrated picture of fraud. The Home Office has recognised the need to improve the end-to-end reporting system to join up intelligence-gathering and reporting with action to investigate crimes and resolve them to the satisfaction of victims and is considering how to do so. For example, Action Fraud, using the National Fraud Segmentation, have assessed the different types of threat and the vulnerability of different parts of the UK population to them.

2.12 There is a range of views about how best to communicate news of threats and how business and individuals should respond. The Programme's own January 2014 Cyber Security Communications Plan does not set out the strategic allocation of roles clearly and, so far, ministers, GCHQ, the CERT and websites such as Cyber Streetwise and Get Safe Online have all played roles.[7] Many stakeholders noted that it would be helpful for government to have a single, identifiable individual who could communicate to industry and the public in the event of a threat.

2.13 The challenge of communicating effectively on cyber security issues was illustrated by the National Crime Agency's (the NCA's) June 2014 announcement of a 2-week opportunity to deal with 2 forms of malware known as CryptoLocker and GOZeuS. The NCA gave only generic advice to the public but directed them to the Get Safe Online website where diagnostic tools were available. Although this intervention was successful in drawing attention to the situation, the volume of traffic that followed meant that the website collapsed. Some members of the public were therefore temporarily unable to access the planned channel for official advice. The NCA responded by advising people to go to the Get Safe Online social media sites or the CERT.[8] Following this experience, Get Safe Online has increased the capacity of their website in order to deal with such incidents.

[6] Survey findings, available at: www.infosec.co.uk

[7] Available at: www.getsafeonline.org; www.cyberstreetwise.com

[8] Available at: www.nationalcrimeagency.gov.uk/news/news-listings/386-two-week-opportunity-for-uk-to-reduce-threat-from-powerful-computer-attack

2.14 The final strand involved in dealing with cyber threats is international, where the United Kingdom has continued to work with bilateral and multilateral partners to address the international dimensions of the problem. The Foreign & Commonwealth Office has provided guidance and assistance, including financial support, to cyber crime initiatives in the Commonwealth, the United Nations Office on Drugs and Crime and the Council of Europe. It has also participated in activities in the UN General Assembly, the Organisation for Security and Cooperation in Europe, the European Commission and NATO to support its objective of an open, vibrant and stable cyberspace that supports open societies.

Part Three

Encouraging businesses and citizens to mitigate risk

3.1 The Programme has spent £12.4 million in 2013-14 on engagement with the private sector and the public, via the Home Office, the Department for Business, Innovation & Skills and other delivery partners, with plans to spend around £21.1 million in 2014-15. The Programme's objectives in this area have been to improve awareness of the cyber threat among business and the public, reduce the number of attacks on businesses, ensure a coherent approach across government and work with those responsible for critical national infrastructure to improve protection.

3.2 The government has made some progress in encouraging business and individual citizens to mitigate risks, although the challenge remains considerable. Our survey of stakeholders revealed that the Programme was making an impact in this area, with a score across all sectors of 3.2 out of 5 with this score rising slightly to 3.4 among industry respondents. The generally expressed view was that, despite the volume of activity, there was still more to be done, given the scale and fast-moving nature of the challenge, in changing attitudes in business and people's behaviour patterns. It is difficult, however, to isolate government's contribution to changing behaviours from the commercial pressures for change that now exist in many sectors.

3.3 Larger companies have made good progress in addressing the specific risks from cyber threats, although the Cabinet Office cannot demonstrate how much of this is due to its own efforts as opposed to commercial or reputational drivers. The Financial Times' Bellwether[9] survey of FTSE 350 Company Secretaries in November 2013 found that 98% were aware of the government's 10 Steps cyber security guidance,[10] and 67% had discussed cyber security at board level

3.4 The latest FTSE 350 Cyber Governance Health Check Tracker Report,[11] published in November 2013, shows that many of the FTSE 350 companies are starting to recognise the risk from cyber on their strategic risk registers. However, this risk is not always managed at board level and in a number of cases board members lack the skills necessary to understand and address this risk appropriately.

[9] FT-ICSA Boardroom Bellwether Survey, available at: www.icsa.org.uk/products-and-services/knowledge-and-guidance/research/ft-icsa-boardroom-bellwether

[10] *10 steps to cyber security*, available at: www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets

[11] *FTSE 350 Cyber Governance Health Check Tracker Report*, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/268643/bis-13-1293-ftse-350-cyber-governance-health-check-tracker-report.pdf

3.5 In many cases funded by the Programme, there is now a range of information for business available from government produced by a range of bodies including GCHQ, the Cabinet Office, the Foreign & Commonwealth Office and the Department for Business, Innovation & Skills. In addition, the Ministry of Defence now requires its suppliers to meet the 'Cyber Essentials' standard as part of its standard contracting process.

3.6 In addition to this UK government-issued guidance, major and international businesses may be considering other industry or international standards and guidance. These include the ISO 27000 series, the new PAS 555:2013[12] and PAS 754:2014,[13] the Australian 35 Mitigation Strategies and the US National Institute of Standards and Technology Cyber Security Framework, as well as their own industry recommended standards and regulations.

3.7 Industry stakeholders were of the view that this range of advice risked confusing its intended audiences. This was especially true of the Small and Medium Enterprises (SME) community, where there is a greater need to scale the guidance to fit these smaller businesses. SMEs are often too small to employ dedicated IT staff, and the impact of breaches can be just as damaging. Both government and industry organisations are trying to solve this problem working with small business organisations and by providing more specific guidance for SMEs. These include:

- The Information Assurance for Small and Medium Enterprises' 10 steps to Cyber Security – Guidance for SMEs[14] (developed in conjunction with the Cabinet Office);
- The Institute of Chartered Accountants in England and Wales' 10 steps to cyber security for the smaller firm;[15] and
- The Department for Business, Innovation & Skills' Cyber Essentials scheme.

3.8 The latest PwC *Information Security Breaches Report*[16] shows that, while there has been a decrease in reported attacks of around a fifth for small companies (a similar fall to large companies), the financial impact of their worst reported attacks nearly doubled from £35,000–£65,000 in 2013 to £65,000–£115,000 in 2014. The equivalent impact on large businesses had increased by around a third.

[12] PAS 555:2013 Cyber security risk – Governance and management – Specification.

[13] PAS 754:2014 Software Trustworthiness – Governance and management – Specification.

[14] 10 Steps to Cyber Security – Guidance for SMEs, available at: www.iasme.co.uk/index.php/advice/10steps

[15] 10 steps to Cyber Security for the smaller firm, available at: www.icaew.com/~/media/Files/Technical/information-technology/information-security/06-cyber-security-chartech-supplement-nov-2013.pdf

[16] *Information Security Breaches Report*, PwC, 2014, available at: www.pwc.co.uk/audit-assurance/publications/2014-information-security-breaches-survey.jhtml

3.9 Another way of changing business behaviour that government has used is the Centre for the Protection of National Infrastructure, which provides protective security advice to businesses. It has made some progress in changing attitudes among larger companies, especially through its briefing team, which has given threat briefings to around 175 companies. The Cabinet Office recognises, however, that making further progress in protecting critical national infrastructure is a priority for the Programme. The principal constraints in this area are the small numbers of personnel with the right technical expertise and the limited capacity of regulators to engage with this agenda. The Cabinet Office is aware of these issues and has allocated funds in 2014-15 to address this, with the intention of allocating further funds in 2015-16.

3.10 The government has tried to supplement its work with industry with initiatives aimed at increasing cyber awareness of citizens. According to the tracker put in place by the Home Office to measure the impact of the Cyber Streetwise campaign, this is having some impact. Sixty-five per cent of citizens are now undertaking at least 10 of the 17 recommended cyber security behaviours, an increase of 2% in the first 6 months of the campaign and setting a trajectory which the Home Office believes will allow it to achieve its original target of a 4% to 5% shift in consumer behaviour by April 2015.

3.11 This is contrasted by the lack of impact of this campaign among SMEs who have remained at 8% undertaking 10 or more of the 14 cyber security behaviours. This lack of movement may be due to SMEs investing their limited resources into meeting the behaviours that are most critical to their business. While the campaign appears to be raising awareness among the public, this has not yet been reflected in the actions of business.

3.12 The Home Office has indicated that they are developing a revised approach for the next phase of its Cyber Streetwise Awareness Campaign which is designed to increase its impact among SMEs. It is also hopeful that the introduction of BIS's Cyber Essential Scheme will help to increase traction and awareness among this group.

Part Four

Support to trade and exports

4.1 An important part of the Programme's strategy is to combine protection of the United Kingdom against the threats of cyber attack and cyber crime with the delivery of economic value through the productive use of cyberspace by business. Progress in encouraging exports is slow but stakeholders believe that the government's underlying approach is correct.

4.2 Of all of the 5 challenges surveyed, this is the area in which the Programme has made the least progress towards its objectives, with an average score of 2.8 out of 5 from our stakeholders. This score fell to 2.5 out of 5 among industry respondents.

Delivery to date

4.3 In 2014-15, the Cabinet Office plans to spend £0.3 million on support to exports through UK Trade & Investment (UKTI), which is the lead department for supporting trade and exports and is providing matched funding for a planned export support programme of £0.6 million. Several other departments undertake trade and export activity, including the Home Office, the Foreign & Commonwealth Office and the Department for Business, Innovation & Skills, some of whom contribute further expenditure from their own budgets.

4.4 The view from many established companies in this sector is that the government's overall approach is sound and should help increase exports towards its stated target of £2 billion. They believe that government understands the opportunities available and is providing high-level support for trade missions and trade shows where politicians' messages support industry products and services. However, they believe that implementation has been too slow.

4.5 The Cabinet Office originally intended that UKTI should have a cyber security marketing strategy in place by March 2012, but it wasn't until May 2013 – 14 months after the deadline – that UKTI published this strategy. UKTI has been slow to mobilise on the basis of this strategy and only began leading work to develop strategies for each target market from February 2014.

4.6 UKTI's efforts on cyber exports are based in their Defence and Security Organisation, whose focus tends to be on large deals with major defence and aerospace prime contractors. The Home Office's work on government-to-government deals also tends to give preference to established companies.

4.7 There is a concern among SMEs that this approach may mean that they do not get the support they need. Smaller and less established companies find it difficult to gain or fund attendance at trade fairs, often do not have the experience and resources to compete in contract negotiation processes and often lack a demonstrable track record. Acting as a subcontractor to a larger company also brings different difficulties such as retaining intellectual property and losing vetting status once a contract finishes. SMEs have the opportunity to influence policy in these areas through representation on the Cyber Growth Partnership and through TechUK, the main UK trade association for this sector.

4.8 The placement of cyber exports within UKTI's Defence and Security Organisation may also lead to a loss of opportunities in business-to-business sales where many opportunities exist for UK SMEs. A BIS-commissioned report[17] identifies the defence and intelligence cyber sub-market as the most mature but also the smallest in the UK. UKTI is recruiting staff with expertise in finance and critical national infrastructure to provide support for this sector.

Measuring success

4.9 The government has made belated progress in responding to the Committee of Public Accounts' observation that it should develop a methodology to support delivery of its export target, with the release of a national measure in July 2014. UKTI has agreed this methodology with the Cabinet Office and it is now the national measure for cyber exports.

4.10 This measure should allow the government to demonstrate progress towards its £2 billion cyber exports target. The challenge of measuring this target is potentially compounded by the difficulty in identifying sources of cyber revenue in what is an emerging and ill-defined industry. Cyber revenue may be generated as part of a much larger IT, defence or engineering and construction contract, making it difficult to split out from the contract as a whole.

4.11 Separately, there is a question over what counts as UK income from cyber exports. The nature of cyber products means that it is often possible for operations in the UK with intellectual property developed by UK employees to be owned by a foreign company. The ultimate destination for this income being generated by UK intellectual property may therefore not be the UK economy. All of these factors make accurate measurement of the target difficult.

4.12 Despite these challenges, official UK statistics show that UK cyber exports are rising and increased by 22% between 2012 and 2013. If current trends continue the UK should be on track to meet the £2 billion annual target by 2016.

[17] *Competitive analysis of the UK cyber security sector*, Pierre Audoin Consultants, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf

Part Five

Reducing the skills gap

5.1 The Cabinet Office has commissioned and coordinated a range of activities to oversee major changes in education and training, including establishing new university courses, changing school and university curricula and providing training for public servants with responsibility for information assurance. But demand for skills in both public and private sectors remains considerable and there is still uncertainty about exactly how best to prepare people for the increasingly wide range of jobs in which people need to have some understanding of cyber risks and opportunities.

Scale of the challenge

5.2 The Cabinet Office allocated £8 million in this area in 2013-14 across government, industry and academia and plans to spend around £10.8 million in 2014-15. Its objective is to encourage a balanced programme of activity across the education and training sectors to solve existing and longer-term cyber skills gaps. Given the scale of the challenge, the Cabinet Office's strategy has been to choose to fund a wide range of partners, from established organisations to new schemes.

5.3 The main risk to the delivery of skills-related objectives is that industry has yet to present a clear picture of the skillsets required, due to the immaturity and diversity of cyber as a sector. During the last year the Department for Business, Innovation & Skills has led a business engagement exercise to try to better understand the cyber security skills needs of businesses. This involved workshops with over 50 businesses and an online survey but no widespread agreement could be reached as to the technical requirements needed by business.

5.4 Without business defining the models of skills they require it is difficult to identify the gaps and begin to address them. In addition, the various professional bodies in this sector have struggled to establish agreed career and training pathways. GCHQ intends that its Certified Professional Scheme should begin to address the need for professional cyber security pathways.

5.5 It is clear from discussions with stakeholders that the cyber skills situation is complex and multifaceted. Some feel that the skills shortfall in cyber and IT more generally are part of a wider challenge to encourage more students to take Science, Technology Engineering and Mathematics (STEM) subjects. They therefore see government-funded schemes which specifically target schools and the refresh of the curriculum as the best way to solve the problem. Others believe, however, that this approach does not do enough to deliver the specific technical skills which are in such demand in the short term. In addition, as public services are increasingly delivered through digital channels, the number of general and senior managers, policy advisers and communications staff who need some knowledge of cyber issues is growing rapidly.

5.6 Most stakeholders that we spoke to believed that a multi-pronged approach to tackling the skills gap was nonetheless the right approach. Respondents gave the Programme an average score of 3.6 out of 5 in our survey. There was a belief that while some of the schemes would not be as successful as others, the sheer number of activities under way would help ensure that there was a significant increase in the cyber skills available in the medium and long term.

5.7 Major challenges remain however. The Programme risk register highlights the risk that there are not enough skilled personnel in the public sector to deliver the Programme's objectives. It notes that the public sector is losing critical staff and there is an insufficient supply of professionals to replace them. The Ministry of Defence has had some success in building capacity through large-scale general awareness training and the recruitment of cyber reservists, but, across government, there is an ongoing demand for technical specialists and managers and policy advisers who understand cyber and information assurance issues.

Effectiveness of government response

5.8 In response to these challenges, the Programme has funded a wide range of initiatives and organisations. These schemes target all elements of society from developing new cyber security teaching materials for GCSE and A-level, through developing new coding modules for use within Computer Clubs for Girls, to funding apprenticeships. These schemes will deliver some benefits in the short term, but other benefits will take longer. For example, the first PhD students from the new Centres for Doctoral Training will not graduate until 2017.

5.9 In addition, the Cabinet Office is funding activities to engage those who might not enter cyber-related employment through traditional educational routes. The Cyber Security Challenge, which is 45% funded by the Programme, is a good example of this. The Challenge consists of a series of national competitions, learning programmes, and networking initiatives, whose objective is to engage those currently outside formal employment in the cyber security profession but who might have the necessary skills to excel in this field.

5.10 The Challenge has proved popular with participants and is effective at raising awareness, although its ability to scale up its operations is not yet proven. While the early stages of the Challenge are online, the latter stages are face-to-face and require a large amount of time and logistics which may not be scalable to meet future demand.

5.11 Even in areas of the public sector where the skills requirement is clearer, there has been mixed progress in delivering training programmes. Since 2011, the National Archives has run training courses for 462 Senior Information Risk Officers and 2,170 other Information Assurance roles. Over 334,000 people have completed the 'Protecting Information' and 'Responsible for Information' online training modules.[18] The apprenticeship scheme for the intelligence community has also been successfully delivering a new cadre of people into posts and GCHQ is beginning to accredit Masters degrees at 6 universities. The training of police, however, has suffered from delays in establishing courses and a much slower take-up of officers attending than expected.

5.12 As part of its wider objectives and planning for the longer term, GCHQ has recognised and is engaging with 11 Academic Centres of Excellence at universities across the United Kingdom to enhance both the quality and scale of academic research. The Cabinet Office is also providing funding for 2 Centres of Doctoral Training to support 100 more candidates for cyber security PhDs.

[18] This figure does not include military or public sector staff who download the course on to their own systems.

Part Six

Delivering value for money

6.1 The Cabinet Office is managing the Programme effectively but cannot yet demonstrate a clear link between the large number of individual outputs being delivered and an overall picture of benefits achieved. The Cabinet Office still needs to set out which activities should become mainstream across government and which are transformational and should be led by any successor programme.

Managing the Programme

6.2 The Programme has a rigorous governance framework and the Cabinet Office has now improved the Programme's approvals process. Delivery partners submit business cases for approval by the Senior Responsible Owner and HM Treasury in order to bid for allocations. The Cabinet Office assesses the delivery of the Programme using monthly reporting and monitoring arrangements, and raises issues as appropriate through the governance hierarchy. Peer reviews of proposals and annual 'health check' exercises have helped to improve quality and capture lessons learned.

6.3 The Programme is part of the government's Major Projects Portfolio and therefore undergoes annual Major Project Authority (MPA) Gateway reviews to assess delivery confidence and ensure that it follows programme management best practice. The most recent assessment, in May 2014, awarded the Programme 'Green' status, which means that, "successful delivery of the programme appears highly likely".

Demonstrating benefits

6.4 The Programme is clearly delivering benefits under all 4 of the Programme's objectives and industry and academia stakeholders agree that this is still the correct strategy. There is also considerable international acclaim for the United Kingdom's lead in this area. Our survey respondents rated the value for money of the Programme fairly highly, with an average score of 3.5 out of 5.

6.5 Despite the creation of a complex benefits tracking tool, the Cabinet Office cannot yet demonstrate a clear link between the large number of individual outputs being delivered and an overall picture of benefits achieved. The Programme is designed to deliver 21 strategic benefits, which break down into 55 measurable benefits, each of which are supported by a different number of metrics. The total number of metrics that the Cabinet Office monitor is 256, although the frequency of reporting and underlying robustness of some of the metrics varies.

6.6 It is inherently difficult to formulate a single quantified measure of overall progress towards the Programme's ultimate objective of making the UK safer in cyberspace. The Cabinet Office therefore carries out annual 'health checks' of delivery against its strategic cyber security objectives, checking levels of ambition, and identifying areas for additional focus and increased investment. This exercise informs the annual allocation of the Programme's funds.

6.7 Given the number and wide range of delivery partners, programme delivery is managed at the working level by 7 theme-based Cyber Delivery Capability Groups; their role is to drive the delivery of their respective elements of the Programme. Their work with delivery partners has helped to drive up the quality of business cases. In the early stages of the Programme, some of these business cases were poor quality, in part because of the uncertainties involved in delivering new projects. They have now improved, and the Cabinet Office requires them to show clearly how money will be used to deliver outputs or activity which link to specific benefits.

6.8 Programme staff are working to improve benefits realisation, including trying to set out the return on investment of different work strands so that the Cabinet Office can make comparisons of the relative value for money of those strands. Some benefits are inherently difficult to demonstrate, such as expenditure to improve the capability of the intelligence agencies or the influencing work done by the Foreign & Commonwealth Office.

6.9 The Cabinet Office is therefore still dealing with some of the challenges in assessing value for money that we identified in our 2013 Landscape Review, including the difficulty of publicly assessing the value of classified expenditure and the challenge of comparing the relative benefits of such a wide range of activities and delivery partners. The Cabinet Office has recognised as a formal risk in its risk register the possibility that insufficient work is under way to deliver all the planned benefits and is working to ensure that approved activity is on track to do so.

Future value for money

6.10 The Cabinet Office recognises that the next spending review and Strategic Defence and Security Review will together set the framework for the future size and shape of any centrally coordinated work on cyber security. There is general consensus among all stakeholders that a successor programme of some kind is vital to maintain momentum and continue to build capability.

6.11 There is also consensus that the Cabinet Office needs to undertake work in advance of the spending review and Strategic Defence and Security Review processes to set out options for the future approach. In particular, the Cabinet Office should set out how any successor programme might deliver the maximum transformative effect and whether some of the current Programme's objectives can be allocated to industry, regulators, auditors, insurers and other parts of the public sector, as the handling of cyber security risks becomes more integrated into standard management activity.

6.12 Regardless of what future activity the centre of government undertakes, there is a challenge to ensure that the benefits currently planned will be monitored and delivered once the current Programme finishes. The Cabinet Office's assumption is that a successor programme would continue to monitor benefits realisation. If there were no successor programme, or if it did not have the resources to monitor benefits, the onus for benefit realisation would fall to delivery partners.

Appendix One

Our audit approach and methodology

1 The objective of this exercise was to provide an update to Parliament of progress made by the Cabinet Office in delivering the National Cyber Security Programme. In particular, we focused on those areas in which the Committee of Public Accounts had expressed an interest. The objective of this exercise was not to draw value for money conclusions, but to provide independent assurance of progress made.

2 We were unable to provide public commentary on some areas of expenditure within the National Cyber Security Programme because of levels of security classification involved. We have, however, conducted work in these areas, including file review and interviews, to satisfy our own assurance purposes.

3 We undertook semi-structured interviews with a wide range of officials responsible for running the Programme and for implementing its various projects, as well as representatives from industry and academia. Public Sector organisations involved included:

- Cabinet Office
- Department for Business, Innovation & Skills
- Department for Culture Media & Sport
- Department for Work & Pensions
- Foreign & Commonwealth Office
- Government Communications Headquarters
- HM Revenue & Customs
- Home Office
- Ministry of Defence
- UK Trade & Investment.

4 We interviewed and/or received written evidence from the following industry representatives:

- ADS
- Cyber Security Challenge
- FireEye
- The Institute of Chartered Accountants of England and Wales
- The Institution of Engineering and Technology
- The Malvern Cluster
- Lockheed Martin
- PwC
- Qinetiq
- Sophos
- Symantec.

5 We organised a round table for academics to discuss the 5 issues raised by the Committee of Public Accounts. Attendees came from the following institutions:

- Birkbeck, University of London
- Bristol University
- Chatham House
- Cranfield University
- Imperial College London
- London School of Economics
- Royal Holloway, University of London
- Southampton University.

In addition, we also interviewed academics from Oxford and Warwick Universities in separate discussions and attended a discussion of the Academic Liaison Panel of the Information Assurance Advisory Council.

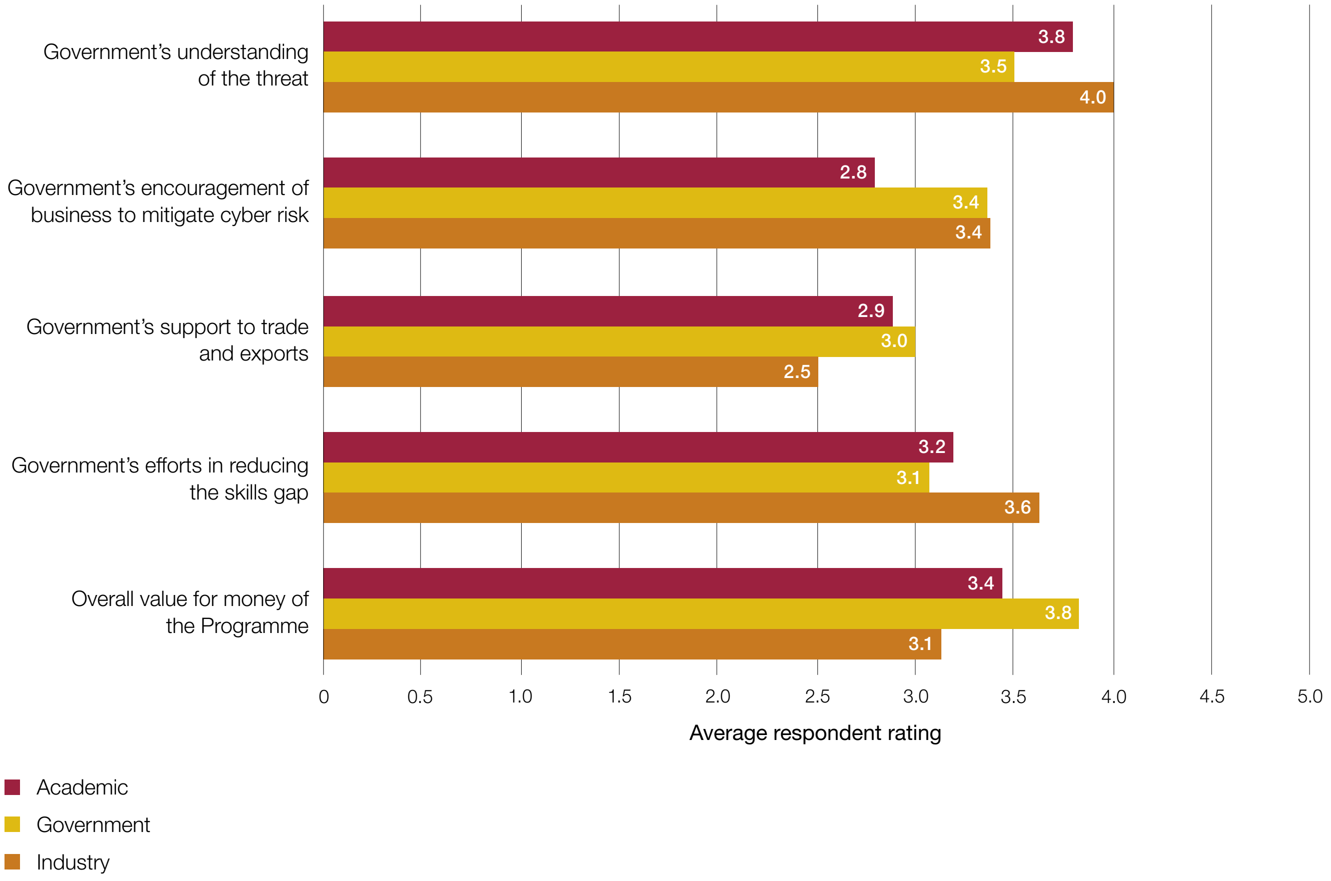
6 We reviewed a selection of documents relating to the National Cyber Security Programme, including financial management records, the benefits realisation tool, business cases and programme management documents.

7 We undertook a short survey of many of the people we interviewed. This was designed to produce a snapshot of views of the key areas of the National Cyber Security Programme. The results are shown in **Figure 4**.

8 The survey produced 34 responses, divided between industry (10), government (14) and academia (10). We asked those responding to our survey to rank performance in each area of the Programme with a score between 1 and 5, where 1 = very poor performance and 5 = excellent performance. We then assessed the scores overall and by the sector to which the respondent belonged.

Figure 4

Results of survey on 5 key challenges



Note

1 Values stated above are rounded to 1 decimal place.

Source: National Audit Office survey

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.

£10.00

ISBN 978-1-904219-40-8

9 781904 219408

National Audit Office

Design and Production by NAO Communications
DP Ref: 10510-001