National Audit Office

Report
by the Comptroller
and Auditor General

Cabinet Office

Progress of the 2016–2021 National Cyber Security Programme

HC 1988 SESSION 2017–2019 15 MARCH 2019

Key facts

£1.3bn

National Cyber Security Programme budget 2016-21

£648m

remaining funding for the final two years of the five-year Programme

3

number of the Programme's 12 objectives for which the Department assesses the supporting projects are all currently on track

8	number of the Programme's 12 objectives where at least 80% of the projects that support the objective are currently on track, with fewer than 80% on track against the twelfth objective
1	number of the National Cyber Security Strategy's 12 strategic outcomes for which the Department has 'high confidence' in its assessment that it will be met by 2021
11	number of strategic outcomes we are unable to report progress on for national security reasons. However, we can report that the Department has 'moderate confidence' in the evidence supporting progress in achieving four of them and 'low confidence' in a further six. The twelfth strategic outcome – 'understanding the cyber threat' – is fully excluded from the analysis
326	metrics the Department has identified to track performance of both the Programme and the Strategy. However, one-third (107) of these are currently not being measured, either because the Department has low confidence in the evidence underpinning a metric or it is planned as a future measure of performance
£169 million	value of Programme expenditure loaned or transferred in the first two years to support other activities, representing 37% of funding
72%	percentage of large UK companies reporting a cyber-attack in the previous 12 months, with 9% of those reporting multiple attacks per day
1,100+	number of cyber security incidents dealt with by the National Cyber Security Centre since its formation in October 2016

Summary

1 United Kingdom (UK) businesses and citizens increasingly operate online to deliver economic, social and other benefits, making the country more and more dependent on the internet. The UK's digital economy contributes a higher percentage to gross domestic product than in any other G20 country, and the UK aspires to be a world leader in digital economy and government. Consequently, it is connecting more and more government services to the internet; for example, 98% of applicants registering for Universal Credit did so online. This reflects growing digital connectivity across society, where 90% of UK households had internet access in 2018, compared with 77% in 2011.

2 However, the internet is inherently insecure, and attempts to exploit its weaknesses – known as cyber-attacks – continue to increase and evolve. The risk of deliberate or accidental cyber incidents is heightened by the increasingly interconnected nature of networks, systems and devices in use by organisations and individuals. Government's view is that cyber risks can never be eliminated but can be manged to the extent that the opportunities provided by digital technology, such as reducing costs and improving services, outweigh the disadvantages.

3 While departments and public bodies are responsible for safeguarding their own information, since 2010 government has decided that it needed centrally driven strategies and programmes to ensure the UK effectively manages its exposure to these risks. The Cabinet Office (the Department) leads this work, through successive National Cyber Security Strategies published in 2011 and 2016; and separate National Cyber Security Programmes designed to help deliver each Strategy between 2011–2016 (NCSP1) and 2016–2021 (the Programme).

4 The 2016 National Cyber Security Strategy's (the Strategy) vision is that "the UK is secure and resilient to cyber threats, prosperous and confident in the digital world". Government recognises this is a complex challenge that also needs the involvement of businesses and the public to manage their own exposure to cyber risk. The Strategy outlines the roles and responsibilities that individuals, businesses, organisations and government need to take to make sure that their systems are secure. The Strategy is supported by expenditure of £1.9 billion.

5 The Strategy focuses on the steps government will take to make the UK more secure online, covering the overarching themes of Deter, Defend and Develop across 12 strategic outcomes (**Figure 1** on pages 6 and 7). It is designed to be a cross-government approach, with specific departments (referred to as lead departments) responsible for each of the Strategy's 12 strategic outcomes (plus a thirteenth – the overarching governance as managed by the Department). The Strategy's 12 strategic outcomes are regarded as equally important and are not prioritised.

Figure 1
Overview of the National Cyber Security Strategy 2016–2021

National Cyber Security Strategy 2016–2021

Deter

The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.

1 The UK has the capability to effectively detect, investigate and counter the threat from the cyber activities of our adversaries.

2 The impact of cybercrime on the UK and its interests is significantly reduced and cyber criminals are deterred from targeting the UK.

Defend

We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents and to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.

3 The UK has the capability to manage and respond effectively to cyber incidents to reduce the harm they cause to the UK and counter cyber adversaries.

4 Our partnerships with industry on active cyber defence mean that large-scale phishing and malware attacks are no longer effective.

5 The UK is more secure as a result of technology products and services having cyber security designed into them and activated by default.

6 Government networks and services will be as secure as possible from the moment of their first implementation. The public will be able to use government digital services with confidence and trust that their information is safe.

7 All organisations in the UK, large and small, are effectively managing their cyber risk, are supported by high-quality advice designed by the National Cyber Security Centre (NCSC), underpinned by the right mix of regulation and incentives.

7.1 We understand the level of cyber security across the Critical National Infrastructure and have measures in place to intervene where necessary, to drive improvements in the national interest.

Overarching themes

Lead department delivering the Strategy and Programme objectives

- National Cyber Security Centre (NCSC)
- Cabinet Office
- Home Office
- Foreign & Commonwealth Office
- Department for Digital, Culture, Media & Sport

Note

1 Objective 7 has been split into two, to separate responsibility for Critical National Infrastructure, which the Cabinet Office oversees, from the Department for Digital, Culture, Media & Sport's work on incentivising and regulating other businesses.

Source: Cabinet Office

Develop

We have an innovative growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

8 There is the right eco-system in the UK to develop and sustain a cyber security sector that can meet our national security demands.

9 The UK has a sustainable supply of home-grown cyber-skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors and defence.

10 The UK is universally acknowledged as a global leader in cyber security research and development, underpinned by high levels of expertise in UK industry and academia.

11 The UK government is already planning and preparing for policy implementation in advance of future technologies and threats and is 'future-proofed'.

Underpinning these themes, we will pursue **International** action and exert our influence by investing in partnerships. We will shape the global evolution of cyberspace in a manner that advances our wider economic and security interests.

12 The threat to the UK and our interests overseas is reduced due to increased international consensus and capability towards responsible state behaviour in a free, open, peaceful and secure cyberspace.

Governance

13 UK government policies, organisations and structures are simplified to maximise the coherence and effectiveness of the UK's response to the cyber threat.

6 The Strategy includes £1.3 billion for the Programme. The Programme's objectives are organised under the same headings as the Strategy's 12 strategic outcomes (Figure 1). The Department uses a range of metrics to assess progress against the objectives and the strategic outcomes. The Programme has a broad scope, from developing cyber skills in the UK to technical measures to defend attacks, to considering how to incentivise organisations to make their digital systems more secure.

Study scope

7 Our audit sought to answer the question: "Is the Cabinet Office effectively coordinating the 2016–2021 National Cyber Security Programme?" This includes understanding how the Programme contributes to the delivery of the Strategy's overarching strategic outcomes. Our report examines the government's approach to cyber security (Part One); how the Department set up and manages the Programme (Part Two); progress in delivering the Programme (Part Three) and finally examines what the Programme expects to achieve up to 2021 and beyond (Part Four).

8 We have not examined the other activities that support the Strategy, such as the effectiveness of individual departments' expenditure on the protection of their digital systems and information, and other activities that contribute to enhancing the UK's cyber security. This includes the Department for Education's £84 million computing teacher training centre announced in the 2017 budget.

Key findings

On the government's approach to cyber security

9 Our previous work has shown that cyber security poses a major challenge for government. We have undertaken several reports which set out the difficulties departments have encountered in ensuring the UK is safe online, although the true overall cost of online fraud is unknown. In 2017, the Annual Fraud Indicator estimated fraud losses in the UK of £6.8 billion for individuals and £140 billion for the private sector. Our June 2017 *Online fraud* report noted that more than half of fraud is committed online. Our report found that government did not have a clear mechanism for identifying, developing and sharing good practice to prevent people becoming victims. Our April 2018 investigation into the WannaCry cyber-attack found that more than one-third of NHS trusts in England were impacted by the incident, resulting in an estimated 19,000 appointments being cancelled. The then Department of Health did not know whether local NHS organisations were suitably prepared for a cyber-attack (paragraphs 1.6 and 1.7).

10 The risk of cyber-attacks is rising as the UK's increasing connectivity makes it more vulnerable to a growing and evolving threat. The UK has one of the world's most internet-enabled economies: in 2016, one-eighth of the UK's gross domestic product came from the digital economy, the highest across the G20. This makes the UK more vulnerable to the threat from hostile countries, criminal gangs and individuals, which continues to increase and evolve as it becomes easier and cheaper to launch attacks. Trends in cyber-attacks are hard for government to predict because the nature of technology evolves rapidly and perpetrators are quick to take advantage of these changes. A government survey in 2018 found that 43% of UK businesses reported at least one cyber security breach in the previous year (paragraphs 1.3 to 1.5 and 1.8 to 1.14).

11 Government is intervening more to tackle the growing cyber risk. Government believes that NCSP1 delivered substantial improvements to UK cyber security, but its approach – including relying on market forces to drive secure cyber behaviours among companies – did not achieve the scale and pace of change required to stay ahead of the threat. Through the 2016 Strategy, government is taking a more proactive role to deliver the required improvements; for instance, helping business by investing in the UK cyber sector and driving up standards of cyber security across the economy. To support this new approach government increased funding from £860 million for NCSP1 to £1.3 billion for the current Programme (paragraphs 1.15 to 1.21).

On progress in delivering the Programme

12 The Programme was reprofiled in the first two years in order to address higher government priorities, and by a lack of capacity to deliver. Having set up the Programme the government concluded it needed to prioritise additional funding on counter-terrorism activities. Additionally, the Department had limited evidence to draw on from NCSP1, and a lessons-learnt exercise conducted at the end of NCSP1 added little further information. Consequently, HM Treasury loaned £100 million of Programme funding – to be returned later in the Programme – to support counter-terrorism work and £69 million permanently transferred on to other national security activities, representing more than one-third (37%) of planned funding for the first two years of the Programme. Although these activities contributed to enhancing cyber and wider national security they were not originally intended to be funded by the Programme, and this delayed work on projects such as elements of work to understand the cyber threat (paragraph 2.5 and Figure 2).

13 The Department did not produce a business case for the Programme, meaning there was no way to assess how much funding was required. The government used the Strategic Defence and Security Review and Spending Review in 2015 to establish the overall direction of cyber security expenditure and approve individual project business cases. However, when HM Treasury set the funding in 2015 the Department did not produce an overall Programme business case to systematically set out the requirement and bid for the appropriate resources. Since then, the Department has used the Strategy to guide the Programme's activities and assigned funding to the lead departments based on the project-level business cases they submit to achieve their objectives (paragraphs 2.3 and 2.4).

14 Lead departments are largely on track to deliver against their objectives, although funding for the remainder of the Programme is below the recommended level. Each of the Programme's 12 objectives is being delivered through a series of lower-level projects. All projects supporting the 'incident management', 'active cyber defence' and 'international' objectives are being delivered against current plans. Against a further 8 objectives the Department expects to achieve at least 80% of projects, but achieve fewer than 80% of projects against the 'critical national infrastructure' objective. In 2018-19 lead departments were encouraged by the Department to submit multi-year 'minimum', 'recommended' and 'ambitious' project bids for the remaining three years of the Programme. The ambitious bids came in 33% over the available budget, despite significant planned increases in funding for the remaining years of the Programme. Following a detailed review process the Department determined that many bids either did not have enough evidence to support their prospects of successful delivery or failed to meet Programme investment criteria. The overall financial settlement for the three remaining years of the Programme ultimately fell between the totals of the recommended and minimum bids requested by lead departments (paragraphs 3.5, 3.17, 3.18 and Figure 6).

15 The Department does not yet have enough evidence to prioritise those activities that make the biggest impact or address the greatest need. Lead departments have been measuring progress against their objectives and are largely on track to deliver their individual projects. The Department, however, did not use the period of the reprofiling to develop a robust performance framework at the Programme-level, only introducing one in 2018. It therefore does not have enough evidence to effectively prioritise funding on those objectives that are likely to deliver the biggest impact, address the greatest needs and deliver best value for money. For some of the more innovative parts of the Programme there is limited historical data from which the Department can draw and some of the strategic outcomes remain challenging to measure. The dependencies between objectives are unclear; for example, setting out the links between the 'cyber skills' and 'science and technology' objectives. One area where the Department does have evidence of impact is in Active Cyber Defence, where funding has been increased due to the success of the programme (paragraphs 2.7, 2.8, 2.12 to 2.15, 3.12 and 3.13).

16 The government successfully established the National Cyber Security Centre. Government established the National Cyber Security Centre (NCSC) in October 2016 as the UK's technical authority on cyber security by merging four existing organisations. Part of its work is to deliver Active Cyber Defence, which aims to protect the majority of the UK from the majority of cyber-attacks the majority of the time. However, although Active Cyber Defence has delivered measurable results, it is still developing a baseline to gauge the impact it is having against the scale of the problem. The NCSC is also responsible for understanding the threat that is posed by potential adversaries, leading the response to any cyber-attacks, such as the 2017 WannaCry incident, and helping organisations that have suffered a cyber-attack (paragraphs 3.6 to 3.11).

17 The Programme has already reduced the UK's vulnerability to specific attacks. The NCSC has reported tangible results from its Active Cyber Defence activities. It developed a tool that identified fake emails, leading to 54.5 million fake emails being blocked in 2017-18. However, once cyber criminals realised that their fake emails were being detected they set up spoof government websites so that fake emails originating from these sites could not be detected. The NCSC therefore developed a tool to counter this activity, resulting in a drop in fake emails and spoof websites. There has also been a reduction in phishing attacks originating from the UK, with the UK's share of global phishing attacks falling from 5.3% to 2.2% in two years (paragraphs 3.12 and 3.13).

On progress in delivering the Strategy

18 It is unclear whether government will achieve the Strategy's strategic outcomes. The Department is responsible for coordinating delivery of the Strategy, but this depends on delivery of the Programme's projects by other departments, contributions by organisations and individuals outside government and other government expenditure. Reductions in scope of some individual projects, while sufficient to meet lowered Programme objectives, makes it more challenging for lead departments to achieve the Strategy's strategic outcomes. However, this risk is difficult to assess, partly due to the complex and evolving cyber threat, but also because the Department has not undertaken work to assess whether the £1.9 billion of funding was ever sufficient to achieve the Strategy's strategic outcomes. Consequently, the Department has stated that it may take longer than 2021 to address all the complex cyber security challenges set out in the Strategy, although it is yet to determine when the remaining strategic outcomes might be achieved (paragraphs 2.4 and 3.14 to 3.18).

19 The Department has 'low confidence' in the evidence supporting half of the Strategy's strategic outcomes, and currently only expects to achieve one by 2021. In February 2019 the Department reported that it had 'high confidence' in its assessment that lead departments would meet one of the Strategy's 12 strategic outcomes by 2021, 'incident management' (Figure 1). For security reasons we cannot report progress against any further strategic outcomes. However, with the exception of the 'understanding the threat' strategic outcome we can report on the Department's confidence in the quality of the evidence used to make those classified assessments on the remaining 10 strategic outcomes. Of these, four were categorised as 'moderate confidence' and six at 'low confidence' – the latter meaning "uncertainty in key areas of evidence". This is a recent improvement, as the evidence underpinning five of the six 'low confidence' strategic outcomes were reporting as 'very low confidence' in the previous progress report in November 2018 (paragraph 2.13, 3.14 to 3.15 and Appendix Three).

Tackling cyber risk in the future

20 Programme management weaknesses are likely to continue to hamper delivery of the Programme and consequently the Strategy up to 2021. Prior to 2018, lead departments measured their own objectives. Since then, the Department has introduced a more robust performance framework to measure both the Programme and Strategy's performance and asked lead departments to spend more on measuring progress against achieving the Strategy's strategic outcomes. It will nonetheless be difficult in the short term for the Department to identify what the Programme needs to do to achieve the Strategy as currently the Department only has 'high confidence' in the evidence underpinning one of its 12 strategic outcomes (paragraphs 2.12 to 2.15, 3.14 to 3.22, Appendix Three).

21 The Department has started preparations for an approach to cyber security after 2021, but risks repeating previous mistakes. None of the new capabilities the Programme has already delivered are funded beyond 2021. The Department has begun to consider what the government's vision for cyber security will look like after then and intends to coordinate a collective bid by lead departments into the 2019 Spending Review. However, it seems unlikely that the Department will have decided on its future approach to cyber security in time to inform funding decisions for the 2019 Spending Review, which is likely to determine government funding beyond the end of the current Strategy in 2021. Not having such an approach in place in time for the Spending Review risks making the same mistake made in 2015, when cyber security funding was agreed before the Department published its Strategy outlining the government's approach to cyber security (paragraphs 4.4 to 4.11).

Conclusion on value for money

22 By refreshing its National Cyber Security Strategy in 2016 the government has shown an important commitment to improving cyber security. Such an approach is vital to ensure that the rapidly evolving risk from cyber-attacks does not undermine the UK's ambition of building a digital economy and transforming public services. Achievement of the Strategy's strategic outcomes is supported by the £1.3 billion National Cyber Security Programme, which has provided a focal point for cyber activity across government and has already led to some notable innovation, such as the establishment of the National Cyber Security Centre.

23 However, despite recent improvements in the Programme's management and delivery record, it was established with inadequate baselines for allocating resources, deciding on priorities or measuring progress effectively. With two years of the Programme still to run this makes it hard to say whether it will provide value for money. Ultimately, the Department can best demonstrate value for money if the Programme's objectives are delivered by 2021 and can then be shown to have maximised their contribution to the wider Strategy. Looking ahead to the UK's longer-term position, the Department needs to build on its current work to ensure there is adequate planning for what activity government might undertake after the existing Programme ends.

Recommendations

24 Given the increasing importance of cyber security, government should develop a new approach to cyber security after the current Strategy and Programme end in 2021. Our recommendations therefore focus on what the Department needs to do to ensure an effective transition from the end of the current Strategy and Programme to any future activity:

a **The Department should establish which areas of the Programme are having the greatest impact or are most important to address.** This balance of investment information should influence where the Department focuses its resources up to 2021 as well as informing any future cyber security strategy and feeding into future business cases. We would expect this exercise to reduce or cease funding certain areas of Programme activity or transfer them into core departmental budgets.

b **The Department should continue to consult with other government departments to understand their cyber security priorities.** This would allow them to contribute to any future strategy and programme and enable the Department to aggregate cyber opportunities and risks to better prioritise overall government activity in this area. As these activities will need to be funded it should also allow the Department to better cost any future programme bid and ensure there is no lull in activities between the end of the Programme and any follow-on cyber security activity.

c **The Department should build on its current work to develop a strategy for UK cyber security after 2021.** In advance of the 2019 Spending Review, the Department should consult across government and other relevant organisations. We would expect this strategy to be principles-based, identifying the unique role that the centre of government can play, the responsibilities of other departments, and the scale and nature of the government's cyber security support to the wider UK economy and society.

d **The new strategy should clearly set out a future division of labour.** It should establish which activities should be centrally funded, which are private sector responsibilities and which are core departmental activities. Based on the principles established in the new strategy, some capabilities will be new and others will require sustaining over the longer term, which may best be achieved through 'mainstreaming' into core departmental funding. We would expect this to be complete in time to deliver, if required, a business case containing a costed, programme-level bid into the Spending Review.

e **The Department should consider a more flexible programmatic approach to cyber security.** The previous two National Cyber Security Programmes have been for five years, although the cyber security field is evolving rapidly. Under any future approach the Department should consider a mixture of shorter programmes to be more responsive to changing risks and longer-term investment in other areas, such as skills.