National Audit Office

Report
by the Comptroller
and Auditor General

Cabinet Office

Protecting information across government

HC 625 SESSION 2016-17 14 SEPTEMBER 2016

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.