National Audit Office

Report
by the Comptroller
and Auditor General

Cabinet Office

Protecting information across government

HC 625 SESSION 2016-17 14 SEPTEMBER 2016

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 785 people. 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 £1.21 billion in 2015.

National Audit Office

Cabinet Office

Protecting information across government

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 13 September 2016

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

12 September 2016

HC 625 | £10.00

This report considers the effectiveness of government in defining its strategic approach to protecting information across central government departments.

© National Audit Office 2016

The material featured in this document is subject to National Audit Office (NAO) copyright. The material may be copied or reproduced for non-commercial purposes only, namely reproduction for research, private study or for limited internal circulation within an organisation for the purpose of review.

Copying for non-commercial purposes is subject to the material being accompanied by a sufficient acknowledgement, reproduced accurately, and not being used in a misleading context. To reproduce NAO copyright material for any other use, you must contact copyright@nao.gsi.gov.uk. Please tell us who you are, the organisation you represent (if any) and how and why you wish to use our material. Please include your full contact details: name, address, telephone number and email.

Please note that the material featured in this document may not be reproduced for commercial gain without the NAO's express and direct permission and that the NAO reserves its right to pursue copyright infringement proceedings against individuals or companies who reproduce material for commercial gain without our permission.

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.

11131 09/16 NAO

Contents

The National Audit Office study team consisted of:
Yvonne Gallagher, Chris Grant, Elizabeth Livingstone and Nigel Vinson, 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

Key facts

200

number of cyber national security incidents dealt with by GCHQ per month in 2015, up from 100 per month in 2014

8,995

number of data breaches recorded by 17 largest departments in 2014-15

£300m

limited government estimate of annual spend on security in 34 departments. Actual costs are thought to be 'several times' this figure

12	number of separate organisations in the centre of government with responsibility for aspects of protecting information
£28 million	estimated annual government expenditure on external IT security support
£200 million to £400 million	savings estimated per year, by 2014, from adopting the Public Services Network (PSN), as outlined in the 2011-12 business case. Actual PSN savings in 2014 were £103.4 million. No further savings are expected
73	the number of teams covering security in central government departments
1,600	number of protective security staff (information, physical and personnel) in central government departments

Summary

1 Protecting the information government holds from unauthorised access or loss is a critical responsibility for departmental accounting officers. But departments are increasingly required to balance this responsibility with the need to make this information available to other public bodies, delivery partners, service users and citizens via new digital services.

2 The Prime Minister is ultimately responsible for the security of the UK government. She is supported in this by the Cabinet Secretary, who chairs a permanent secretary committee which sets the overall direction and strategy for government security. Across departments, responsibility for information security lies with the respective ministers, permanent secretaries and their management boards.

3 In recent years, cuts to departmental budgets and staff numbers, and increasing demands from citizens for online public services, have changed the way government collects, stores and manages information. Major drivers for this change include successive IT and digital strategies since 2010, as well as the 2012 *Civil Service Reform Plan*, which placed greater responsibility on departments to protect their own data holdings.

4 Concurrently, the threat of electronic data loss from cyber crime, espionage and accidental disclosure has risen considerably. Alongside this new challenge, reporting to the Information Commissioner's Office (ICO) by public bodies shows that the loss of paper records remains significant.

Study scope

5 This report considers the effectiveness of the centre of government (the centre) in defining government's strategic approach to protecting information across central government departments (the departments) (Part One); the centre's performance in protecting information, including managing specific projects (Part Two); and departments' performance in protecting their information (Part Three).

6 The centre consists of various teams within the Cabinet Office as well as other organisations such as CESG (see **Glossary** on page 42) and the National Cyber Security Centre. The central government departments consist of the 17 largest departments of state, although we have included other bodies where the evidence allows, as many of these issues are not unique to central government.[1]

1 In alphabetical order, these are: Cabinet Office; Department for Business, Innovation & Skills (now part of the Department for Business, Energy & Industrial Strategy); Department for Communities and Local Government; Department for Culture, Media & Sport; Department for Education; Department for Environment, Food & Rural Affairs; Department for International Development; Department for Transport; Department for Work & Pensions; Department of Energy & Climate Change (now part of the Department for Business, Energy & Industrial Strategy); Department of Health; Foreign & Commonwealth Office; HM Revenue & Customs; HM Treasury; Home Office; Ministry of Defence and the Ministry of Justice. Although correct at the time of writing, recent Machinery of Government changes mean that this list may have now changed.

7 Specifically, we sought to answer the question: "Is the Cabinet Office effectively coordinating the protection of government's information?" The criteria and principles we used to explain and assess government's performance were as follows:

- On the centre's evolving approach to managing the protection of information (Part One):
    - we describe how well the centre has coordinated its approach to protecting information across government (paragraphs 1.10–1.26).
- On the performance of the centre (Part Two), we examined:
    - **the government's performance in protecting information:** We were looking to see whether government had a clear approach which married departmental responsibilities with a plan at the centre of government that identified the benefits, opportunities and risks of operating in this rapidly evolving area (paragraphs 2.2–2.5);
    - **security breach reporting:** We assumed government activity in this area would be guided by a collated assessment across government on the number of breaches, their effect and mitigating actions, and a comprehensive long-term action plan to reduce their impact (paragraphs 2.6–2.19);
    - **managing strategic information risks:** We would expect government to have a clear understanding of the strategic risks to protecting information, based on accurate returns from departments covering a number of disciplines, including the sharing of best practice and identifying any gaps in capability (paragraphs 2.20 and 2.21); and
    - **the performance of centrally managed projects:** We would expect the centre to deliver cost-effective performance from the projects for which it is responsible, using clear cost, timescale and performance data to outline the benefits delivered (paragraphs 2.22–2.44).
- On departmental performance in protecting information (Part Three), we examined:
    - **governance in departments and delivery chains:** We reviewed a sample of governance arrangements to see if there were comprehensive and robust arrangements in departments for managing the protection of information, including through delivery chains (paragraphs 3.2–3.13);
    - **the financial impacts of the revised approach to protecting information:** We assessed whether government understood how much its previous approach to protecting information used to cost, against how much it now costs – and how many staff are involved (paragraphs 3.14–3.20); and
    - **deploying people with the right skills:** Building on our previous work in this area, we assessed whether government had a clear understanding of its skills requirements for protecting information, and a comprehensive plan for addressing any capacity or capability gaps (paragraphs 3.21–3.35).

8 We did not examine the physical or personnel security aspects of protecting data, such as guarding or vetting. Nor did we directly examine the protection of information within local government or local health, education or emergency service organisations.

Key findings

9 The main body of this report contains our evidence of government's performance against the above criteria. Paragraphs 10 to 17 below set out our most important findings. In essence, they show that the Cabinet Office has not yet established a clear role for itself in coordinating and leading departments' efforts to protect their information. Furthermore, its evolving ambition to undertake such a role is weakened by the limited information it has on departmental costs, performance and risks.

On protecting information in government

10 **Too many bodies with overlapping responsibilities operate in the centre of government, confusing departments about where to go for advice.** As at April 2016, at least 12 separate teams or organisations in the centre of government had a role in protecting information, many of whom produce guidance. And the governance arrangements above them are unclear and fragmented, with no formal links between the three most important information security decision-making bodies in the Cabinet Office (paragraphs 1.21–1.26, Figures 4 and 5).

11 **Increasing dependencies between central government and the wider public sector mean that traditional security boundaries have become blurred.** At present, the Cabinet Office remit for security only extends to central government departments. However, there is a clear dependency between central government and the wider public sector, driven by increasing information flows, the demands of public service provision and shared technical infrastructure (paragraphs 1.3, 1.13, 1.15 and 2.7).

12 **The new National Cyber Security Centre (NCSC) will bring together much of government's cyber expertise, but wider reforms will be necessary to further enhance the protection of information.** The NCSC should streamline central government processes for dealing with information incidents in cyberspace. However, the scale and pace of the challenges of protecting information are such that these structural changes are unlikely to be sufficient on their own unless Cabinet Office also supports departments in addressing the wider problems set out in this report. The NCSC is designed to work with government and the private sector: whether it has the capacity to do so effectively remains to be seen (paragraph 1.30).

On the performance of the centre

13 The Cabinet Office does not collect or analyse government's performance in protecting information on a routine basis. This means it has little visibility of information risks in departments and has limited oversight of the progress departments are making to better protect their information. Reporting personal data breaches is chaotic, with different mechanisms making departmental comparisons meaningless (paragraphs 2.2–2.21).

14 The Cabinet Office needs to improve delivery of its centrally managed projects. The Government Security Classifications (GSC) system, the Public Services Network (PSN) and Foxhound pose considerable business change, cultural and technical challenges but have been slow to deliver planned benefits. Alongside their primary objectives, all three projects were intended to achieve significant financial savings, but none have fully delivered those financial benefits yet (paragraphs 2.22–2.44).

On departmental performance in protecting information

15 Some departments have made significant improvements in information governance, but most have not given it the same attention as other forms of governance. The Cabinet Office does not provide a single set of governance standards for departments to follow, and does not collate or act upon identified weaknesses. Only a few departments set security standards through their supply chain (paragraphs 3.2–3.13).

16 The Cabinet Office does not have access to robust expenditure and benefits data from departments to take informed strategic decisions on protecting information. This is in part because departments do not always collect or share robust expenditure or benefits data. The Cabinet Office has recently collected some data on security costs, although it believes that actual costs are 'several times' the reported £300 million figure. Departments often do not share advice and knowledge effectively, either resulting in them repeating work at additional cost or missing the opportunities presented by adopting new technologies (paragraphs 3.14–3.20).

17 In the context of a challenging national picture it has been difficult for government to attract people with the right skills. The government established a security profession in 2013, and has undertaken some initial work to establish professional learning and development. Demand for skills and learning across government is growing and is likely to continue to grow. Plans to cluster security teams may initially share scarce skills but will not solve the long-term challenge, and will pose questions for departmental accountability (paragraphs 3.21–3.35).

Conclusion

18 Protecting information while re-designing public services and introducing new technology to support them is a complex challenge for government. To achieve this, the centre of government requires departments to risk manage their information, but few departments have the skills and expertise to achieve this by themselves. How successful government is in dealing with this challenge will therefore continue to depend on effective support from the Cabinet Office and other bodies at the centre of government.

19 The Cabinet Office is taking action to improve its support for departments, but needs to set out how this will be delivered in practice. To reach a point where it is clearly and effectively coordinating activity across government, the Cabinet Office must further streamline the roles and responsibilities of the organisations involved, deliver its own centrally managed projects cost-effectively and clearly communicate how its various policy, principles and guidance documents can be of most use to departments.

Part One

Protecting information in government

1.1 Protecting the information it holds is a critical responsibility of government. This Part defines what we mean by protecting information, and examines the UK's developing approach to it across central government. It assesses the impact that the government's strategy for increasingly delivering public services online has had, and the challenges facing the government in providing a coherent approach to protecting information.

Information assurance and the protection of information

1.2 The Prime Minister is ultimately responsible for the security of the UK government. She is supported in this by the Cabinet Secretary, who chairs a permanent secretary committee which sets the overall direction and strategy for government security. Across departments, responsibility for information security lies with the respective ministers, permanent secretaries and their management boards.

1.3 The Cabinet Office is responsible for coordinating information security across central government departments. Its remit does not extend to the wider public sector. However, there are increasing dependencies between central government and the wider public sector which mean that traditional security boundaries have become blurred. These dependencies are driven by increasing information flows, the demands of public service provision and shared technical infrastructure.

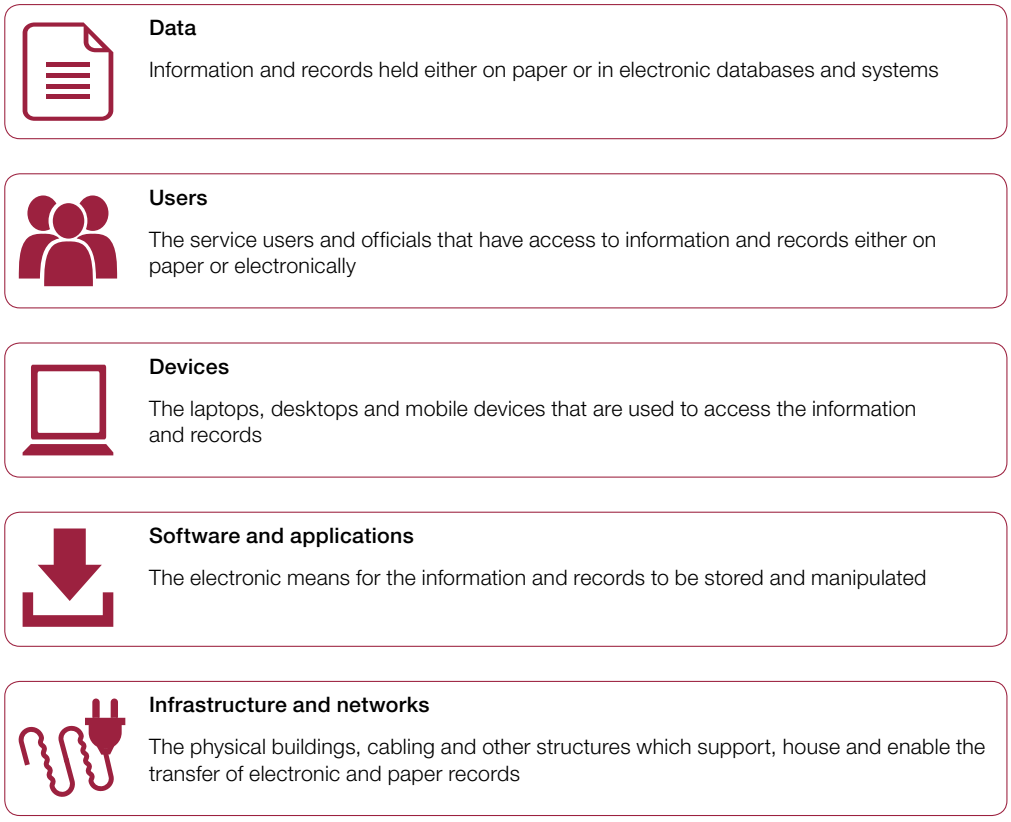
1.4 The UK government uses the term 'information assurance', which it defines as: "the confidence that information systems will protect the information they handle and will function as they need to when they need to…"[2] Effective information assurance involves a balance between ensuring information is accessible (in terms of the availability and integrity of the data) for business needs, and ensuring it is protected. Although the latter can also cover physical and personnel security, this report focuses solely on how information contained in documents, IT systems or through the delivery of different technologies is protected. We therefore use the term 'protecting information'.

2 HMG IA Standard No 2 – Risk Management and Accreditation of Information systems [Issue 3.2, January 2010]. This standard is no longer extant, but the definition of information assurance remains relevant for the purposes of this report.

1.5 Much of the information needing protection in central government still includes large quantities of paper-based records. However, over the last decade, the proliferation of the internet and mobile electronic devices has meant the older discipline of protecting information now overlaps heavily with cyber security – the assurance of networked systems and services.

1.6 As well as secure data holdings, a credible information protection strategy relies on robust systems and practices at the various levels (**Figure 1**). People – both service users and officials – need to understand the information they are using. Then government needs to deploy the right knowledge, behaviours and processes, supported by a range of effective departmental and cross-government services and technology and data centres. Failures in any of these areas can undermine the whole enterprise.

Figure 1
Components of information protection in the UK public sector



Source: National Audit Office analysis of government information

1.7 Compliance with data protection laws is also an important part of protecting information, increasing the accountability on departments for the information they hold. The 1998 Data Protection Act governs the protection of personal data in the UK.[3] The Information Commissioner's Office (ICO) ensures personal data is handled according to the Act, having the authority to fine departments where breaches occur.[4]

Government's previous approaches

1.8 Historically, government's information was largely paper-based and did not need to be immediately accessible or easily shared between departments, businesses or citizens. Technology was built around the paper-based processes and departments often added security as a secondary requirement. Arrangements for protecting information were based on this environment and designed to defend against unsophisticated technical threats that are unrecognisable from today's situation. The centre of government nonetheless gave additional assistance to departments involved in national security (the so-called 'high-threat club') and parts of the critical national infrastructure, where it recognised that the threat of unauthorised access was higher.[5]

1.9 To support this approach, several bodies in the centre of government directed departmental information assurance activities with strong oversight of policy and practices, and set mandatory and detailed standards. The Cabinet Office took overall responsibility for this oversight, supported by bodies with specialist expertise such as CESG and the Centre for the Protection of National Infrastructure (CPNI).[6] Departmental accounting officers continue to be responsible for their departments' security and report performance in this area in their annual reports and accounts.

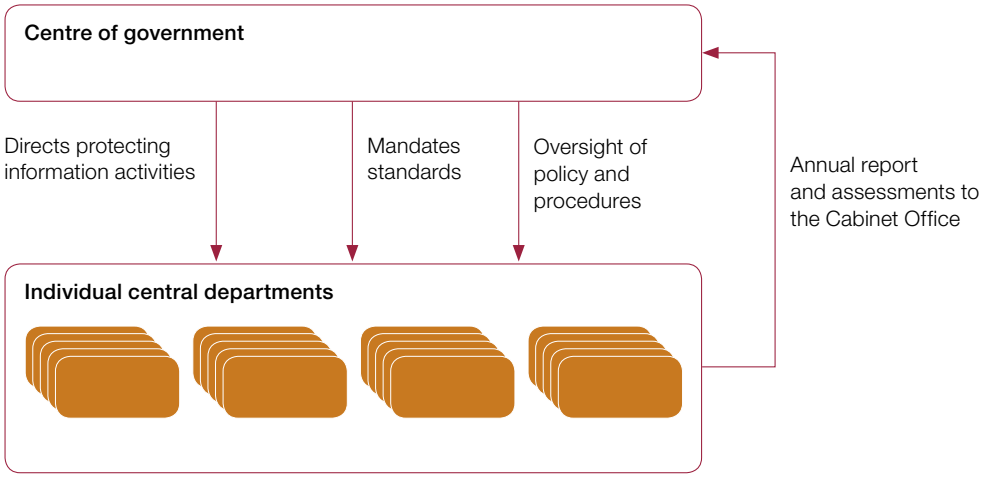
1.10 In 2004 the senior information risk owner (SIRO) role was created to provide a focus for addressing information risks at board level in departments. After the 2007 loss of child benefit data by Her Majesty's Revenue & Customs, the SIRO role was made mandatory as part of the Cabinet Office's 2008 *Data Handling Procedures in Government* report.[7] This re-emphasised that the Cabinet Office would continue to set 'cross-government mandatory standards' for information assurance, and that departments would be responsible for implementing these in their own areas. The Cabinet Office created a coordinating function, known as the Office of the Government SIRO, or OGSIRO, in 2012.

3 Data Protection Act 1998. Available at: www.legislation.gov.uk/ukpga/1998/29/contents
4 The Information Commissioner's Office is also responsible for other legislation which relates to personal data, such as the Freedom of Information Act. See: https://ico.org.uk/
5 The term 'high-threat club' has usually been taken to include the Office of the Prime Minister, the Ministry of Defence, the Foreign & Commonwealth Office, and the security and intelligence services.
6 CESG is the information security arm of the Government Communications Headquarters (GCHQ) and is the national technical authority for information assurance. CPNI protects national security by providing protective security advice.
7 Cabinet Office, *Data Handling Procedures in Government*, June 2008, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf

1.11 Departments and, indirectly, commercial suppliers to government were mandated to meet these standards as part of their broader compliance with the *Manual of Protective Security* and the *HMG Security Policy Framework*.[8] This compliance is monitored through provision of annual assessments and reports to the Cabinet Office. Key government security policies, such as the Government Protective Marking Scheme and practical assurance standards, provided the basis for a common approach to protecting information in central government.

1.12 **Figure 2** shows the influences in place to support government's information protection requirements. The main strength of this information assurance model was that the centre had a single approach to information risks and opportunities across government, based on centralised advice and guidance.

Figure 2
Information assurance – the legacy model



Source: National Audit Office analysis of government information

8 Cabinet Office, *HMG Security Policy Framework*, April 2014, available at: www.gov.uk/government/publications/security-policy-framework

The Cabinet Office's evolving approach to protecting information

1.13 In recent years there have been a number of legislative, policy, technological and consumer changes that have had an impact on the Cabinet Office's approach to protecting information. One key reason for the new approach was the focus of the government elected in 2010 on achieving cost reduction. It also recognised that many citizens had become sophisticated users of technology and increasingly expected public services to be delivered online. Government saw this as an opportunity to deliver its services more cost-effectively.

1.14 To support the digital aspects of the public service transformation agenda, the Cabinet Office published a number of strategies, many of which had implications for how departments should protect information:

- March 2011 – *Government ICT Strategy* (augmented several months later by four sub-strategies and a Strategic Implementation Plan).[9]
- July 2011 – *Government Shared Services Strategic Vision*.[10]
- June 2012 – *The Civil Service Reform Plan*.[11]
- November 2012 – *Government Digital Strategy.*[12]
- December 2012 – *Next Generation Shared Services Strategic Plan*.[13]

1.15 The Cabinet Office established the Government Digital Service (GDS) to implement the government's 'digital by default' approach as set out in the 2012 *Government Digital Strategy*. Since then, GDS has set up common platforms: GOV.UK as the common web portal; GOV.UK Verify for common identity authorisation; and the G-Cloud, a government procurement framework for cloud services. It also established the Office of the Government Chief Technology Officer to drive government technology reform. GDS also took responsibility for the management of the Public Services Network (PSN), the successor to Government Secure Intranet (GSi), which was designed to connect central and local government and other public services.

1.16 The government's view was that, in order to deliver its vision of better connected digital environments, it needed to change the existing protecting information processes. The impact of this would be that specialists would be better able to articulate the risks inherent in the new ways of working.

9 Cabinet Office, *Government ICT Strategy*, March 2011; HM Government, *Government Cloud Strategy*, October 2011; HM Government, *Government End User Device Strategy*, October 2011; HM Government, *Government ICT Capability Strategy*, October 2011; HM Government, *Greening Government: ICT Strategy*, October 2011; HM Government, *Government ICT Strategy – Strategic Implementation Plan*, October 2011, available at: www.gov.uk/government/publications/uk-government-ict-strategy-resources

10 Cabinet Office, *Government Shared Services: A Strategic Vision*, July 2011, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/61166/government-shared-services-july2011.pdf

11 HM Government, *The Civil Service Reform Plan*, June 2012, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/305148/Civil-Service-Reform-Plan-final.pdf

12 Cabinet Office, *Government Digital Strategy*, November 2012, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/296336/Government_Digital_Stratetegy_-_November_2012.pdf

13 Cabinet Office, *Next Generation Shared Services The Strategic Plan*, December 2012, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/83717/19284_Next_Generation_3rd_Online.pdf

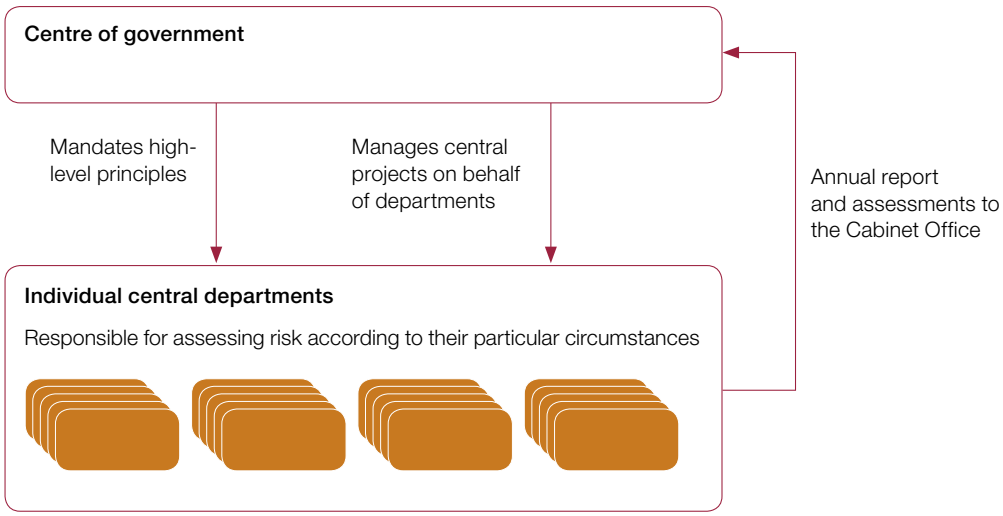
1.17 The 2012 *Civil Service Reform Plan* had already placed greater accountability on departments for implementing major projects and policies in their businesses, including information holdings. The 2014 revised *HMG Security Policy Framework* re-emphasised the focus on departments' responsibility for assessing their own level of risk and assurance.[14] This presented a set of high-level principles with reduced prescription and re-emphasised the requirement for departments to assess and understand the risks to their own information, and that accountability for managing these risks fell to departmental permanent secretaries.

1.18 The Cabinet Office included the Government Security Classification (GSC) policy with the aim of simplifying the system used to classify government data from six tiers to three. It also took responsibility for the delivery of an IT shared service, called Foxhound, to replace systems in those departments which held data requiring a higher level of security and which it regarded were no longer fit for purpose. We cover these two projects and the PSN in more detail in Part Two.

1.19 These and other reforms have contributed to the UK's strong international reputation in digital government. The UK government's approach to security policy, and in particular the simplification of its classification system, is being replicated by the US, Australia and a number of other technologically advanced nations. In addition, many of the UK's recently developed standards for enterprise technology, cloud services and cyber security have also been widely adopted internationally and by industry.

1.20 Figure 3 illustrates what has changed in the evolved approach to protecting information.

Figure 3
Evolved approach to protecting information



Source: National Audit Office analysis of government information

14 Cabinet Office, *HMG Security Policy Framework*, April 2014, available at: www.gov.uk/government/publications/security-policy-framework

The Cabinet Office's progress in protecting information

1.21 As part of the move away from taking a prescriptive approach to protecting information, the Cabinet Office has tried to take a more strategic role in offering support and guidance to central government departments. However, senior-level governance remains complex and unclear and, until recently, a wide array of central teams have been involved in information assurance and protecting information, sometimes offering overlapping and contradictory advice.

1.22 Central governance of security, which includes overseeing the protection of information, is unclear. There are several lines of accountability and senior oversight, with little coherence between them. These include the Official Committee on Security (which meets at permanent secretary level), the National Security Council Cyber and Resiliency subgroups (ministers and officials) and the Information Risk Advisory Board (the IRAB), which has not met for almost two years. There are also a plethora of working-level groups, including those to support modernising government and digital working. Although the IRAB is the group most clearly identified with information security it has little influence and no formal connection to the Official Committee on Security. As part of the programme to modernise security, the Cabinet Office is undertaking a review of governance and accountability with the aim of simplifying the structure underneath the Official Committee on Security.

1.23 As at April 2016, at least 12 separate teams or organisations had a role in protecting information. These are illustrated in **Figure 4**. They include: the Centre for Cyber Assessment (CCA); the Crown Commercial Service (CCS); CESG; the Computer Emergency Response Team (CERT-UK) and its internal government counterpart GovCertUK; the Centre for the Protection of National Infrastructure (CPNI); Government Communications Headquarters (GCHQ); Government Digital Service (GDS); the Government Security Secretariat (GSS); the Office of Cyber Security and Information Assurance (OCSIA); the Office of the Government Senior Information Risk Owner (OGSIRO); and the UK National Authority for Counter Eavesdropping (UKNACE).[15]

1.24 Failure to coordinate this work has meant that a large number of bodies continue to have overlapping mandates and activities. In November 2015, the then-Chancellor of the Exchequer noted this problem and the need to: "address the alphabet soup of agencies involved in protecting Britain in cyberspace".[16]

15 A full list of bodies and their responsibilities is set out in the Glossary at page 42.
16 HM Treasury, 'Chancellor's speech to GCHQ on cyber security', November 2015, www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

Figure 4

The Chancellor's 'alphabet soup' of bodies at the centre of government

● Central bodies involved in information assurance activity

Note

1 See Appendix Three for the glossary of departmental and central bodies' names.

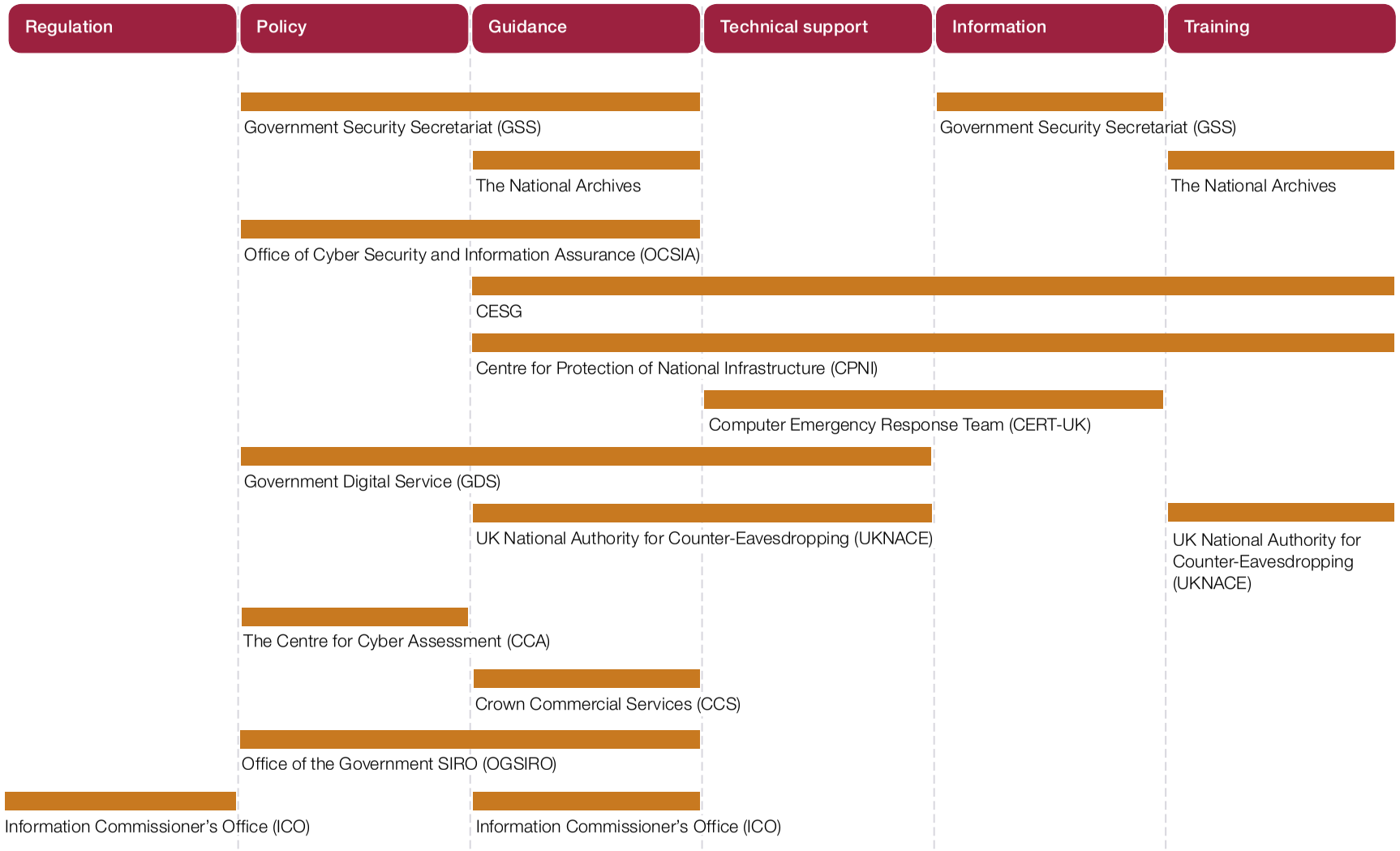
Source: National Audit Office analysis of government information

1.25 As well as confusion about the range of bodies involved in protecting information, there is also misunderstanding about the dissemination of policy, guidance and advice (**Figure 5** overleaf). Until recently, several organisations have produced security policy in some form, including GSS (which is responsible for the *HMG Security Policy Framework*); OGSIRO (policy regarding holding information outside the United Kingdom, known as 'offshoring') and GDS (the role of security within government's technology strategy). CESG and CPNI also produce guidance that departments often interpret as mandatory.

1.26 There is no clear division of responsibility between these organisations, which makes it difficult for departments to know where to turn for pragmatic security advice or what to do when they receive conflicting advice. None of the departments we interviewed understood the specific roles of the various bodies involved, making it difficult to identify any single arbiter of standards or guidance.

Figure 5

The various bodies or teams with whom public sector organisations interact to protect their information



Note

1 See Appendix Three for a glossary of organisations and description of their activities.

Source: National Audit Office analysis of government information

The Cabinet Office's response

1.27 Given all the challenges identified above, the Cabinet Office has taken a number of steps to reduce duplication, simplify guidance and optimise the employment of scarce numbers of skilled security staff and resources to improve how information is protected across government.

1.28 In March 2016, it completed an internal review of government security: its central finding was that 'government's existing security structures and roles will not adequately support the next phases of our cyber security, workplace and digital strategies' – an assessment which the evidence of our work supports.

1.29 The review's recommendations are now in the first stages of implementation. The Cabinet Office is now combining the roles and remits of OCSIA, GSS and OGSIRO into a single organisation – the Cyber and Government Security Directorate – and has created the post of Government Chief Security Officer to lead it. The post-holder will be responsible for all aspects of government protective security.

1.30 In addition, the government has announced the establishment of the National Cyber Security Centre (NCSC). This new body will combine the roles of CESG, CERT-UK and GovCertUK, CCA and relevant functions from CPNI.[17] The NCSC is designed to support government and the private sector: whether it has the capacity to do so effectively remains to be seen. The scale and pace of the challenges of protecting information are such that these structural changes are unlikely to be sufficient unless the Cabinet Office can also support departments in addressing some of the problems we set out in Parts Two and Three.

17 HM Government, *Prospectus Introducing the National Cyber Security Centre*, May 2016, available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf

Part Two

Performance of the centre

2.1 This Part examines the impact of the Cabinet Office's support to departments, as well as departments' own performance in a number of critical areas. These are: government's performance in protecting information; security breach reporting; managing strategic information risks; and the performance of centrally managed projects.

Government's performance in protecting information

2.2 There has been a considerable increase in the volume of cyber attacks – the number of incidents dealt with by GCHQ per month which threatened UK national security doubled to around 200 between 2014 and 2015.[18] Prior to October 2015, the Cabinet Office did not collect information on or analyse government's performance in managing the risks of protecting information on a routine basis. This means it has had little visibility of information risks in departments and has limited oversight of the progress departments are making to better protect their information. Since then it has run a programme to capture data about information risk, about which we say more in paragraph 2.21.

2.3 With the possible exception of bodies involved in national security or protecting critical national infrastructure, the centre of government has few mechanisms for understanding whether the procedures departments are putting in place to assure their information are adequate. This makes it more challenging to assess specific risks to some departments as well as aggregate risks across the whole of government. This will become increasingly challenging as more information is shared across government, as the protecting information arrangements of the weakest organisation could expose other departments.

18 HM Treasury, *Chancellor's speech to GCHQ on cyber security*, November 2015, available at: www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

2.4 It is the responsibility of individual departments to set their own programmes for risk management exercises, supported by a number of programmes run from within the Cabinet Office, but practices vary. Some departments, such as the Department for Work & Pensions (DWP), have run risk management exercises to understand their information risks, involving both senior management and technical staff. DWP applies a proactive approach to breach readiness and the protection of its information assets. This involves benchmarking its security against industry and other standards and taking a holistic approach to risk management that supports business agility, security policies and a more accurate understanding of the aggregated risks to the department's information assets.

2.5 There is also a balance between adopting new technologies and developing new processes to exploit the potential benefits, and vice versa. For example, the Cabinet Office is adopting new technologies, such as Gmail and Google Apps, and its staff have to develop appropriate protecting information protocols to keep pace. HM Revenue & Customs (HMRC) has adopted new approaches, such as putting information in a secure cloud system, but the challenge of achieving significant technical change with legacy systems has made this a complex undertaking.

Security breach reporting

2.6 Formal reporting of security breaches might make risks clearer to departments. However, current processes are dysfunctional. Departments must report data breaches in their annual reports, but each organisation reports its breaches in different ways. Knowledge gained from incidents is therefore not effectively shared across government. For example, the Ministry of Defence has established a dedicated reporting mechanism for dealing with suspicious emails, but this good practice has not been adopted across other departments.

Protecting personal data

2.7 The Cabinet Office is not responsible for public bodies outside central government, so does not collect data on their breach incidents. However, when the security of personal data is breached, departments and other public bodies decide what to report to the Information Commissioner's Office (ICO), in line with the requirements of the Data Protection Act. Apart from communication service providers, such as BT and TalkTalk, public and private organisations do not have to report personal data breaches to the ICO.

2.8 The 2014-15 set of annual reports from the 17 largest departments record data incidents that they regard as either ICO-reportable or non-reportable breaches (**Figure 6** overleaf). Departments recorded 14 ICO-reportable incidents, and a further 8,981 non-ICO reportable incidents. Five departments reported no data losses in either category. The lack of detail in the self-reporting data means it is not possible to determine how significant any of the 8,981 incidents were. The data reflect public reporting as signed off by accounting officers and highlight major variations in incident reporting processes across departments.

Figure 6

Number of 2014-15 data incidents reported/not reported to the ICO from the 17 largest departments

Department	Incidents reported to ICO	Incidents recorded by departments but not reported to ICO
HM Revenue & Customs[1]	3	6,038
Ministry of Justice[2]	3	2,798
Department for Work & Pensions	2	0
Cabinet Office[3]	1	–
Department for Education[4]	1	14
Department for Environment, Food & Rural Affairs[5]	1	33
Department for Transport	1	6
Foreign & Commonwealth Office[6]	1	2
Ministry of Defence	1	50
Department for Business, Innovation & Skills[3,7]	0	–
Department for Communities and Local Government	0	2
Department for Culture, Media & Sport[3]	0	–
Department of Energy & Climate Change	0	0
Department for International Development	0	0
Department of Health[8]	0	5
Home Office[9]	0	33
HM Treasury	0	0
Sub-totals	**14**	**8,981**
Total		**8,995**

Notes

1 HM Revenue & Customs data for incidents recorded by the department but not reported to the ICO includes 6,000 minor incidents that potentially had an impact on customers but were not managed centrally by the department.

2 Ministry of Justice figures for incidents recorded by the department but not reported to the ICO relate to those that were deemed by the data controller to not fall within the criteria for reporting to the ICO. These figures include those for the Ministry's arms-length bodies as well.

3 These departments did not include data in their annual report and accounts on any incidents that they had recorded centrally and not reported to the ICO.

4 Department for Education data are for the department and its executive agencies only.

5 The Department for Environment, Food & Rural Affairs data are for the core department, executive agencies, non-departmental public bodies and the Forestry Commission.

6 The Foreign & Commonwealth Office data are for the core department only.

7 The return for the then-Department for Business, Innovation & Skills (now part of the Department for Business, Energy & Industrial Strategy) data includes core department and partner organisations within the accounting boundary.

8 The return from the Department for Communities and Local Government reflects data updated since the publication of their annual report.

9 The Department of Health data are for the core department only.

10 The Home Office data are for the core department and HM Passport Office only.

Source: Departments' annual report and accounts 2014-15

2.9 These data do not match the ICO's own records of public bodies' personal data breaches, which relate to incidents reported directly by departments to the ICO, or cases set up in response to complaints or other intelligence sources.

2.10 As regards incidents reported to the ICO, many incidents involve an element of human error (such as sending information to the wrong person) but that nevertheless reflect a lack of appropriate organisational controls. **Figure 7** overleaf shows the different kinds of breaches.

2.11 As part of its role as the regulator of the Data Protection Act, the ICO can impose penalties on organisations that breach any of the eight data protection principles, including that relating to the security of personal data. Penalties can be imposed in cases where there has been a serious breach of the Act, which has the potential to cause substantial damage or distress to those affected.

2.12 The current arrangements for fines and reporting personal data breaches could be significantly extended in 2018, assuming that the United Kingdom introduces the Europe-wide General Data Protection Regulation. These reforms will bring in mandatory reporting of personal data security breaches, and significantly larger fines. This means departments need to begin work now to adopt more clear and consistent reporting, to learn and share lessons, and to reduce the number of breaches so that they can avoid these significant fines.

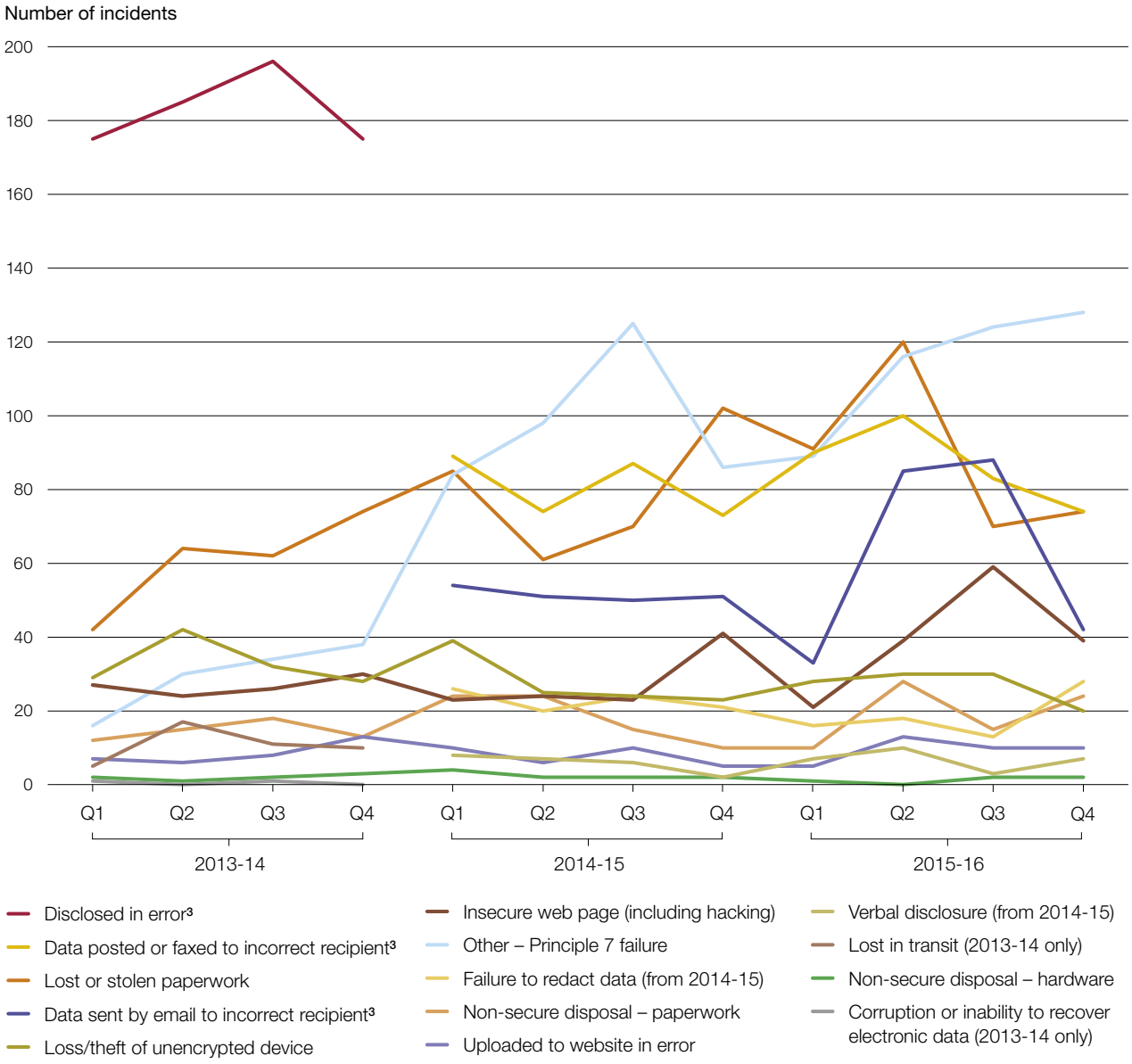
2.13 By sector, health consistently had the largest number of breaches (**Figure 8** on page 25). These figures offer limited information about relative risk, however, as each organisation reports in different ways. For example, unlike the rest of government, the Department of Health insists that all personal data breaches must be reported. These are collated through its Information Governance Toolkit (IG Toolkit). Level 2 breaches on the IG Toolkit automatically result in a report to the ICO through the Information Governance Serious Incidents Requiring Investigation (IG SIRI) reporting tool. The Department of Health has also suggested setting up a network across government to learn from 'near misses' of personal data, but this has not been adopted.

2.14 Automatic reporting of personal data breaches and all incidents at Level 2 and above may be why the health sector is registering more breaches than other sectors. Data trends over time, rather than relative positions between sectors, may therefore be a more meaningful indication of progress in addressing information risks. The Department for Health also believes that organisations that have high reporting rates are more likely to be safer, as a culture of reporting incidents and near misses allows the early identification of threats.

Figure 7

Trends in data security incidents by type by quarter from April 2013 to March 2016

Throughout the period the number of Principle 7 breaches has continued to grow



Notes

1 These figures relate to the period April 2013 to March 2016.

2 'Other Principle 7 failures' are security incidents that cannot be categorised as one of the other types. Examples include failure to password protect emails containing personal information, use of the carbon copy function in an email rather than blind carbon copy, and processing personal data relating to work on a non-business computer.

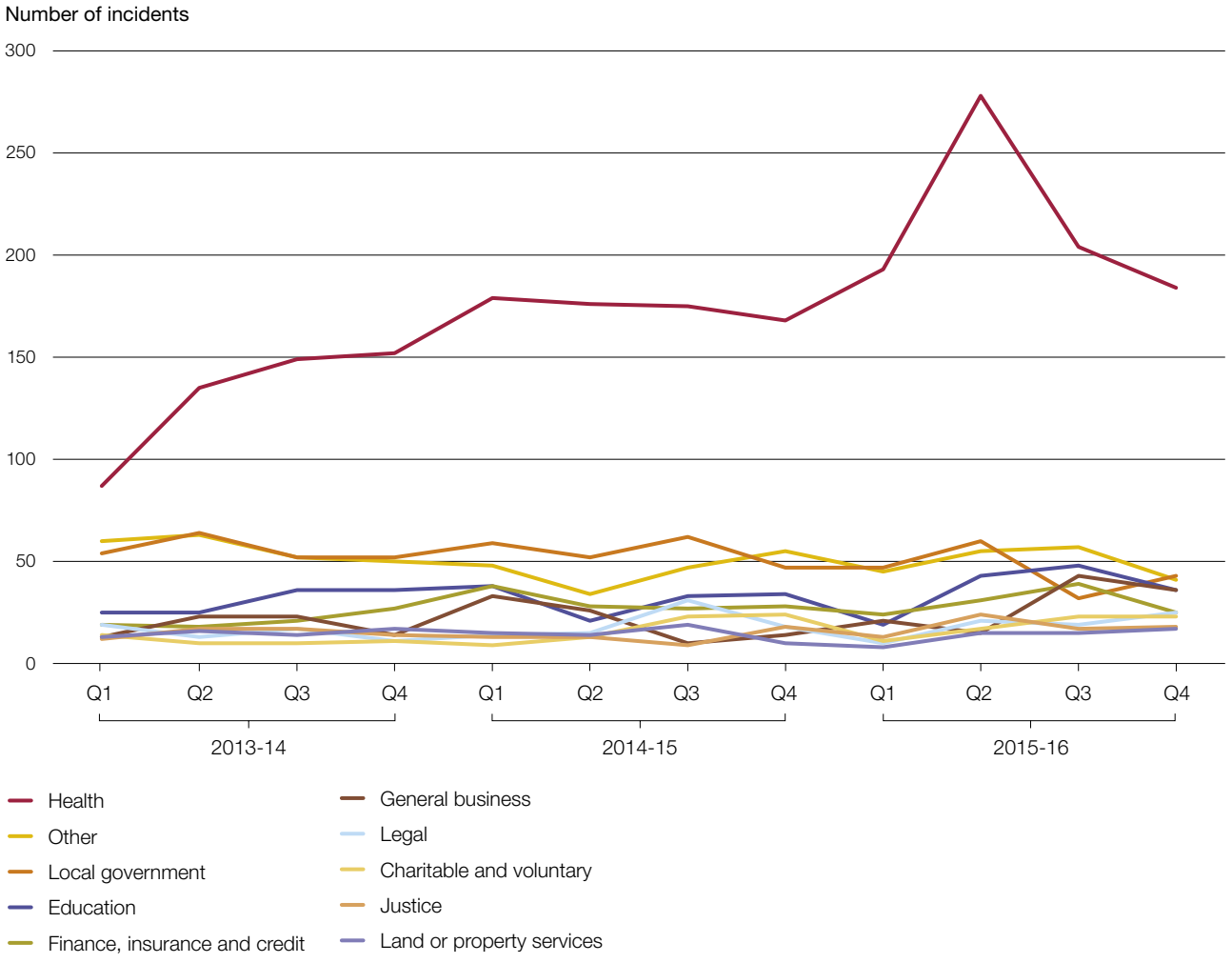
3 From 2014-15, the category 'Disclosed in error' was split into two new categories: 'Data posted or faxed to incorrect recipient' and 'Data sent by email to incorrect recipient'. Hence there is a break in categories between Quarter 4 2013-14 and Quarter 1 2014-15.

Source: Information Commissioner's Office, *Data security incident trends*, June 2016

Figure 8

Trends in data security incidents by sector by quarter from April 2013 to March 2016

Automatic reporting of health sector breaches has resulted in a high level of incidents declared to the ICO



Note

1 These figures relate to the period April 2013 to March 2016.

Source: Information Commissioner's Office, *Data security incident trends*, June 2016

2.15 As indicated in Figure 8, there was a peak of cyber activity in the heath sector in the second quarter of 2015-16. Previously, the centre had not considered health to be a high-threat sector for cyber attacks, despite the ICO trend data consistently indicating breaches, since most of these were losses of paper records.

2.16 Once the scale of this activity was clear, the Department of Health received technical assistance from the centre of government, which it believed was extremely helpful. The Department of Health established its own Care Computer Emergency Response Team (CareCERT) in autumn 2015 to identify threats and respond, and the cyber threat is now taken more seriously throughout the sector.

2.17 The Cabinet Office's National Cyber Security Programme (NCSP) provided funding of £2.5 million in 2015-16 to set up CareCERT to support the 46,000 health bodies in the UK.[19] The next phase of the programme – NCSP2 – has provided £2.3 million in 2016-17 to extend CareCERT further, including an e-training platform for health and social care staff, on-site testing of the cyber defences of local health and social care organisations, and producing advice and guidance. Further NCSP funding is dependent on CareCERT proving successful and beneficial for the health and social care system.

2.18 The health and care system poses unique challenges in the context of cyber security. The system employs around 1.6 million people in more than 40,000 organisations, each with vastly differing information security resources and capabilities. To address these concerns, the role of the National Data Guardian for Health and Care was established by the secretary of state for health in November 2014.

2.19 The secretary of state asked the National Data Guardian to contribute to a review of data security being carried out by the Care Quality Commission (CQC), including to develop new data security standards that can be applied to all health and care organisations; and, with CQC, develop a method of testing compliance with the new standards. The review was published on 6 July 2016, alongside a government consultation on how to take forward the proposed new data security standards, closing 7 September 2016.

Managing strategic information risks

2.20 The centre is trying to improve its understanding of strategic information risks to better protect government. To mitigate its limited visibility of these risks the Cabinet Office has always required departments to submit an annual information security return. However, these have been highly variable in quality, take more than eight months from issuing to departments to collation by the centre, and have not included quantified measures that could give a picture of trends. The Cabinet Office is updating the template to generate more quantifiable feedback that it can use to better address information risks.

2.21 The Cabinet Office has been running a programme since October 2015 designed to capture data about information risk across government. To support this, CESG has published 15 good practice principles to define the basic protective measures for bulk data systems.[20] Evidence from departments suggests that they do not always have in place the controls recommended by CESG, particularly for their legacy IT systems. One issue of concern is patching, where parts of central government use software that is no longer being supported by the manufacturer or have older IT contracts which do not support regular system updates.

19 Comptroller and Auditor General, *Update on the National Cyber Security Programme*, Session 2014-15, HC 626, National Audit Office, September 2014. Available at: www.nao.org.uk/report/update-on-the-national-cyber-security-programme/

20 CESG, *Protecting Bulk Personal Data*, July 2016, available at: www.cesg.gov.uk/guidance/protecting-bulk-personal-data

The performance of centrally managed projects

2.22 The centre is managing a number of projects designed to enable government to better manage its information. Three initiatives – the Government Security Classifications (GSC) system, the Public Services Network (PSN) and the Foxhound project – illustrate the challenges the Cabinet Office faces in implementing centrally managed projects.

2.23 These projects comprise considerable technical, business change and cultural challenges but have been slow to deliver their planned benefits. In addition, alongside their primary objectives, all three projects were intended to achieve significant financial savings. However, poor planning means that the Cabinet Office does not know if these savings have been delivered.

The Government Security Classifications system

2.24 Historically, the Government Protective Marking Scheme used a six-point system to classify information.[21] These markings instructed users on how to handle and protect information and were designed for the protection of paper documents. However, in recent years, the system was not applied consistently across government. Its six classification levels, and the bespoke infrastructure designed to meet unique government requirements, were considered relatively expensive to maintain, although the government has never provided a cost for this support.

2.25 In April 2014, the government introduced the GSC. This has a three-point classification scale, with limited comparability with the previous system.[22] The Cabinet Office had a clear vision of the benefits of introducing a simplified classification system. Crucial to its success would be the use of a single, lower tier of security classification (Official) to allow departments to replace expensive, bespoke IT with more flexible and cheaper commercially available systems. Applied across the whole of government, it would simplify arrangements for sharing information across government and with citizens.

2.26 The new system has been implemented across central government but there is inconsistent take-up within the wider public sector. In a 2015 poll of senior information risk owners (SIROs) from across the public sector, fewer than half (44%) said they understood how to operate effectively within the new classification system. The Cabinet Office does not know what impact this inconsistent understanding has had on the ability of central and local government to work together.

2.27 Despite more than two years of policy development and communications, departments were poorly prepared for the implementation of the GSC. Many have seen the benefits of implementing the new system, but some still have concerns about their ability to protect information. There is considerable confusion about how to use the classification system properly and misunderstanding about the requirements for securely transmitting and storing information classified as Official outside government networks, including the use of cloud and encryption services.

21 These classifications were: Unclassified; Protect; Restricted; Confidential; Secret and Top Secret.
22 These classifications are: Official; Secret and Top Secret.

2.28 This confusion is undermining departments' ability to assure the information correctly. For example, with no Unclassified level, some departments are treating Official and Unclassified in the same way, moving information freely across the internet and using personal email accounts. Other departments insist on sending Official information only between encrypted departmental accounts.

2.29 Some departments, including parts of the Cabinet Office, use the suffix 'Sensitive' after certain Official documents to indicate handling requirements that are similar to Official, but enhanced. However, some departments treat it as a higher classification level than Official. The Foreign & Commonwealth Office (FCO) applies the GSC but acknowledges that some users still equate Official – Sensitive to the old classification of Restricted. This is being addressed through training and communication activities.

2.30 It is not always straightforward to use the GSC alongside marking systems employed by other organisations which do not match GSC markings, although this problem predates its introduction. The Cabinet Office tried to mitigate this issue with additional handling instructions but adoption of good practice is still patchy. This means that staff can look for an equivalent definition, leading to additional marking which then undermines the simplicity of the GSC system. The result is that there is no common understanding of each classification, nor agreed handling protocols. This potentially undermines each classification's security status as it moves between – and is re-interpreted by – staff in different departments.

2.31 The business case for the GSC was not based on achieving financial savings. It stated, however, that as most of government information was classified as Official, replacing former systems supporting Unclassified, Protect, Restricted and parts of Confidential with a single system could lead to significant future savings. The use of commercial, rather than government, encryption at Official level would also benefit from existing investment rather than expensive, bespoke solutions.

2.32 The strategic business case for the GSC used industry comparators to estimate savings each year of between £110 million and £150 million. However, it noted that a more detailed financial business case should be completed. The Cabinet Office has not done this, nor did it do any alternative analysis. As a result, it cannot say whether the financial benefits are being delivered as planned.

The Public Services Network

2.33 The PSN is the successor to the government secure intranet (GSi). The PSN is used by central government departments, local authorities and other public sector bodies. It is the responsibility of the Cabinet Office and is delivered by service providers, such as BT, that are approved to supply connections and services over the PSN.

2.34 The PSN project initially had two objectives:

- to provide an assured network over which central and local government could safely collaborate and share services for the benefit of citizens; and
- achieve substantial government cost savings. In 2010, the government forecast that "The public services network will deliver at least £500 million (of) savings per year by 2014".[23] The *PSN business case update 2011-12* revised this estimate to between £200 million and £400 million per year by 2014.

2.35 Initially, the entry standard for departments to join the PSN was substantially tightened compared with the GSi, both to address the weaknesses of an ageing GSi and because the PSN aimed for a greater sharing of – and therefore potential risks to – government services.

2.36 However, the increased security requirements, for example around encrypting data, proved problematic and too costly for many local authorities. For example, many local authority staff used mobile digital devices that represented 'unsecured endpoints', potentially allowing unauthorised access to the PSN.

2.37 Consequently, many authorities were initially refused connection to the PSN. The project team responded by changing some of the criteria, for example by establishing encrypted and non-encrypted functions. The last local authority joined PSN in September 2014, six months after the deadline. Any organisations that now fail to meet PSN security standards are not removed from the network but are supported in addressing weaknesses.

2.38 However, this means that the vision of a single secure network is no longer an objective, eroding the ease of data-sharing. As well as the differing security standards of those on PSN, recent changes allow departments and local authorities to opt out of PSN and choose their own network.

2.39 Where the PSN has not hindered data-sharing it has added costs in some departments as they have required additional security features to be able to share data, although these are not netted off against the PSN savings declared by central government.

2.40 The PSN's other objective was to save money. Against the original savings target of £500 million – and the revised target of £200 million to £400 million – per year by 2014, the PSN's declared savings from central government have been: £60 million in 2011-12; £127 million in 2012-13; £116 million in 2013-14; and £103 million in 2014-15. The PSN team does not anticipate making any more savings against the original PSN baseline. However, the current infrastructure was designed to support the original, more secure PSN, and government is now looking to change this to reduce costs to better match the new PSN requirements.

23 HM Government, *The Government ICT Strategy – Smarter, cheaper, greener*, January 2010, p.13, available at: http://webarchive.nationalarchives.gov.uk/+/http:/www.cabinetoffice.gov.uk/media/317444/ict_strategy4.pdf

Foxhound

2.41 The Foxhound project was originally designed to deliver a single, secret network across government by April 2014. It aimed to provide improved security and functionality, while offering considerable cost savings by replacing many older systems. As a more secure system offering mobile and remote access, Foxhound was designed to replace 15 separate confidential networks and other classified systems. Against its original aspirations, the system is three years late and not on track to deliver the £308 million of anticipated benefits over 10 years. It is clear, therefore, that the original business case was optimistic in assuming that technical and funding issues could be addressed quickly enough to ensure that the system was in service by 2014.

2.42 Although the project's core objectives remain, the original aspirations for when they would be delivered were re-set in 2014, when the Cabinet Office took steps to put the project on a new footing. The resulting outline business case – submitted and agreed in 2015 – revised the scope and schedule of the project and projected savings of £398 million over 10 years when set against an industry comparator. There is now a central budget of £50 million to develop Foxhound, which was approved as part of the 2015 Strategic Defence and Security Review.

2.43 With the agreement of the permanent secretaries who sit on the Official Committee for Security, the Cabinet Office decided it was best placed to manage this project as the technical requirements were demanding and it could use the concentrated skills and expertise of its staff to deliver it rather than depend on one department to do so. A team is now in place to deliver the technology, a managed service and the necessary business change and training across an initial 11 partner departments.

2.44 The technology to support Foxhound is being developed using agile methodology and the first iteration – a live proof of concept – is currently being used in the Cabinet Office and three other departments. The Cabinet Office expects an initial roll-out from mid-2016. It plans to deliver the full mobile, remote-access capability incrementally, when it has addressed remaining technical and security challenges. In the absence of Foxhound there has been a gap between Official and higher classification information. This both increases the risk of information being compromised and adds costs supporting a range of legacy systems.

Part Three

Departmental performance in protecting information

3.1 This Part assesses the performance of central government departments (the departments) by examining: governance in departments and delivery chains; the financial impact of the revised approach to protecting information; and deploying people with the right skills.

Governance in departments and delivery chains

3.2 Many departments have told us that it is a significant challenge for their boards and senior staff to fully understand their changing responsibilities for protecting their information. There is varied practice in how ministers and non-executive directors use IT and access departments' networks and we found several examples of practices which did not conform to departments' information security policies. Many senior staff were also unaware of the arrangements for protecting their information in other parts of their organisation, such as in arms-length bodies.

3.3 Although some departments have made significant progress in improving their senior staff's governance of information protection, many decision-makers lack relevant experience. Our recent survey of digital skills in government showed that most digital leaders did not sit on their department's main board and that there was a need to improve both the capacity and capability of staff involved in protecting information.[24] There are no professional standards, and traditionally the protecting of information has not been given the same attention as other disciplines such as procurement or finance by boards and audit and risk committees.

3.4 Audit and risk committees can also provide assurance on protecting information for boards, but their potential has yet to be fully realised. Audit and risk committees are designed to hold boards to account, for example on financial, legal and other regulatory matters. HM Treasury's advice is that at least one member of the committee should have recent financial experience and ideally be financially qualified. There is no equivalent requirement for experience in protecting information.

24 National Audit Office, *The digital skills gap in government: survey findings*, December 2015, available at: www.nao.org.uk/report/the-digital-skills-gap-in-government-survey-findings/

3.5 Finding the balance between exploiting and protecting the information that organisations hold is a board-level responsibility. The National Archives, which provides information assurance training for boards, and a number of non-executive directors across government told us that boards' discussion on risk appetite can be limited. Boards struggle to know who to include in any discussion on information risk, and therefore how to understand and agree a tolerable level of that risk. This situation may become more complicated as efforts to improve cost-effectiveness and give citizens better access to information will result in more data being shared between departments.

3.6 There are examples of improving practice in this area. The Department of Health has agreed with the Cabinet Office that health information is a critical organisational risk. The Department of Health has worked with CESG to categorise those risks using a new risk framework. Previously, departments had been left to determine the magnitude of their own risks. The Department of Health was able to reduce its critical risks from 15 to one. This should allow it to focus its resources more effectively. The Department for Work & Pensions (DWP) has joined up the traditionally separate strands involved in information assurance, such as its digital, security, assurance and management bodies, to better understand its risks.

3.7 The government uses departments, their arms-length bodies and the private and voluntary sectors to provide its services through supply or delivery chains.[25] The values of these chains can be considerable. More than 86% of the Department of Health's £123 billion budget for 2014-15 was spent outside the core department, so it is critical that appropriate arrangements, involving a mix of public and private delivery partners, are in place to protect information wherever it is used.

3.8 Assuring supply chains is more challenging than protecting information within the centre of government. The government recently reported that supply chains "will be hit hard" if they have weaker cyber security measures than their customers.[26] The longer the supply chain, the more challenging it is to understand the information risks and the measures put in place – particularly if they reside in the private sector where the government has no automatic jurisdiction. In addition, many small and medium-sized enterprises cannot afford to provide the level of security required for securing government information.

3.9 The threat to government supply chains and delivery partners is considerable, and increasing. The *2015 Information Security Breaches Survey*, commissioned by the government, reported that 90% of all large UK organisations suffered a security breach in 2015 – up from 81% in 2014.[27] More than two-thirds (69%) of large companies were attacked online by an external threat in 2015, up from 55%. The average rate of breaches was more than one per month, at an average cost of between £1.46 million and £3.14 million, up from £600,000 to £1.5 million in 2014.

25 An arm's-length body is an organisation that delivers a public service, is not a ministerial government department and which operates to a greater or lesser extent at a distance from ministers.

26 CERT-UK, *Quarter Two Report*, July – September 2015, www.cert.gov.uk/wp-content/uploads/2015/11/CERT-UK-Quarterly-Report-Jul-Sept-2015.pdf

27 HM Government, *2015 Information Security Breaches Survey*, 2015, available at: www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

3.10 The government has made available guidance, such as the *10 Steps to Cyber Security* and *Cyber Essentials*, and practical assistance via the Cyber-security information Sharing Partnership (CiSP), which shares cyber threat information with more than 1,500 companies. This service is run through the national Computer Emergency Response Team (CERT-UK) and both the Ministry of Defence and Department of Health have their own sector-specific CERT teams.

3.11 However, in line with the delegation of protecting information responsibilities, these measures are voluntary for departments, and uptake is variable. The Ministry of Defence, through its Defence Cyber Protection Partnership, employs both CiSP reporting and *Cyber Essentials* with its delivery partners, allowing it to set a baseline for information security across its activities and more easily identify any weak links in the supply chain.

3.12 However, apart from a single specialist information assurance expert, all departmental staff we spoke to were confused by the differences between *10 Steps to Cyber Security* and *Cyber Essentials*, as well as the ISO 27001 information security management system, which some organisations accredit against. At a recent conference for security professionals, while most of the audience were aware of *Cyber Essentials*, only around a quarter were using it.

3.13 The Cabinet Office recognises that it is too removed from departmental business to be prescriptive about how supply chains are assured, but it is apparent that the government can do more. Information protection considerations could be built into all relevant government contracts as part of the service provision. For example, contracts could require the use of ISO standards, *Cyber Essentials* or *10 Steps to Cyber Security*, as appropriate. This could cover issues such as minimum software standards, as patching in government and the supply chain is sporadic. For example, the government had eight years' warning before Microsoft stopped supporting Windows XP in April 2015.[28] But by that time the Metropolitan Police reportedly had 35,000 computers still running XP, as do most of the nearly 10,000 GP practices across the UK.[29]

The financial impact of the revised approach to protecting information

3.14 For the centre of government to take strategic decisions on protecting information, and departments to take a risk-based approach to protecting their information, detailed figures on expenditure and the benefits of current activities and projects are required. We found no single body responsible for this and no central set of management information covering this area. The costs of protecting information across government are therefore unclear.

28 Microsoft stopped support for general users in 2014, but the UK government paid £5.5 million for a year's extension to April 2015.

29 Available at: www.computing.co.uk/ctg/news/2406063/met-police-still-using-windows-xp-on-over-35-000-of-its-desktops-and-laptops

3.15 As part of its March 2016 security review, the Cabinet Office gathered some financial and other information on how much government spends on protecting information.[30] Returns from 34 departments (of 44 ministerial and non-ministerial bodies) reveal that there are at least 1,600 staff undertaking security (information, physical and personnel) roles (**Figure 9**).

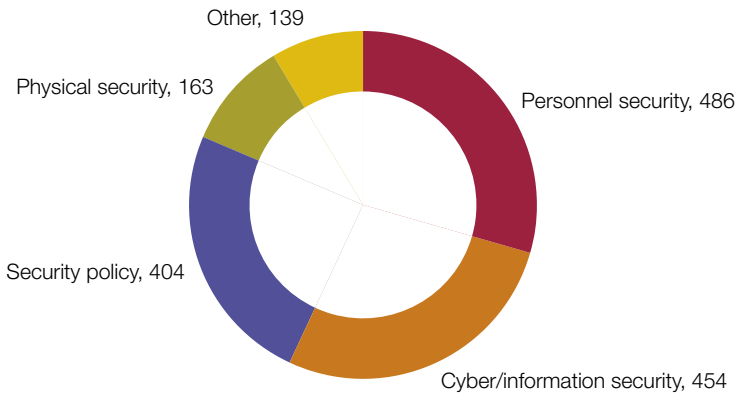
3.16 The Cabinet Office also estimated that expenditure by these 34 departments on protective security was at least £300 million annually. However, it noted that the true figure could be several times higher because many departments cannot separate spending on cyber and physical security from IT and estates contracts. Also, the estimate does not include the costs of securing the government's overseas estate and infrastructure, such as embassies and consulates.

External support costs and sharing benefits across government

3.17 The Cabinet Office's March 2016 review estimated that departments will spend £28 million on external IT security consultants in 2016. One effect of departments taking more of a risk-based approach to protecting their own information has been that they have to make decisions about the cost-effectiveness of accessing security advice in different ways. Where departments are deciding to use private sector consultants it is usually because they lack sufficient numbers of skilled information security professionals of their own. It can also be because some departments do not properly understand their own security needs. As a consequence, they cannot take a risk-based approach to protecting their information or act as an intelligent customer for external support.

Figure 9
Government security staff

Estimated breakdown of government staff across security areas



Source: Government Security Secretariat, *Transforming Government Security: Review*, March 2016

30 Government Security Secretariat, *Transforming Government Security: Review*, March 2016.

3.18 One vital role for which departments often use private sector support is for the accreditation of IT systems. This was previously often carried out by consultants who were part of the CESG Listed Adviser Scheme (CLAS). In 2015, the government scrapped this scheme because they considered it costly and largely focused on accrediting against generic standards, rather than encouraging a risk-based approach to information security.

3.19 Departments are now more able to define their requirements and select appropriate solutions. Some of our interviewees – such as Companies House – welcomed this freedom. They understood their business sufficiently to know what services they needed, recently constructing a digital performance platform.[31] Others, however, either did not have the expertise to implement the Cabinet Office's risk-based approach, or were unable to secure the right external support. For example, CESG tried to re-focus CLAS consultants to take a risk-based approach to protecting information in departments, but claimed their quality was too variable. CESG has now introduced a CESG Certified Professional Scheme, which is designed to ensure that members have the necessary skills to discharge information adviser roles at different levels, depending on their experience.[32]

3.20 In addition, departments do not often share advice and knowledge effectively across government, either resulting in them repeating work at additional cost or missing the opportunities presented by adopting new technologies. For example, the Cabinet Office has adopted Google Apps, but the formal accreditation has not been shared effectively across government, and few other departments yet have the risk-based skills to adopt this or any other commercial technology.

Deploying people with the right skills

3.21 The increasing use of digital systems and the changing security landscape has placed additional requirements on departments to deploy staff with the skills to design, develop and operate all aspects of protecting information. This applies both to handling data in joined-up government operations and to building, buying and operating appropriately secure infrastructure and systems.

3.22 In recent years, demand in the private sector for digital and cyber skills has grown significantly. This leaves departments facing challenges in trying to develop capability and capacity, as they are usually unable to match the financial and other benefits offered by private sector companies. We have reported previously that the UK has a shortage in digital and cyber skills. Industry and the government are competing for the same scarce staff.[33] The government also reduced staff in all areas over this time and this has resulted in the loss of some expertise.

31 Companies House, *Big insights: collecting, analysing and presenting data*, blog, May 2016, available at: https://companieshouse.blog.gov.uk/2016/05/31/big-insights-collecting-analysing-and-presenting-data/

32 CESG, *Certified Professional Scheme*, October 2015, updated May 2016. Available at: www.cesg.gov.uk/articles/cesg-certified-professional-scheme

33 National Audit Office, *The Digital Skills Gap in Government: Survey Findings*, available at: www.nao.org.uk/report/the-digital-skills-gap-in-government-survey-findings/

3.23 Across central government there are 73 teams covering security (physical, personnel and technical/information), with more than 1,600 staff. However, the Cabinet Office believes there are too few staff with specialist information protection skills, and departments contract with the private sector to provide technical and consulting services as a result. The Cabinet Office's March 2016 review estimated that central departments will spend around £28 million on external IT security consultants in 2016.

3.24 There is a national shortage of skilled people available for information protection, and this is reflected in the public sector. Some departments, such as HMRC and DWP, where the consequences of a successful cyber attack are severe, have promoted these skills in-house and recruited specialist staff, but major skills shortages remain even in these departments. In 2014 DWP established a digital academy to upskill its staff, and in 2015 it invited other departments to attend its first cross-government course. In 2015-16 DWP also increased spending on technical and skills projects to increase information protection, despite tight budgets, while reducing overall expenditure.

3.25 The Cabinet Office does not know whether departments in general will have sufficient, skilled people in post as the demand for online public services grows and the cyber threat increases. In 2013 the centre responded to skilled staff shortages by setting up a government security profession. While some progress has been made to establish a core learning and development curriculum, with limited resource the profession cannot make real progress on addressing the skills shortage and define what 'good looks like' for physical, personnel and, in particular, technical security.

3.26 The National Archives, building on its experience with managing knowledge and information, provides Cabinet Office-funded training for departmental board members as well as staff who are responsible for managing information. The National Archives has found that the competence of board-level staff varies considerably. Some departments equip their non-executive directors with encrypted laptops; others use their personal email accounts, which are likely to be far less secure. Government non-executive directors that we interviewed noted that most non-executive directors were unfamiliar with their department's information risk assurance processes, and therefore unable to hold the board to account.

3.27 The departments and arms-length bodies that we interviewed all praised The National Archives for its training. As an organisation with access across government, The National Archives also offers a useful, although narrowly focused, insight into the pace of change in information assurance across government. For example, its six-week information management assessments highlight good and poor practice in departments, which can be shared between organisations.

3.28 The National Archives has also produced an online resource for all staff, as well as those responsible for protecting information. It has also trained some 7,500 staff across government. However, this work largely focuses on ensuring low-level compliance and awareness. Its work and findings are also optional for departments. Organisations with the weakest information assurance procedures are, in its view, less receptive to suggested improvements.

3.29 Below board level, we found that many departments struggled to place people with the right skills in the critical roles of senior information risk owners (SIROs) or departmental security officers (DSOs). Across government there is no mandatory training, certification or regulation of SIROs or DSOs.

3.30 Skills training for SIROs has been limited. Although some training has been provided centrally SIROs are not compelled to attend – and many fail to do so.[34] The SIRO role is always an additional responsibility for staff – there are no full-time SIRO posts – and some in government believe the task is too demanding for generalists with part-time responsibilities.[35] There is no central oversight of SIRO quality assurance, so poor performance and development needs cannot easily be identified and addressed.

3.31 At a recent conference for SIROs from across local and central government, nearly half (45%) of SIROs felt they were not adequately prepared for their role. Separately, some central government SIROs we spoke to said that they had received no guidance at all as to their responsibilities. While the majority of SIROs have some background in protection, this is often in more traditional areas such as physical and personal security.

3.32 Until recently, the centre of government recognised that there was a need to build a community of SIRO professionals, but limited progress was being made in achieving this objective. Central government support was largely focused on SIROs in the main departments, with no direct assistance to their counterparts in local government. Similarly, SIROs in arms-length bodies often received little support. One noted to us that they were excluded from the main departmental board, which hampered the flow of information through the organisation. In May 2016, the Cabinet Office began planning the formal withdrawal within central government of the SIRO role, and the development of chief security officers, which are intended to be full-time posts.

3.33 To address skills shortages and other challenges, the Cabinet Office's March 2016 review proposed pooling government's 73 existing security teams.[36] Central government will now adopt four security clusters across all departments to deliver vetting, cyber and physical security services and to communicate best practice and education for staff and boards. The first cluster will enter the pilot phase in October 2016.

3.34 Ultimately, departments remain responsible for their own information, and are best placed to manage risks and be accountable to Parliament for information breaches, so managing the risks within a cluster governance structure will need further explanation.

3.35 On sharing good practice across government, the centre does not have a formal process for identifying and sharing these benefits. For example, the Ministry of Defence has introduced specific procedures to reduce the number of successful phishing emails, although none of the other departments we spoke to were aware of them.[37]

34 Government Security Secretariat, *Transforming Government Security: Review*, March 2016, paragraph 5.7.
35 A SIRO will generally be a senior member of an organisation. They are responsible for identifying all of the organisation's information risks; agreeing the organisation's risk profile; and making sure that appropriate safeguards are in place so that the risks can be mitigated. See the definition of SIRO on GOV.UK: www.gov.uk/service-manual/making-software/information-security.html#senior-information-risk-owner-siro
36 Government Security Secretariat, *Transforming Government Security: Review*, March 2016, paragraph 2.2v.
37 Phishing is the attempt to acquire sensitive information such as usernames, passwords and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in electronic communications such as emails.

Appendix One

Our audit approach

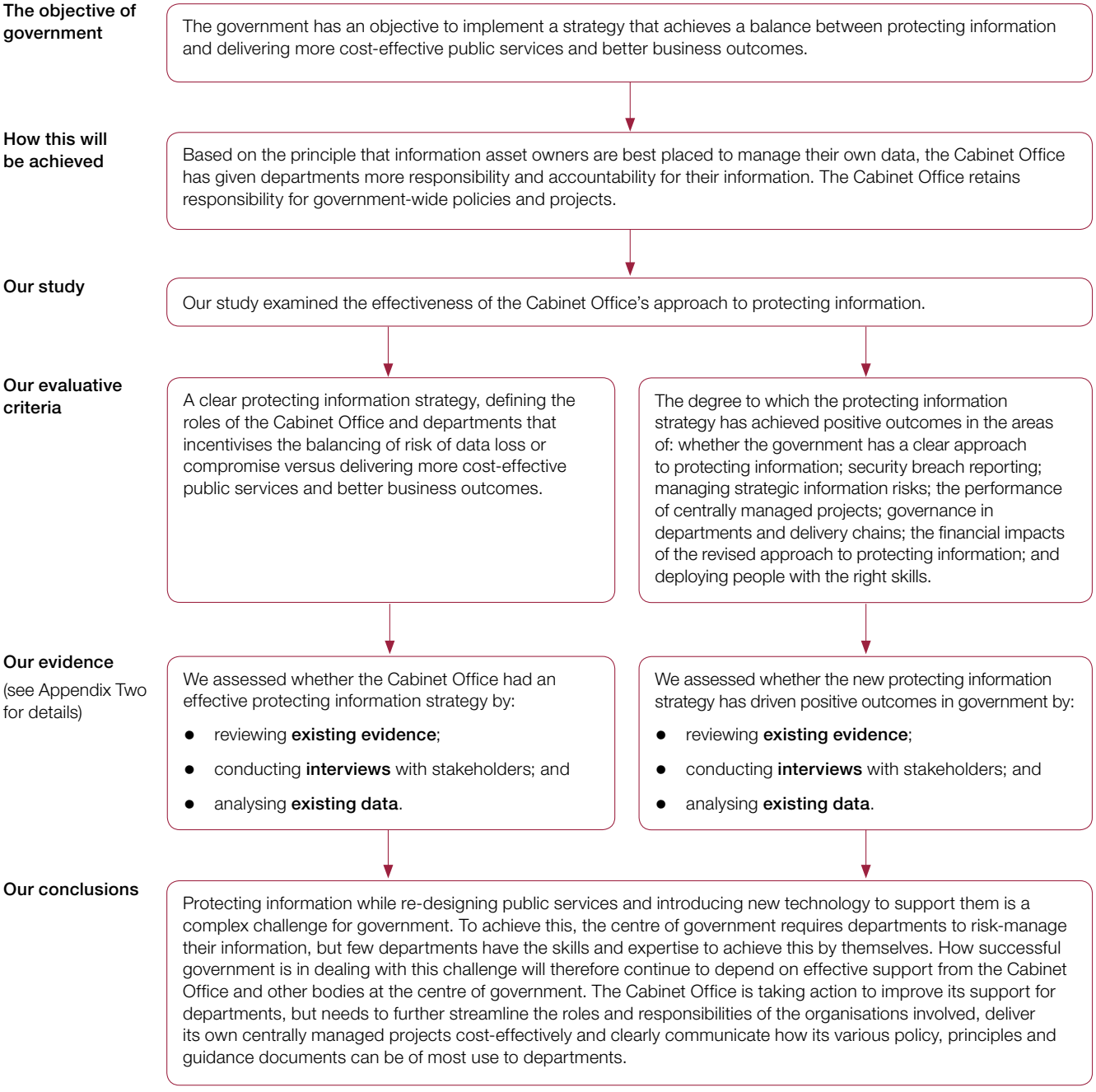
1 This study examined the effectiveness of the Cabinet Office's approach to protecting information. We reviewed:

- whether the Cabinet Office has put in place an effective protecting information strategy; and
- the degree to which central government departments are delivering against this strategy.

2 We applied an analytical framework with evaluative criteria that consider what progress Cabinet Office has made in implementing an effective protecting information strategy and how this is being implemented across government. By 'effective', we mean achieving an optimal balance between protecting information and making data available to help deliver more cost-effective public services and business outcomes.

3 Our audit approach is summarised in **Figure 10**. Our evidence base is described in Appendix Two.

Figure 10
Our audit approach



Appendix Two

Our evidence base

1 Our independent conclusions on the Cabinet Office's approach to protecting information across government were reached following our analysis of evidence collected between May 2015 and June 2016.

2 We applied an analytical framework with evaluative criteria, which consider what arrangements would be optimal for managing a system for protecting information across government. Specifically, in attempting to measure the efficiency and effectiveness of the government's approach to protecting information, we examined seven key areas:

- the government's performance in protecting information;
- security breach reporting;
- managing strategic information risks;
- the performance of centrally managed projects;
- governance in departments and delivery chains;
- the financial impacts of the revised approach to protecting information; and
- deploying people with the right skills.

3 Our study evidence was drawn primarily from the centre of government (those listed in Figure 4, which primarily included teams working in the Cabinet Office, plus others such as CESG) and central government departments. The latter consisted of the largest 16 of the 24 ministerial departments (it excluded the Attorney General's Office; Northern Ireland Office; Office of the Advocate General for Scotland; Office of the Leader of the House of Commons; Office of the Leader of the House of Lords; Scotland Office; UK Export Finance; and the Wales Office) plus HM Revenue & Customs (see Figure 6).

4 However, some of our data came from a wider government population: for example, the evidence underpinning the resources and staffing that support information security across government (Figure 9) comes from 34 government departments.

5 We have not directly set out to assess other public bodies, such as local government, NHS trusts, GP practices and the emergency services. However, some of our evidence has come from those sources, and is marked accordingly where appropriate. Nor have we examined physical and personnel security (for example, vetting).

6 Our interview schedule accordingly focused primarily on the Cabinet Office and these central government departments. We undertook semi-structured interviews with stakeholders, including a range of teams in the Cabinet Office, as set out in Part One. We then selected other departments to interview either because they were at higher risk from information security breaches or because they had particular challenges in protecting their information while changing their business practices.

Appendix Three

Glossary

Acronym	Full name	Description of activities
BIS	Department for Business, Innovation & Skills	Responsible for investing in skills and education to promote trade, boost innovation and help people to start and grow a business. BIS also protects consumers and reduces the impact of regulation.
CCA	Centre for Cyber Assessment	Responsible for producing analysis of cyber threats for government departments to inform operational and policy response.
CCS	Crown Commercial Service	Provides commercial services to the public sector, bringing together policy, advice and direct procurement.
CO	Cabinet Office	Responsible for supporting the Prime Minister and ensuring the effective running of government. Takes the lead in certain critical policy areas.
CERT-UK	Computer Emergency Response Team	Responsible for national cyber security incident management as well as some elements of international cooperation.
CESG	CESG	The information and security arm of the Government Communications Headquarters (GCHQ).
CiSP	Cyber-security information Sharing Partnership	A joint industry – government initiative to share information on cyber threats and vulnerability.
CPNI	Centre for the Protection of National Infrastructure	Protects national security by providing protective security advice to organisations considered Critical National Infrastructure.
DCLG	Department for Communities and Local Government	Responsible for setting policy to support local government and regions in England. This includes planning, building regulations and urban regeneration.
DCMS	Department for Culture, Media & Sport	Responsible for protecting and promoting the UK's cultural and artistic heritage. Helping businesses and communities to grow by investing in innovation and highlighting Britain as a fantastic place to visit.
DECC	Department of Energy & Climate Change	Responsible for making sure that the UK has secure, clean, affordable energy supplies. Promotes international action to mitigate climate change.
DEFRA	Department for Environment, Food & Rural Affairs	Responsible for safeguarding the natural environment, supporting the food and farming industry and the rural economy.
DfE	Department for Education	Responsible for education, children's services, higher and further education policy, apprenticeships and wider skills in England, and equalities.
DFID	Department for International Development	Leads the UK's work to end extreme poverty.

Acronym	Full name	Description of activities
DfT	Department for Transport	Responsible for planning and investing in the transport infrastructure to keep the UK on the move.
DoH	Department of Health	Responsible for leading, shaping and funding health and care in England.
DWP	Department for Work & Pensions	Responsible for welfare, pensions and child maintenance.
FCO	Foreign & Commonwealth Office	Responsible for promoting the UK's interests overseas. Supports UK citizens and businesses around the globe.
GCHQ	Government Communication Headquarters	Security and intelligence organisation. It is tasked by the government with protecting the nation from threats such as terrorism and criminal activity, especially via the internet. It is also responsible for securing the UK's communications.
GDS	Government Digital Service	Leads the government's digital transformation and aims to make public services digital by default.
GovCertUK	The Computer Emergency Response Team for UK Government	A counterpart of CERT-UK. Responsible for national cyber security incident management for the public sector.
GSS	Government Security Secretariat	Responsible for areas of security policy. Previously, it also issued guidance and frameworks.
HMRC	HM Revenue & Customs	The UK's tax, payments and customs authority. Responsible for collecting taxes.
HMT	HM Treasury	Responsible for maintaining control over public spending. Sets the direction of the UK's economic policy and work to achieve economic growth.
HO	Home Office	Responsible for keeping citizens safe and the country secure.
ICO	Information Commissioner's Office	Regulatory role that covers enforcing legislation such as the Data Protection Act and the Freedom of Information Act.
MoD	Ministry of Defence	Responsible for protecting the security, independence and interests of the UK.
MoJ	Ministry of Justice	Responsible for the criminal justice system.
OCSIA	Office of Cyber Security and Information Assurance	Provided strategic direction and coordinates action relating to enhancing cyber security and information assurance through the National Cyber Security Programme (NCSP).
OGSIRO	Office of the Government Senior Information Risk Owner (SIRO)	Provides guidance and assistance to the departmental information assurance community in handling incidents and developing risk appetite.
TNA	The National Archives	Provided training for information asset owners and boards across central government over the past three years as part of their funding under the five-year National Cyber Security Programme.
UKNACE	UK National Authority for Counter-Eavesdropping	Responsible for detecting and protecting against technical espionage and attacks.

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

Design and Production by NAO External Relations
DP Ref: 11131-001

£10.00

ISBN 978-1-78604-073-2