House of Commons
Committee of Public Accounts

Protecting information across government

Thirty-eighth Report of Session 2016–17

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 25 January 2017

HC 769
Published on 3 February 2017
by authority of the House of Commons

The Committee of Public Accounts

The Committee of Public Accounts is appointed by the House of Commons to examine "the accounts showing the appropriation of the sums granted by Parliament to meet the public expenditure, and of such other accounts laid before Parliament as the committee may think fit" (Standing Order No. 148).

Current membership

Meg Hillier (*Labour (Co-op), Hackney South and Shoreditch*) (Chair)

Mr Richard Bacon (*Conservative, South Norfolk*)

Philip Boswell (*Scottish National Party, Coatbridge, Chryston and Bellshill*)

Charlie Elphicke (*Conservative, Dover*)

Chris Evans (*Labour (Co-op), Islwyn*)

Caroline Flint (*Labour, Don Valley*)

Kevin Foster (*Conservative, Torbay*)

Simon Kirby (*Conservative, Brighton, Kemptown*)

Kwasi Kwarteng (*Conservative, Spelthorne*)

Nigel Mills (*Conservative, Amber Valley*)

Anne Marie Morris (*Conservative, Newton Abbot*)

Bridget Phillipson (*Labour, Houghton and Sunderland South*)

John Pugh (*Liberal Democrat, Southport*)

Karin Smyth (*Labour, Bristol South*)

Mrs Anne-Marie Trevelyan (*Conservative, Berwick-upon-Tweed*)

Powers

Powers of the Committee of Public Accounts are set out in House of Commons Standing Orders, principally in SO No. 148. These are available on the Internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Dr Stephen McGinness (Clerk), Dr Mark Ewbank (Second Clerk), George James (Senior Committee Assistant), Sue Alexander and Ruby Radley (Committee Assistants), and Tim Bowden (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Committee of Public Accounts, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 4099; the Committee's email address is pubaccom@parliament.uk.

Contents

Summary

Well documented data security breaches at Tesco, Northern Lincolnshire and Goole NHS Trust, Sage, and TalkTalk have recently thrown the challenge of protecting information into the spotlight. The threat from cyber attacks has been one of the UK's top four risks to national security since 2010, yet it has taken the Government too long to consolidate and co-ordinate its 'alphabet soup' of agencies involved in protecting Britain in cyberspace. The Cabinet Office's role in protecting information remains unclear within central government, and there appears to be no coordination across the wider public sector. There is little oversight of the costs and performance of government information assurance projects, and processes for recording departmental personal data breaches are inconsistent and dysfunctional. Poor reporting of low level breaches, such as letters containing personal details being addressed to the wrong person, reduces our confidence in the Cabinet Office's ability to protect the nation from higher threat cyber attacks. The use of the internet for cyber crime is evolving fast and the government faces a real struggle to find enough public sector employees with the skills to match the pace of change.

Introduction

Protecting the information government holds from unauthorised access or loss is a critical responsibility for departmental accounting officers, particularly with the increasing need to disseminate this information to other public bodies, delivery partners, service users, and citizens via new digital services. The Cabinet Office is responsible for coordinating this activity across central government departments. However, increasing dependencies between central government and the wider public sector means traditional security boundaries have become blurred. In recent years, the threat of electronic data loss from cyber crime, espionage, and accidental disclosure has risen considerably; the Government Communications Headquarters (GCHQ) dealt with 200 national cyber security incidents (defined as attacks which threatened UK national security) per month in 2015, up from 100 per month in 2014. Concurrently, personal data breach reporting remains highly variable, with some departments recording thousands of incidents in the 2014–15 financial year and five departments recording none at all. In October 2016, GCHQ launched the new National Cyber Security Centre, designed to act as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. The Cabinet Office's second National Cyber Security Strategy was published in November 2016.

Conclusions and recommendations

1. **It has taken too long to consolidate and coordinate the 'alphabet soup' of agencies involved in protecting Britain in cyberspace.** The threat from cyber attacks has been one of the UK's top four risks to national security since 2010. Numerous teams and organisations were formed in government, with overlapping mandates and activities related to protecting information. 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". As recently as April 2016, there were still at least 12 separate teams or organisations in the centre of government with a role in protecting information. There were several lines of accountability with little coherence between them. The Cabinet Office has since amalgamated many of these bodies; into the National Cyber Security Centre (NCSC), designed to act as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents; and the Cabinet Office's Cyber and Government Security Directorate, responsible for all aspects of government protective security. The breadth of the NCSC's role is considerable and it is still unclear which organisations from across the public and private sectors can call on the NCSC for assistance.

   Recommendation: ***The Cabinet Office should develop a detailed plan for the NCSC by the end of this financial year, setting out who it will support, what assistance it will provide and how it will communicate with organisations needing its assistance.***

2. **The Cabinet Office's approach to protecting information places too little emphasis on informing and supporting citizens, service users, and the wider public sector beyond Whitehall.** There are increasing dependencies and associated information flows between central government, the wider public sector, delivery partners, citizens and service users. The Cabinet Office has no formal role to provide oversight, coordination and support to the wider public sector in the same way that it does for central government. A founding principle of the Government's security strategy is that any public body holding official information or data is responsible for securing it that data. The Cabinet Office is relying on those organisations to resolve the majority of security requirements through commercially available products and services, but also to know when the risk is significant enough to contact the NCSC. According to the Barclays Digital Development Index, Britain is below Brazil, South Africa and China at keeping our phones and laptops secure. There is too little emphasis on informing and supporting the public sector, delivery partners, and individual users of government websites, particularly on what to do if a data breach incident occurs. This is of particular concern given the Government's extensive reliance on arm's length bodies to deliver core public services and functions, with more than 450 arm's length bodies through which the Government spends around £250 billion annually.

Recommendation: ***The government should establish a clear approach for protecting information across the whole of the public sector and delivery partners—not just central government—and clearly communicate to all these bodies how its various policy and guidance documents can be of most use, including during a data breach incident.***

3. **Centrally managed government information projects are not yet delivering as planned.** The Government Security Classifications system (a three-point system to classify information consistently across government), the Public Services Network (a high performance network to allow public sector bodies to share resources securely) and the Foxhound project (a confidential network to allow the sharing of classified information across government) have been slow to deliver planned benefits or significant financial savings due to poor planning. These projects pose considerable business change, cultural and technical challenges because the systems in place need to be sufficiently robust to keep up with the pace of change. Initial project assumptions have been optimistic and have not been challenged at regular intervals to ensure they remain valid and facilitate accountability. For example, the Government ignored its own advice by not undertaking a detailed financial business case for the Government Security Classifications system. This project was initially forecast to deliver between £110 million to £150 million annually in benefits. Having never completed a detailed financial business case, the Department did not have confidence in these figures and consequently has not had a baseline against which to judge whether the GSC has produced any financial benefits.

   Recommendation: ***The Cabinet Office should ensure that there is robust challenge built into the design of these projects and review them regularly. It should monitor spend against budget and be clear that the expected benefits for cyber security are still achievable.***

4. **The Cabinet Office's attitude to departmental reporting has led to poor monitoring of the costs and performance of individual departments' efforts to protect information.** The Cabinet Office does not mandate how departments should report on the costs and benefits of their information protection initiatives, nor does it believe that a clear, central view of these costs would be useful for its decision making. The Cabinet Office argued that fundamentally different requirements for protecting information across departments means there are different expenditure profiles, which limit the usefulness of having such information for central decision-making. However, only the Cabinet Office is in a position to demand clear and consistent cost and performance data across central government departments, to allow it to assess challenges and allocate resources accordingly to minimise risks and maximise value for money.

   Recommendation: ***The Cabinet Office should regularly assess the cost and performance of government information security activities, and identify a set of baseline indicators that departments should report against to support this objective.***

5. **The Cabinet Office's ability to make informed information security decisions is undermined by inconsistent and chaotic processes for recording personal data breaches.** There are major and unexplained variations in the extent to which individual departments report security breaches. In 2014–15, the 17 largest departments recorded a total of 14 data incidents that they considered reportable to the Information Commissioner's Office, and recorded 8,981 non-reportable incidents. Of the 8,981, Her Majesty's Revenue and Customs recorded 6,038 (67%) and the Ministry of Justice 2,798 (31%). The other 15 departments recorded only 145 between them, fewer than 2% of the total. Several departments recorded no non-reportable incidents at all, including the Department for Work and Pensions, a large department with a comparable level of online activity to HMRC. We are aware that numerous low-level breaches do occur, such as letters containing personal details being addressed to the wrong person; however these are not consistently recorded as data breaches. The Cabinet Office does not collect or analyse departments' performance in protecting information on a routine or timely basis and was not aware of the wide variability and inconsistency of departments' self-reporting processes prior to the National Audit Office's analysis. Departments with a high reporting rate are likely to be better protected because they have developed a reporting culture to allow early identification of threats. Without a consistent approach across Whitehall to identifying, recording and reporting security incidents, the Cabinet Office is unable to make informed decisions about where to direct and prioritise its attention.

   Recommendation: ***The Cabinet Office should consult with the Information Commissioners' Office to establish best practice reporting guidelines and issue these to departments to ensure consistent personal data breach reporting from the beginning of the 2017–18 financial year.***

6. **The Government is struggling to ensure its security profession is suitably skilled.** The Cabinet Office established a security profession in 2013 to develop professional learning and career development activities for civil servants working in this field. However, it remains unclear as to what skills gaps exist and how to fill these in the face of UK-wide skills shortages in this field. The Cabinet Office is also unwilling to mandate a minimum skills standard for departments in the security profession. It is planning to amalgamate 40 separate departmental security teams into four larger clusters, and has established the first pilot cluster, to better enable the sharing of scarce skills across central government.

   Recommendation: ***The Cabinet Office should write to us within six months of this report, setting out its findings from the pilot security cluster and what steps it is taking to improve government's capability in this area.***

1 The role of the centre of government in protecting information

1. On the basis of a report by the Comptroller and Auditor General, we took evidence from the Cabinet Office on its role in protecting information across government and how it intends to improve capability across government in protecting information.[1]

2. Protecting the information government holds from unauthorised access or loss is a critical responsibility for government and departmental accounting officers, whether that information is held as paper-based records or in electronic formats. The consequences of data losses and breaches of systems are substantial and can lead to significant harm, distress and reputational damage that can undermine entire programmes. In 2015, GCHQ dealt with an average of 200 national cyber security incidents (defined as attacks which threatened UK national security) per month—up from 100 in 2014. In the same year, government's 17 largest departments recorded 8,995 personal data breaches.[2]

3. The Prime Minister is ultimately responsible for the security of the information government holds. She is supported in this by the Cabinet Secretary, who chairs a committee which sets the overall direction and strategy for government security. The Cabinet Office is responsible for coordinating this activity across central government departments. In each government department, responsibility for information security lies with the respective ministers, permanent secretaries and their management boards. 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, manages and protects 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.[3]

Coordinating roles and responsibilities

4. Since the publication of the 2010 National Security Strategy, the government has classified cyber attacks as one of the top four threats to the UK's national security. The Cabinet Office's second National Cyber Security Strategy, published in November 2016, re-emphasised this threat. Given the apparent importance of the issue, we asked the Cabinet Office whether it was directing sufficient attention to cyber security.[4]

5. As at April 2016, at least 12 separate teams or organisations in the centre of government had a role in protecting information. A lack of coordination between these bodies resulted in overlapping and sometimes contradictory specifications and requirements. This has meant that departments have been confused about the roles of these bodies and have not known where to turn to for definitive advice. The Cabinet Office explained that this proliferation of guidance is a result of it trying to account for individual risks as they arose but that it is now attempting to consolidate and streamline the guidance the centre

1 C&AG's Report, *Protecting information across government*, Session 2016–17, HC 625, 14 September 2016
2 C&AG's Report, paras 1.1, 1.8, Key Facts
3 C&AG's Report, paras 2, 3
4 Qq 1, 3

of government produces. 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".[5]

6. The Cabinet Office has since amalgamated many of these bodies; into the National Cyber Security Centre (NCSC), designed to act as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents; and the Cabinet Office's Cyber and Government Security Directorate, responsible for all aspects of government protective security. Given that the NCSC only opened in October 2016, its ability to resolve the coordination problems inherent in the previous structure of information protection bodies is untested.[6]

7. The Cabinet Office explained that the success of its objective for the NCSC to provide a clear, single source of advice on cyber security and protecting information would depend on the relevant institutions working together in a new way. The Cabinet Office believes it would have achieved its goals for simplifying the provision of advice when users are directed to the correct organisation by whichever body they first contact.[7]

Looking beyond Whitehall

8. The Cabinet Office is responsible for coordinating information security across central government departments. Its remit does not extend to the wider public sector despite significant data flows between central and local bodies. For example, in 2014–15, the Department of Health spent more than 86% of its £123 billion budget outside the core department. Where central government information is passed onto third parties, the issuing department is responsible for ensuring the information is handled in accordance with government-set rules and regulations. The Cabinet Office acknowledged that protecting information, whether it is in the public sector supply chain or industry, is a challenge for the centre of government. The Cabinet Office has concerns about both the ability of those organisations to meet the standards of central government and the ability of departments to assess and evaluate whether those standards are being met and to know when it is necessary to issue a mandate.[8]

9. According to the Barclays Digital Development Index, Britain is below Brazil, South Africa and China at keeping the nation's phones and laptops secure: 41% of UK citizens change passwords regularly compared with 59% in India, and only 13% of UK citizens use password generating software, compared with a third of citizens in China and India. An objective of the 2011 National Cyber Security Strategy was for the Government to work with companies that own and manage the UK's Critical National Infrastructure (CNI) to ensure key data and systems continue to be safe and resilient. To measure progress against this target, the Cabinet Office referred to the Government FTSE 350 Cyber Governance Health Check Report, published May 2016. 113 firms participated, representing around a third of the FTSE 350. While this survey found some improvement in public and

5 Qq 1, 19, 20; C&AG's Report, para 1.24
6 Qq 20, 22, 23, 26, 41
7 Qq 26, 41
8 Qq 135–139; C&AG's report para 3.7

commercial understanding of cyber risk management, many companies still need to develop basic information assurance standards to prevent low level malware attacks such as interference with password entries.[9]

10. We queried whether individuals and organisations outside the centre of government will have access to the support and advice of the NCSC. The Cabinet Office set out its expectation that such individuals and organisations should be seeking information protection services from commercial providers with the NCSC's role being to provide approval of services that are fit-for-purpose. The NCSC has an accessible website that provides contact details enabling government and public to communicate with the agency. However, we have concerns over the ability of the NCSC to manage the volume of security incidents previously channelled through a number of different bodies. 68 incidents were reported to the NCSC in its first month of operation. These incidents varied in scale, nature and target. The Cabinet Office noted that it is unlikely that every inquiry will receive a personal response and that this process relies on the customer understanding when a risk should be escalated to the NCSC.[10]

Centrally managed government information projects

11. The Cabinet Office is managing a number of projects designed to enable government to better manage its information. The three projects are: the Government Security Classifications (GSC) system, the Public Services Network (PSN) and the Foxhound project. The GSC system, a three-point system for classifying information consistently across government, has replaced the previous six-point security classification system. Its implementation should allow departments to replace expensive, bespoke IT with more flexible and cheaper systems. The PSN is the successor to the government secure intranet and was intended to achieve substantial government cost savings by providing an assured network over which central and local government could safely collaborate. The Foxhound project was originally designed to deliver a single, secret network across government that would offer considerable cost savings by replacing many older systems. Poor planning means that the Cabinet Office does not know if these savings have been delivered.[11]

12. The strategic business case for the GSC used industry comparators to estimate savings each year of between £110 and £150 million. There was no detailed financial business case for this project, since the Cabinet Office could not find accurate data to cover all aspects of security expenditure. Although Departments can make efficiencies by adopting commodity IT services, it is difficult to measure these efficiencies because the benefits are several steps away from changing the classification system. The Cabinet Office therefore cannot say whether it achieved any financial benefits as originally proposed for the GSC.[12]

13. The original plan for the PSN was that it would deliver at least £500 million of savings per year by 2014. The *PSN business case update 2011–12* revised this estimate to between £200 million and £400 million per year by 2014. The project achieved annual savings of £60 million, £127 million, £116 million and £103 million respectively in the four years to 2014, all of which are less than the lower limit of the revised estimated annual savings.

9 Qq 33–40; Cabinet Office (PIG0003)
10 Qq 28–30, 33, 43, 62, 104; Cabinet Office (PIG0003)
11 Q 48; C&AG's Report paras 2.22, 2.24, 2.25, 2.33, 2.34, 2.41
12 Qq 54–57; C&AG's Report para 2.32

The Cabinet Office agreed this was a result of unrealistic projections set at the start of the project. The PSN team does not anticipate making any more savings against the original PSN baseline.[13]

14. The Foxhound project is, against its original aspirations, 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. The Cabinet Office noted that the Infrastructure and Projects Authority has completed a review of the Foxhound project in July 2016 and had found improvements. Consequently it moved the project from a red rating to a red-amber rating.[14]

13 Qq 52–53; C&AG's Report para 2.40
14 Qq 48, 50

2 Consistent standards across government

Oversight of costs and performance

15. The Cabinet Office does not mandate how departments should report on the costs and benefits of their information protection initiatives. It is instead trying to provide a framework within which departments can deliver. However, there is a voluntary feel to the process of departments reporting this information. The Cabinet Office told us that it often gets told "we ask too many questions too frequently of Departments about what they are doing".[15]

16. There is no single body responsible for collecting data on the cost and benefits of current information security activities and projects. The costs of protecting information across government are therefore unclear. The Cabinet Office explained that it does not collect cost and benefits data across departments because the activities are too dissimilar to be comparable and it is difficult to isolate the cost of the security elements of a project from the overall expenditure. It gave the Department of Work & Pensions (DWP) and Her Majesty's Revenue & Customs (HMRC) as examples of two departments with comparable businesses but fundamentally different security systems; DWP is building and securing the universal credit system compared to HMRC securing a decades-old VAT mainframe system. Both tasks would have very different expenditure profiles and requirements, which the Cabinet Office feels would limit the usefulness of having such information for central decision-making.[16]

17. Only the Cabinet Office is in a position to demand clear and consistent cost and performance data across central government departments. The threat from hostile attacks upon UK cyber space is one of the top four risks (highest priority taking account of both likelihood and impact) to the UK's national security. The Cabinet Office is currently making decisions on a 'system by system and department by department' basis, and there is no central register of cyber risk and the cost and progress towards mitigating that risk. Without this, the Cabinet Office is limited in its ability to make a strategic assessment of where to allocate resources to minimise risks and maximise value for money.[17]

Security breach reporting

18. The Cabinet Office does not collect or analyse government's performance in protecting information on a routine or timely basis and departments' self-reporting processes vary widely. The National Audit Office found that in 2014–15, the 17 largest departments recorded a total of 14 personal data incidents that they considered reportable to the Information Commissioner's Office, and recorded 8,981 non-reportable incidents. Of the 8,981, HMRC recorded 6,038 (67%) and the MoJ 2,798 (31%). The other 15 departments recorded only 145 between them, fewer than 2% of the total. Several departments recorded no non-reportable incidents at all, including the DWP, a large department with a comparable level of online activity to HMRC. We are aware that numerous low-level breaches do occur,

15 Q 146, C&AG's Report, para 3.14
16 Qq 146–147
17 Qq 145–147

such as letters containing personal details being addressed to the wrong person; however these are not consistently recorded as data breaches by departments. The Cabinet Office was not aware of the wide variability and inconsistency of departments' self-reporting processes prior to the National Audit Office's analysis.[18]

19. There is uncertainty by departments over when to record and report a data breaches because guidance from the Information Commissioner's Office is not sufficiently specific for adoption by the Government. Departments with a high reporting rate may in fact be better protected because they have developed a reporting culture to allow early identification of threats. The Cabinet Office noted that HMRC, which recorded the highest number of breaches in 2014–15, has an online reporting tool to record data breaches. Other departments' systems are less established or have less maturity and capability for collecting that data. The Cabinet Office is considering whether to roll-out HMRC's data breach reporting tool to the rest of Government. It emphasised that the government's response to cyber-security threats is critical and that it needs to focus on ensuring processes and capabilities are in place to be able to respond effectively.[19]

20. The European Union General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (NIS) are due for introduction in May 2018. The Secretary of State for Culture, Media and Sport, the Rt Hon Karen Bradley MP, confirmed the UK will be implementing the GDPR at the Culture, Media and Sport Select Committee on 24 October. The NIS Directive will be implemented via secondary legislation.[20]

21. The GDPR mandates that a notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR also recognises that it will often be impossible to investigate a breach fully within that time period and allows the organisation to provide information in phases. If the breach is sufficiently serious to warrant notification to the public, the organisation must do so without undue delay. The UK was a major contributor to the design and development of the GDPR and the Cabinet Office will have a role in interpreting these regulations for UK government departments. However, the Cabinet Office is trying to converge government's use of data, IT and systems with the industry model and commercial good practice to reduce the need for reinterpretation.[21]

Skills levels

22. There is a national shortage of skilled people available for information protection, and this is reflected in the public sector. 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 to establish professional learning and career development activities for all civil servants working in

18 Qq 66, 69, 73, 75; C&AG's Report, Figure 6
19 Qq 66, 77, 85
20 Qq 86–87; Cabinet Office (PIG0003)
21 Qq 86–89; Cabinet Office (PIG0003)

this field. However, departments are struggling to place people with the right skills and there is no mandatory training, certification or regulations of senior information risk owners (SIROs) or departmental security officers (DSOs).[22]

23. The Cabinet Office has asked departments on an annual basis whether their SIROs (a board level official or member of the organisation) were trained, for example through the National Archives training scheme. It found that senior civil servants were often not according the necessary priority to security training courses. In these cases, the Cabinet Office placed responsibility on the DSOs to ensure that senior leaders who are responsible for security understand their responsibilities and the system that they work within. Events such as the TalkTalk or Tesco data breaches have also impressed the need on boards to become more intelligent customers. In May 2016, the Cabinet Office began planning the formal withdrawal of the SIRO role, and the development of chief security officers. This role has now been allocated as a full-time chief security officer who addresses all aspects of security within government.[23]

24. The Cabinet Office agreed that it would be necessary to mandate security training and ensure board familiarity. The Cabinet Office has moved from a system of prescriptive policies and mandating of a few years ago, which resulted in inhibiting technology adoption, to a more flexible description of the security requirement that a department could use to specify and achieve. However, the Cabinet Office found that over time the standard and application of this framework drifted. The Cabinet Office is now planning to amalgamate 40 separate departmental security teams into four larger clusters, and has established the first pilot cluster. These clusters are intended to better enable the sharing of scarce skills across central government. The roll-out of clusters is planned for late 2018 to early 2019 and each cluster will be headed by a trained and certified chief security officer.[24]

22 Q 15; C&AG's Report paras 3.24–3.25
23 Qq 14, 17
24 Qq 46, 108, 113, 119

Formal Minutes

Wednesday 25 January 2017

Members present:

Meg Hillier, in the Chair

Mr Richard Bacon	Anne Marie Morris
Philip Boswell	Bridget Phillipson
Charlie Elphicke	John Pugh
Kevin Foster	Karin Smyth
Kwasi Kwarteng	Mrs Anne-Marie Trevelyan
Nigel Mills	

Draft Report (*Protecting information across government*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 24 read and agreed to.

Introduction agreed to.

Conclusions and recommendations agreed to.

Summary agreed to.

Resolved, That the Report be the Thirty-eighth of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Wednesday 1 February 2017 at 2.00pm

Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

Monday 14 November 2016	*Question number*
Ben Aung, Deputy Director, Cyber and Government Security Secretariat, and **Paddy McGuinness**, Deputy National Security Adviser, Intelligence Security and Resilience	Q1–158

Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

PIG numbers are generated by the evidence processing system and so may not be complete.

1 Cabinet Office Cyber and Government Security Directorate (PIG0003)

2 Information Commissioner's Office (PIG0001)

List of Reports from the Committee during the current session

All publications from the Committee are available on the publications page of the Committee's website. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2016–17

First Report	Efficiency in the criminal justice system	HC 72 (Cm 9351)
Second Report	Personal budgets in social care	HC 74 (Cm 9351)
Third Report	Training new teachers	HC 73 (Cm 9351)
Fourth Report	Entitlement to free early education and childcare	HC 224 (Cm 9351)
Fifth Report	Capital investment in science projects	HC 126 (Cm 9351)
Sixth Report	Cities and local growth	HC 296 (Cm 9351)
Seventh Report	Confiscations orders: progress review	HC 124 (Cm 9351)
Eighth Report	BBC critical projects	HC 75 (Cm 9351)
Ninth Report	Service Family Accommodation	HC 77 (Cm 9351)
Tenth Report	NHS specialised services	HC 387 (Cm 9351)
Eleventh Report	Household energy efficiency measures	HC 125 (Cm 9351)
Twelfth Report	Discharging older people from acute hospitals	HC 76 (Cm 9351)
Thirteenth Report	Quality of service to personal taxpayers and replacing the Aspire contract	HC 78 (Cm 9351)
Fourteenth Report	Progress with preparations for High Speed 2	HC 486 (Cm 9389)
Fifteenth Report	BBC World Service	HC 298 (Cm 9389)
Sixteenth Report	Improving access to mental health services	HC 80 (Cm 9389)
Seventeenth Report	Transforming rehabilitation	HC 484 (Cm 9389)
Eighteenth Report	Better Regulation	HC 487 (Cm 9389)

Nineteenth Report	The Government Balance Sheet	HC 485 (Cm 9389)
Twentieth Report	Shared service centres	HC 297 (Cm 9389)
Twenty-first Report	Departments' oversight of arm's-length bodies	HC 488 (Cm 9389)
Twenty-second Report	Progress with the disposal of public land for new homes	HC 634
Twenty-third Report	Universal Credit and fraud and error: progress review	HC 489
Twenty-fourth Report	The sale of former Northern Rock assets	HC 632
Twenty-fifth Report	UnitingCare Partnership contract	HC 633
Twenty-sixth Report	Financial sustainability of local authorities	HC 708
Twenty-seventh Report	Managing government spending and performance	HC 710
Twenty-eighth Report	The apprenticeships programme	HC 709
Twenty-ninth Report	HM Revenue & Customs performance in 2015–16	HC 712
Thirtieth Report	St Helena Airport	HC 767
Thirty-first Report	Child protection	HC 713
Thirty-second Report	Devolution in England: governance, financial accountability and following the taxpayer pound	HC 866
Thirty-third Report	Troubled families: progress review	HC 711
Thirty-fourth Report	The Syrian Vulnerable Persons Resettlement programme	HC 768
Thirty-fifth Report	Upgrading emergency service communications	HC 770
Thirty-sixth Report	Collecting tax from high net worth individuals	HC 774
Thirty-seventh Report	NHS treatment for overseas patients	HC 771
First Special Report	Protecting the Public's Money: First Annual Report from Chair of Committee of Public Accounts	HC 835

HOUSE OF COMMONS

Public Accounts Committee

Oral evidence: Protecting Information across Government, HC 769

Monday 14 Nov 2016

Ordered by the House of Commons to be published on 14 Nov 2016.

Watch the meeting

Members present: Meg Hillier (Chair); Mr Richard Bacon; Philip Boswell; Chris Evans; Kevin Foster; Nigel Mills; Bridget Phillipson; Karin Smyth.

Sir Amyas Morse, Comptroller and Auditor General, Adrian Jenner, Director of Parliamentary Relations, National Audit Office, Tom McDonald, Director, National Audit Office, and Marius Gallaher, Alternate Treasury Officer of Accounts.

Questions 1-158

Witnesses

I: Ben Aung, Deputy Director, Cyber and Government Security Secretariat, and Paddy McGuinness, Deputy National Security Adviser, Intelligence Security and Resilience.

HOUSE OF COMMONS

Reports by the Comptroller and Auditor General

Protecting information across government (HC 625)

Examination of witnesses

Witnesses: Ben Aung and Paddy McGuinness.

Chair: Welcome to the Public Accounts Committee on Monday 14 November 2016. We are here today off the back of a Report by the National Audit Office about protecting information across Government. This is a very timely issue, given that in today's papers the Tesco data breach is still very high in people's minds, and there have been very well documented breaches at Northern Lincolnshire and Goole NHS Trust, Sage and TalkTalk a year ago, which have thrown some of the challenges into the spotlight. We know that the Government have been changing the plans for how you approach this since about 2010.

Our witnesses today are Ben Aung, who is the deputy director of the Government Security Secretariat. I think it is your first time in front of the Committee.

Ben Aung: It is, yes.

Chair: Welcome. We are a friendly bunch—believe that and you'll believe anything. Paddy McGuinness is from the Cabinet Office, where he is the deputy national security adviser for intelligence security and resilience. Just a small job you've got there, Mr McGuinness.

Paddy McGuinness: Just a tiny one.

Q1 **Chair:** Before we get into the main thrust of the Committee's work today, it is worth highlighting that in 2010 the Government itself identified four key risks for Government. The top threats were terrorism, a major incident such as flooding or another natural disaster, a military intervention, and cyber. Looking at what the NAO have come up with in their Report, we wonder—perhaps you can answer this, Mr McGuinness—whether you believe cyber-security is being treated with the same focus as the other three.

Paddy McGuinness: Yes, I would say it is. We have had a highly established way of dealing with the others for generations. Cyber is a new domain, and new approaches are required. We have been learning, and as a nation we are at the cutting edge of what it is possible for a state to do. I think that is evident in the response to the recent publication of our second national cyber-security strategy just the week before last.

Q2 **Chair:** It was interesting that it was the week before last—just in time for the Committee. We appreciate that. At least it wasn't today, which a lot of witnesses manage to do.

You say it's a new thing—my colleague, Chris Evans, is going to come in on this—but the Government highlighted it in 2010 and we are only just getting the national centre established. What is the reason for that delay?

Paddy McGuinness: We have worked through the development of a collective approach to cyber-security. I took over as the senior responsible officer for the national cyber-security programme in 2014, but I very much subscribe to what was done after 2010. After 2010, we put together for the first time a CERT-UK, which was a bringing together of all the CERTs, or a CERT of CERTs—a single cyber-emergency response team in the Government. We invested in a centre for cyber-assessment, and we invested yet more heavily in the security mission at GCHQ, which is often referred to in the papers as CESG. We have been on a journey with that.

What we have done in the National Cyber Security Centre—I suspect you will want to come on to this—is to bring together those things in a new configuration because of what we have learned in the last five years of working through that journey. We have had good, measurable effect through that journey, and now this is next iteration.

Chair: Okay. I am going to ask Mr Evans to come in, but I am sure we will be coming back to some of those points.

Q3 **Chris Evans:** Mr McGuinness, thank you for coming to the meeting today. I have in front of me "The UK Cyber Security Strategy", which was published in November 2011. I will read from the introduction to you. The last but one paragraph states: "By 2015, the aspiration is that the measures outlined in this strategy will mean the UK is in a position where: law enforcement is tackling cyber criminals; citizens know what to do to protect themselves; effective cyber security is seen as a positive for UK business; a thriving cyber security sector has been established; public services online are secure and resilient; and the threats to our national infrastructure and national security have been confronted." A simple question: how well are you doing against those measures?

Paddy McGuinness: I think we did well in the first five years—

Q4 **Chris Evans:** The first five to 2015?

Paddy McGuinness: To the launch now—we have just launched a second iteration of the strategy. I think we have done well against that. Of course, the best benchmark is how we have done compared with other jurisdictions and partners, and we have done well. We have got some measurable things: cyber-security has become a significant factor in the thinking of both commercial and Government Department boards, skills have developed and academic centres have grown up, and incentives have come into insurance and some other markets. Those are a set of things. Look at the way in which we have communicated Cyber Essentials and 10 Steps to Cyber Security, which are now played back to us. You can tell you are getting somewhere when you speak to an audience and they relay back to you the cyber-messages you have been putting to them for some time. I feel we have done well against those measures.

Of course, we are facing tremendous technological development. We are moving towards the internet of things, and more and more Government services are being delivered online. We need to make measurable progress against those developments in technology. If you look closely at the new national cyber-security strategy, which we have just published, you will see the next iteration, building on what we did in 2011.

Q5 **Chris Evans:** I will come back to that later. It is a question I will probably revisit in a little while. The crux of the question is this. "The UK Cyber Security Strategy" from November 2011 says: "If you are in business this strategy sets out what we will do to help ensure protection of your company". If I had a business, where do I go, considering that at the moment there are—until we have a new body—12 organisations? If I had a business, specifically who do I call?

Paddy McGuinness: The organisations laid out in the Report are principally there—

Chair: I should just say this is on page 17.

Paddy McGuinness: They are principally there to address the needs of Government. Some of them are public-facing. In particular, CERT-UK was public-facing. Business knew to go there. I was looking just before I came out at the figures for the Cyber-security Information Sharing Partnership, which is also referred to in the Report. Over 2,600 businesses, Government Departments and public sector bodies mixed together are now a part of that, but the major part are businesses. There is a thriving way in which information is being shared often in real time with businesses. There is also a set of products that are published. If one searches on cyber-security UK—at these kinds of events one wishes one could immediately search and bring one up on the Google screen to show you—there is a set of products that come up. Now, of course, these will come up from the National Cyber Security Centre.

Q6 **Chris Evans:** I am confused. If I look at paragraph 1.14 on page 14 of the Report, there have been—correct me if I am wrong—five different strategies in place, beginning in March 2011 with the Government ICT strategy. In July 2011 there was the Government shared services strategic vision; in June 2012, the civil service reform plan; in November 2012, the Government digital strategy; and in December 2012, the next generation shared services strategic plan. I make that five different plans within the space of 18 months. So what is the plan? I know you were not a part of the strategy; I don't want to be unfair on you. I am just looking at them and I am quite confused that there are five different plans in 18 months.

Paddy McGuinness: I would be happy to come back to the Committee if I am not able to cover elements of this. What you have underpinning these is a Government approach to cyber-security that has been developing. These have been informed by that. I can speak to that. I cannot speak to these individual ones. For instance, there was a delivery of digital services through the Government digital strategy. That will be

underpinned by a security model that has been developed between the Government Digital Service and CESG, with access to commercial thinking on how to secure network systems.

Q7 **Chair:** I think Mr Evans's point is that if you are a civil servant in the system looking at all of this and what you are trying to do at the centre, it is quite confusing.

Paddy McGuinness: May I make a general point in response to that? That is a profound insight for us when we think about Government security in the round. On the whole, of the people we talk about, doing and living Government security, that is not the main thing that they do. In the main, they are delivering some service to the public, supporting Ministers, doing other tasks, but in doing that they must act securely. Security, whether it be against these programmes, if you have the programmes running orthogonal to them, is running the need to be secure. That is true also if you are running the physical security of a Government estate or you are doing the HR policies of a Government Department, or indeed the Government as a whole. It is always orthogonal, running across them. There will always be a multiplicity of things the Government are doing. The challenge for us is to make sure that raspberry ripple-like through that work runs the necessary security posture. The critical question is: in their development was there a proper assessment and practice of security as they rolled out these strategies, which were to deliver a particular good to the public or to the Government?

Q8 **Chris Evans:** I would have thought it would be easier to produce one overarching strategy rather than five different strategies, which would throw up confusion. Perhaps I am being a bit pedantic. The cyber-strategy was supposed to save the Government £1.7 billion to £1.8 billion a year. We know that. How much do these various strategies cost the Government to produce and implement within the civil service? Again, I am being a bit unfair.

Paddy McGuinness: No, indeed. Again, I don't have that information because my focus is on the security of these.

Q9 **Chair:** Perhaps we can get that information from you in writing.

Paddy McGuinness: Absolutely.

Q10 **Chris Evans:** On having a clear focus on cyber-security, I want to look at paragraph 1.10 on page 12 of the Report. "In 2004 the senior information risk owner...role was created to provide a focus for addressing information risks at board level" in all Departments. I have a question about the very famous 2007 loss of child benefit data by Her Majesty's Revenue & Customs. Do we know what happened to the CDs, and is there any chance that it could happen again?

Paddy McGuinness: I do not know the details of how that was closed off in the end. Steps have been taken since to prevent a recurrence.

Ben Aung: We did not recover the CDs.

Q11 **Chris Evans:** What happened to the CDs? We have heard all sorts of reports. I am interested because this is the most famous Government breach. Can you talk us through what happened?

Ben Aung: An official at HMRC downloaded the child benefit data to two discs and put them in the post to send them to another Government body that was expecting them.

Q12 **Mr Bacon:** It wasn't a Government body. They were sent to the National Audit Office, which is not a Government body. It is an important distinction.

Ben Aung: Okay. It was another body that was expecting them and they never arrived. A thorough search was conducted of the location where they were sent from and of the audit logs on the downloading of them, but they were never recovered. We do not know whether they left the building or whether they made it to the postal room. We never found out.

Q13 **Chris Evans:** I want to refer to figure 1 on the components of information protection. It seems to me that the most vulnerable part of the business is users, and that is an example of that. Why was the post used? Letters and packages get lost every day. Would it not have been easier just to have had some sort of encryption system that could have been shared with the NAO? Why was the post used? Has that practice now been stopped? I mean, if the NAO requested that data now, how would it be shared with them? Would it be shared on a secure server?

Ben Aung: There are options within there; there were options in 2007, as well. As a minimum, the standards at the time would have expected that the data would have been encrypted as it was stored on the CDs, so that even in the event that they were lost there would have been no material impact, because the data would not have been readable.

Now, you could do exactly the same thing. So you could encrypt and store on removable media and send in the post, and that would be fine. Obviously, we have other options available to us that weren't around at the time. So you can send via various portals, you can encrypt and send by email—although, depending on the size or volume of the data, that might not be appropriate.

The key point is that if you cannot have absolute confidence that the data can make its way from A to B securely, then you would need to secure the data itself, and decide—it could be physical media in the post, electronically over the internet or over a secure network—whether it is quite safe.

Q14 **Chris Evans:** I don't want to labour the point too much; this is the last question. How was that closed down? How has the Department left that?

Ben Aung: There were internal procedures, including disciplinary procedures, that occurred; I can't speak to the very specifics of them. But probably the stand-out measure would be that the report, "Data Handling Procedures in Government", which then became a Government standard, mandated the role of the senior information risk-owner and some

subsidiary roles, and to all intents and purposes completely overhauled the way that we have thought about information risk in Government ever since.

Chris Evans: Mr McGuinness, why has the role of the senior information risk-owner been discontinued? Again, I will go to paragraph 3.32 in the Report, which says, "In May 2016, the Cabinet Office began planning the formal withdrawal…of the SIRO role, and the development of chief security officers". At the moment, how many of these SIROs are full-time and working specifically on cyber-security? Do we know?

Ben Aung: There are no full-time SIROs. The definition of a SIRO is a board-level official or member of the organisation—so, this is central Government and the wider public sector—who is responsible for championing and fostering a culture of information and security within that organisation. They also act as the focal point for information risk decisions that can't be handled at practitioner level. They will range from the director of finance, the director of HR, the director of technology, and it is for the accounting officer of that organisation, under the current definition, to choose the individual best placed in their organisation to discharge that function.

The critical point, as I believe applied when the role was designed, was that it would be an established member of that organisation rather than a new person who had just joined. In other disciplines, we've seen champions and tsars come into organisations. This was meant to be the person in the organisation who is able to most materially affect the information risk posture of that organisation.

Q15 **Chris Evans:** But if I was working in human resources in particular—I don't want to jump on HR directors, but in my experience as a former trade union official they are the busiest people in an organisation—how far down do you think cyber-security would be on their list of to-dos of a morning? I mean, if I was an HR director, I wouldn't think cyber-security was my top priority, if I had grievance and disciplinary proceedings, or whatever, there.

Paddy McGuinness: You are absolutely right, which is why we've made the change that we've made. While there were some excellent SIROs and staff working for them who improved information risk in individual organisations, the effect of the SIRO role was uneven. And we have come to the conclusion that this is of such importance, for the range of reasons that have already been laid out by the Committee—simply in terms of national resilience, it matters—that we needed to professionalise it, and that is the focus of the role of the chief security officer function.

Q16 **Chris Evans:** So you expect the chief security officer to be a full-time post, where they are focused entirely on cyber-security, yes?

Paddy McGuinness: Not solely on cyber-security, but on all the aspects of security, because, as you've rightly said—yes, we want network system to be secured, we want buildings to be physically secure and we want good anti-fraud practices, because having those enhances your overall

security, but we need good people security as well. If any of those are weak, your security model is not going to work, so we don't say "We want you, as chief security officer, just to focus on one".

One of the issues we have had in Government, which I am sure we will come on to, has been that what is required is occasionally a very high level of expertise applied to a problem, but quite often a reasonable level of expertise applied to the problem can resolve it. We have set up a model where smaller Departments in particular, which are less likely to have access to a set of people who have cyber-skills or physical security skills, can function with others—I am sure we will come on to this—and can draw down the best high-level expert advice in order to secure the work of their Department.

Tom McDonald: It is worth drawing the Committee's attention to paragraph 3.29, in which we talk about Departments' experiences of trying to deploy people into the SIRO roles. Clearly the move to make the new chief security officers full time is, in principle, an answer to one of the problems that they encountered, but it is not the only problem that they encountered. The other two that I should perhaps mention are that "departments struggled to place people with the right skills" in those jobs and that "there is no mandatory training, certification or regulation of SIROs or DSOs". It will be interesting to explore how those things will be addressed in the new model.

Q17 **Chris Evans:** That is basically the next question I want to ask about these new SIROs and DSOs. Why is there no mandatory training, certification, sharing of best practice or anything like that? Has that been overlooked?

Ben Aung: It was not mandated that SIROs were trained, but we did ask Departments at least annually whether their SIROs were trained or not. We had a couple of avenues to discharge that training. The most notable was by the National Archives, which we funded through the national cyber-security programme to deliver a range of training. I think this is in the report somewhere: it trained in excess of 7,000 individuals with information security roles—senior information risk owners, information asset owners and people who supported them—in a successful and extensive training programme. What we found was that if you were a director general or director in a busy Whitehall Department, the priority you would accord to the full-day training on offer might not necessarily correspond with the necessity for that training. Sometimes people were several months into their job before they received the training. The provision that is made in that instance is that the departmental security officer for that organisation is responsible for ensuring that those people—those senior leaders who are responsible for security, including the accounting officer—understand their responsibilities and the system that they work within. There are multiple avenues by which we train and socialise people with their responsibilities, but there isn't one mandated route.

Paddy McGuinness: May I offer this? That is about the people who can give the Department access to the right kind of security services that it needs to perform its function securely. The other thing we have been

doing is working with departmental boards. We have a model that we built in the previous cyber-security programme, where we engaged FTSE 100 and then FTSE 250 boards in order to see the maturity of their understanding of cyber. We developed that model and applied it, combined in some Departments with forms of pen testing—penetration testing—to improve the maturity of the board engagement with the security issues: yes, cyber-security, but more broadly information security issues. You end up with demand from a board that is increasingly knowledgeable and growing in knowledge.

Events such as TalkTalk, which you mentioned, or indeed Tesco, no doubt, have a wonderfully salutary effect on boards: they tend to become more interested, particularly the most senior people, when they see what happens to boards that do not get their arms around this. So you end up with an intelligent customer in the board and an intelligent commissioner of the security services that are required, but of course you don't try to have all of those services and capabilities in a single Department, because you want them to be able to access the very best that they can.

Q18 **Chris Evans:** In this Committee, we talk a lot about what is going wrong, but you have had some success, with Australia and the US copying the systems. What in particular do they like about our system as opposed to the systems they are using? What are they learning from us? I refer to paragraph 1.19 of the Report, which says that the system is being replicated by the US and Australia. This is a good news question.

Ben Aung: I have a video conference with the Australians tomorrow on exactly this subject. I suppose it is a good news story for security. It is a reflection of the advances made in digital government and the Government Digital Service. What we are seeing when we engage with these partners is that we have converged our strategies for delivering online services, and doing that securely, with good enterprise technology, and doing that securely. We have our simplified classification system, and the approach we have taken to cloud services, enterprise IT generally and classical IT, which is also referenced in the Report, and the sum of all those things is what is very interesting to our partners, who may not be as mature in any of those areas and look at us as a nation that is further ahead, probably across the board, but specifically in very particular difficult areas.

Paddy McGuinness: If I may add to that, from the engagements I have had in Australia and the US, and indeed elsewhere, I think that they admire our ability to bring all of our national capability to bear on a problem. In some other states you find that there is some division between those who are delivering cyber-security and those delivering digital services, but here we have been able to get it so that there is a fairly easy interaction across those things, and the expertise you might get at the very hardest end of the national security experience you can bring to bear on resolving the problems of the service being delivered to the citizen—you can go end to end with it, and that is unusual.

Q19 **Philip Boswell:** I want to ask about something covered by my colleague,

Mr Evans, in respect of central resources and by Mr McDonald in terms of appropriate training. Figure 4 on page 17 of the NAO Report is "The Chancellor's 'alphabet soup' of bodies at the centre of government". There are 12 of them, involved in information assurance. Is there, or was there, any interface management across these bodies? Who is in charge or responsible for ensuring that they integrate their efforts? Does that include interface that is currently best in sector? Would it include the MOD? Would it include the private sector?

Paddy McGuinness: When I look at this list, with the exception of one or two, I think I probably was responsible for making sure that they integrated. The fact that we have integrated them into this new body is indicative of where I took it, with the help of colleagues and in dialogue with others. Many of these are very closely associated. The top two sit on the same floor plate in the Cabinet Office, next to each other, and now we have combined them into a single body and they are one of the bodies that we talk about now. The Centre for Cyber Assessment—the CCA—and the CESG, which was, of course, an arm of GCHQ, were fundamentally joined together. Cert-UK was able to reach back to them and had CESG people on its floor plate so you could go the whole way through. GCHQ and CESG are in some senses the same thing. CESG is the public-facing bit of the security mission of GCHQ as was, now subsumed into the National Cyber Security Centre. GovCertUK and CESG are basically the same thing—many of the same people, with some additions.

Q20 **Philip Boswell:** There is interface across some Departments, but who is responsible for centralising this? Who manages the interfaces and sets the standards across the bodies? We have seen, through the Report, that there are varying standards, varying conformity and varying specifications and requirements.

Paddy McGuinness: This Report, which I must say we very much welcome because it is a great companion to work we were trying to do and it has helped us to adjust.

Chair: Great. I am sure that the NAO will take that plaudit. And in response to Mr Boswell?

Paddy McGuinness: What we are talking about is a situation that there was prior to 2016. Since June this year, we have amalgamated almost all of these bodies into four: there is the GDS, which is something slightly different from the others on the chart, and then all the rest are in three structures. We have already done the integration. We have ended up with a triangle: a policy and standards body, which is the cyber and government security directorate in the Cabinet Office, with a deputy director within that; the National Cyber Security Centre, which has taken in a whole set of these bodies that relate to cyber; and the Centre for the Protection of National Infrastructure, which gives the other security advice—on personnel security, insider risk and the physical security that Mr Evans was pointing out. You end up with a much simpler architecture for those chief security officers and their teams, as intelligence customers, to interface with to get the service they—

Q21 **Philip Boswell:** Who oversees that? Is that your department? Does the buck stop with you, Mr McGuinness?

Paddy McGuinness: Yes. I am happy, to a large extent, to have the buck. Certainly, this directorate works for me.

Q22 **Philip Boswell:** Something else you mentioned is new, but obviously this has been the case since 2010. As I said, I was fortunate enough to be at NATO and SHAPE earlier this year, and cybercrime is now about resources—about throwing massive resources at it, because of the risk. Do you think that you are applying adequate resources, or the right resources? If your interface management is not involving the best of business, the MOD or the private sector—if you are not ticking all those boxes—why should the citizens of the UK trust the Government with data?

Paddy McGuinness: To give a sequenced answer to that, you asked me whether I was responsible for this; I am responsible for integrating this, but clearly, the Centre for the Protection of National Infrastructure is part of the Security Service; it works for the Director General of the Security Service and ultimately therefore is, in its submissions, accountable to the Home Secretary. The National Cyber Security Centre works through the Government Communications Headquarters, GCHQ, to the Foreign Secretary, where there is a matter of authorisation that is required. That is the structure. The Minister in the Cabinet Office, Mr Gummer, is the Minister with responsibility for cyber-security, so that is formally what their command structure is.

You will be pleased to hear that within the National Cyber Security Centre we have indeed drawn together the right set of relationships. We have invested in the previous national cyber-security programme, and we still invest. That is in addition to the funding that the National Crime Agency, police services and the Home Office put towards countering cybercrime. So we have put in additional, hypothecated funding in order further to develop that capability and to underwrite the cyber-expertise of the police as it grows.

Q23 **Chair:** To be clear, the City of London police led on cybercrime initially, but the Met is developing capacity as well.

Paddy McGuinness: A unit within the National Crime Agency, the National Cyber Crime Unit or NCCU, is the lead body on cybercrime. The City of London police lead on aspects of fraud, and they are a great centre of expertise, but that is bespoke and has a particular focus—it is much narrower—but they have a contribution to make. They are a subset. If you drew a picture of national work against cybercrime, you would put them in there.

Q24 **Chair:** So the National Crime Agency is now really the strategic body, is it?

Paddy McGuinness: Absolutely. The agency has the lead on countering cybercrime, so cases such as the Tesco event going on now, where there is a crime being committed, immediately go to the National Crime Agency.

It has staff working alongside the National Cyber Security Centre, and there is a natural flow between the two, so that is well placed. There are also MOD staff who work with and alongside the National Cyber Security Centre. For almost every question you asked, I think the answer is, "Yes, we've addressed that." Of course, we must constantly work on it and look at the maturity of it, but I have very high levels of confidence, not least because we have used hypothecated funding through the previous national cyber-security programme to drive anyway willing departments to be together on the floor plate, to work together, and to have common standards. There is a community of experience. If one looks, for instance, at the outgoing NCA leader on cybercrime, you will see that he has extensive career experience in GCHQ, then subsequently he went to the Foreign Office, where he worked on international aspects of cyber-security.

Q25 **Chair:** From the work we have done around this, as well as what the NAO said, I do not think that there is any doubt that there are very talented people in the system. My colleagues are trying to drive at other issues to do with how it all stitches together. We are talking a lot about process here, but we need to focus on the impact on organisations and people.

Q26 **Chris Evans:** I want to finish off on the alphabet soup. I think you would agree that this seems to have been an ongoing problem for a long time. You have had a situation where a number of these organisations have been producing conflicting advice. With this new cyber-security directorate, can you be sure that this will not occur again, considering you have also got the National Cyber Security Centre running alongside it? You are not going to produce conflicting advice, which we have had in the past?

Paddy McGuinness: We have, I think, a clear segmentation of who is going to give advice. Ministers have been very clear about their expectation regarding the National Technical Authority, and the one source of expertise on this will be the National Cyber Security Centre, so I have high confidence. Doubtless, we are on a journey. We have only just set up this centre, and there may be individuals who do not choose to work that way, but I know that the institutions and the Ministers are committed, so I have a high level of confidence that they will be able to work together.

Q27 **Chris Evans:** If you look at paragraph 1.30, which relates to the National Cyber Security Centre, the outlook is pretty bleak. It says, "The NCSC is designed to support government and the private sector: whether it has the capacity to do so effectively remains to be seen." There does seem to be a question mark over whether this body will provide advice to local authorities and the NHS. Can you give an assurance that it will be fit for purpose and will be able to tackle those smaller departments outside of the centre?

Paddy McGuinness: It is really important to recognise that a founding principle of our overall approach to this—and indeed to information security more broadly, not just within network systems—is that the network owner is responsible for the risk. For instance, a GP practice that

own data and hold data must be responsible for the way that data is held and for securing it. They can and will have advice. They will access services, which they will pay for, from the commercial sector. We are very keen to grow that commercial sector to provide those services—there is already a very strong one in the UK that we are keen to promote. When they get into what might be called a wicked problem, where the muscle of the state is required to crack it, then they might actually have people turning up to resolve it.

Although I would rather not discuss some examples at this classification here, I can think of examples where, on relatively low-security-level networks, because of the nature of the intrusion, some of our most expert, hardest-end national security people have had to go and engage. On the other hand, if it is something that can be done by a commercial company with appropriate patching and by better information assurance practices, then you do not need to use that very scare, high-end, hard-end expertise. So the answer is: yes, they will have access. Often, they will be steered towards commercial providers who can do exactly what is required, and what you will get is what you got with CESG, which effectively is licensing saying, "Yes, this service delivery is good enough."

Q28 **Chris Evans:** You would think that the most central question for any user—I will ask you it straight away—is: how do you get in contact with this body? How easy is it going to be to get in contact with this body?

Paddy McGuinness: With the National Cyber Security Centre? As a business or a user?

Chris Evans: Yes, as a business or a user.

Paddy McGuinness: It is going to be extremely straightforward. I wish I had brought a banner—

Q29 **Chair:** Is there a telephone number?

Paddy McGuinness: A telephone number. Online access as well, absolutely. And a website you can access.

Q30 **Chair:** Are you able to cope with the potential volume? Certain big companies—the banks and telecommunications companies—would have access to GCHQ anyway, so presumably they would have done that sort of thing before if they needed to contact you. Would a small business, a medium-sized business or a local authority all, in equal measure, be able to reach you on that telephone number?

Paddy McGuinness: I would hope that even our most major telecommunications companies, when dealing with something that is the business of the National Cyber Security Centre, would deal with the National Cyber Security Centre and not go straight to the body at GCHQ.

Q31 **Chair:** So because you have got the new body, they would go there.

Paddy McGuinness: Right. There are a whole set of ways in which businesses can engage. As I said, I think two thousand, six hundred and something business are already in a thing called the Cyber-security

Information Sharing Partnership, which is a platform on which they sit, where they are able to exchange—

Q32 **Chair:** Say I am running a business and I have got a data breach. The danger is that you could get a lot of small businesses who have not got the resources in-house; perhaps they are just not up to speed. We will get on to Government Departments. How will you be equipped to deal with the interface with your customers, which would be these institutions?

Paddy McGuinness: I do not think that every inquiry from every business will get a personal response. There is a set of guidance, and access routes to the expertise that you can get freely as a small business. But there will be contact points. If you are hacked in some sense, or have a difficulty with ransomware, then a crime is being committed and you are going to want to go to the National Cyber Crime Unit. If you are looking for guidance on how to secure your systems, those are published. If you get into extreme difficulty, it is possible to have a dialogue with the organisation.

Q33 **Chair:** It sounds like you are relying a lot on those organisations to have the right people in place to know when the risk is big enough to trigger them going to the new National Cyber Security Centre, and not just thinking, "There's a bit of free resource; we'll go there early." The danger is that the capacity out there is not as good as it should be.

Paddy McGuinness: No, indeed. A critical thing that has driven the development of the latest situation of the national cyber-security strategy has been that when we did an analysis of malware that was passing past probes that could be looked at, either by Government or commercial partners such as telecommunications providers who are partners of Government, we found in 2015 that a very high proportion—the percentage was in the high 70s—of the malware scene was eminently preventable with basic patching, just doing the thing you should do to update your patches, and basic information assurance practice. That is, not clicking on that link that says, "Your package is about to arrive." You click and "Argh!"—you get done.

With those very basic things, you could prevent being infected. For the majority of things that happen to you, it is possible to sort out your IT without having to go to the very highest end. The expectation is that the majority of these services will be provided by the market, and you can get expert advice on how to access that.

Chair: Mr Evans highlighted the 2011 strategy, and set out what the aims had been, one of which was about people protecting themselves. This is quite interesting; it is about citizens, but I think it applies across to businesses, too. According to the Barclays Digital Development Index, Britain is below Brazil, South Africa and China at keeping our phones and laptops secure; 41% of UK citizens change passwords regularly—this is a reminder to the Committee to do that—compared with 59% of people in India. Only 13% of UK citizens use password-generating software,

compared with a third of citizens in China and India.

What is the role of the centre in getting the public, individuals and small businesses to do the things that you have just described and I have highlighted there? Then what happens? What can you actually offer them? You say there is a suite of things online, if they know where to look. We will have to do a bit of mystery shopping and check that out. Are you happy with those figures that I have quoted—that only 13% of citizens, for example, have password-generating software?

Paddy McGuinness: I am not familiar with those figures.

Q34 **Chair:** I know I ran through those figures. It was a big aim in 2011 to achieve some better knowledge by the British public.

Paddy McGuinness: Absolutely. I believe we have achieved that. Where we have had measurement of it, we have found there has been an improvement.

Q35 **Chair:** What measurement have you used, just so that we know?

Paddy McGuinness: We looked at, in particular, commercial companies in the first instance. You are right: the really large enterprises tend to be expert anyway. There is a big middle of companies, some of whom are in the FTSE 250, where there is knowledge, and that is growing; we have focused a lot of our attention on the boards. There is work to do in small and medium enterprises, where things are variable, particularly when you get down to the smaller businesses, where it really is orthogonal to their business practice.

Q36 **Chair:** So you are measuring businesses, rather than individuals?

Paddy McGuinness: In the main.

Q37 **Chair:** Who are you using? You said you were getting this from the commercial sector. What information and data are you getting?

Paddy McGuinness: We have done a survey of boards, where we have gone in and looked at their cyber maturity, and we have data that resulted from that.

Q38 **Chair:** So you are like an inspectorate.

Paddy McGuinness: It wasn't an inspectorate, but we went in and, with their co-operation, did a survey of boards.

Q39 **Chair:** How many were in that survey?

Paddy McGuinness: Forgive me; I'll have to get those figures.

Q40 **Chair:** If you could write to us that would be helpful.

Paddy McGuinness: Yes, I can lay that out for you. A critical thing to get across about where we have come on this journey since 2011 is that there has been an improvement, I believe, in public understanding and commercial understanding of what is required. But we have come to a conclusion, given the volume of malware that we are seeing of the kind

that we are discussing here, which is relatively low level, so this is not a high-end hostile state hacking your computer, but this is you doing some of those basic things about phishing emails going to watering holes or your entry of passwords being interfered with and masquerading taking place—one of those three things. We have come to the conclusion that actually we need to operate at network level. In the new national cyber-security strategy—I feel I am eating the sandwiches of the new director of the National Cyber Security Centre as I say this—active cyber-defence is described in outline. We will be basically trying to operate at network level to suppress as much of that as possible. We are trialling it first on Government systems, and then we will roll it further out.

Q41 **Chair:** Okay. We will come on to Government systems in a minute. I want to bring in the Comptroller and Auditor General.

Sir Amyas Morse: Jumping back to Mr Evans's first question, if you look at the cyber-security strategy in 2011, not everything has been accomplished that was said to be accomplished by 2015. That is quite obvious. I think it seems extremely positive; you have a very positive attitude, and you are clearly keen to put forward the most positive view of everything that is going on. I don't think there is anything wrong with that, but the question I have is this: what difficulties are you having that you are really struggling with? What do you need help, support and possibly more resource for? This has a lot of energy, and a lot of good things have been done, but not everything has gone according to plan. It would be great to admit that and talk a little bit about the areas where you need more support and help. If it has not all been progressed at quite the pace that was originally planned, why not? We could learn from that. There are a lot of positive aspects here. This Report is positive, but the danger of just being extremely positive about everything and not very heavy on data is that it is quite difficult to learn much more from the conversation. Can you say what you believe you need help with? What are you finding are the future challenges to moving this forward?

Paddy McGuinness: Can I narrow that? Do you mean security of Government bodies in the round, or do you mean specifically around cyber, as we were talking about the cyber strategy?

Sir Amyas Morse: Well, the strategy had a clear set of goals. Something has been done on many of them, but to say that they have all been fully achieved would be an extreme exaggeration—and you are not saying that. What has proved to be more difficult than was thought in 2011? What can we learn from that, positively to help you move forward?

Paddy McGuinness: It is a really good question. This was a strategy, not a plan. It had stretch targets within it and aspired. That is good, and we should encourage it as a way of thinking. We learnt that the interface between the different bodies that were working on cyber-security through this period was not good enough, and therefore we have combined them in the National Cyber Security Centre, and we need that to work. There is very interesting feedback from American colleagues who set up a body. They said that they knew they had achieved when a particular commercial

organisation went to the department they felt comfortable with, because they knew people, and said, "Could you help us with that?" and the department said, "No. We don't do that. Would you please go to the body that's responsible for this?" It's when we reach that point.

Sir Amyas Morse: So you need that to work. That is one thing.

Paddy McGuinness: We need—this is absolutely critical—the structure or the interplay that Ben has been talking about. We need the people running a department and delivering services to the public to internalise their responsibility for security—for cyber-security absolutely, but also for the security of data, which does not necessarily have to be damaged or at risk through network systems, for the security of their personnel and so on; my word, we need that. That means we need them to understand their accountabilities and live up to them.

One of the difficulties we have—you will often hear it, and it comes out a little bit in the Report—is that departments' accountabilities are a bit stark if you are a small organisation responsible for the data you hold, because you have to prioritise it more than you are used to, and you are probably not a digital native. It is very noticeable that when you do phishing trials in organisations—in other words, you send a phishing email—you get a certain shape of use and of clicking on the link: the more senior you go, the larger the proportion of the stratum, because you are moving out of digital natives. The ones who are more junior in the organisation know not to click on the link. So it is about both personal practice and board practice.

Q42 **Mr Bacon:** So the people running the organisation are stabbing hopelessly at everything that comes in?

Paddy McGuinness: A couple of Government Departments have done this, and it is salutary for their boards to realise that they have had this done to them. They learn the lesson, and it is actually very powerful. It is those kinds of lesson that we need to learn.

Q43 **Chair:** So you are saying it is a cultural change?

Paddy McGuinness: It is culture. That is the most difficult thing. We also need to be intelligent, and we need to have intelligent customers for the services that are going to be delivered. Even if there were a surfeit in commerce of the kind of cyber-expertise that one needs to make systems secure—there is not—and even if we had an adequate skills base in the country, or indeed in the world, you wouldn't have it in every Government Department, so we have to have an intelligent customer interface.

Q44 **Chair:** So is that three things so far?

Paddy McGuinness: Three things.

Q45 **Chair:** It's easy to say that. How are you going to make sure it happens? Is it part of the strategy?

Paddy McGuinness: You have two significant things running at once. You have the national cyber-security strategy, which has a very heavy cyber-security focus, as you would expect, and will do quite a lot of it. If the centre is significantly successful in active cyber-defence, it will for a period change the nature of vulnerability in the UK, because it will become extremely difficult for certain techniques that are used at the moment to be used against us.

Q46 **Chair:** It sounds like the other bits are perhaps more challenging.

Paddy McGuinness: They are. The work that Ben has been doing—the review that we did, to which this Report is a very good partner—takes it in the direction of changing the way in which we organise and think about security in Government, and delivering it in a way that is likely to be more effective, not just more efficient. There is a great temptation, when one looks at the security workforce in a classic Department, to think of it in terms of numbers of people and say, "We've got to reduce the Department. Shall we reduce this?"

We have a model. We are reducing from—correct me if I've got the numbers wrong—40 different security bodies in central Government operating in the Departments down to four. We are going to cluster them. The first cluster is functioning at the moment. We are going to concentrate our security expertise and have the Departments access that. That is significant. I think there is a big leadership challenge for the Departments and for us.

Sir Amyas Morse: Anything to add, Ben?

Ben Aung: No, I think that pretty much sums it up.

Q47 **Chris Evans:** My final question to you is, do you think the systems in place are robust enough to keep up with the rapid pace of change in this area? In the past, it seems to have been cumbersome and slow in reacting. Things are getting faster by the day. Do you think you are robust enough to keep up with that?

Paddy McGuinness: With the cultural change that came with the arrival of the Government Digital Service and the focus on making use of commodity IT and services, if the Government is to pull itself along in what technology can deliver and how secure it can be, I have higher confidence that we will deliver if it hooks itself into these behemoth companies—Google, Microsoft or whatever—rather than keeping it in-house. The really significant thing here is understanding the way in which the Government, apart from in certain special areas where we need to have sovereign national capability to secure what we hold and communicate about, is making use of the extraordinary spend, technical prowess and constant evolution that you get from using commodity IT. It is those partnerships that have become critical.

Chair: I am going to ask Bridget Phillipson to take on the questioning, but I ask the witnesses to keep their answers a bit shorter. We can wait as long as you want, but I think we would all benefit from shorter answers. I

know that Bridget Phillipson will set a good example with short questions.

Q48 **Bridget Phillipson:** I will certainly try. I would like to look at the performance of centrally managed projects. In the Report, the NAO identifies three Government projects: the Government security classifications system, the Public Services Network and Foxhound. Do you think any themes emerge from the performance of those Government projects?

Paddy McGuinness: Those are three very different projects. The Government classification policy was a replacement, with something that was fit for the cyber age, of something that had existed since before the second world war to secure big rooms full of file paper. We will know if it has worked in a few years' time, when we see that people have really adapted to the way in which we structure it. So that is a very particular kind. If you will forgive me, on Foxhound for a national security purpose, I have a note on Foxhound that we have focused very tightly on its underlying capability. The Infrastructure and Projects Authority has done a review of it, termed a delivery confidence assessment, as recently as July, and has found it to be improving—to have gone amber from being red-amber, so it is on its way. I think Foxhound is an unusual programme, but if you think about those three things we have tried to do—high-end sovereign capability, securing the nuclear firing chain, or something; commodity IT, with protections being as good as you would expect from your best commercial provider; and the middle one, which is a hybrid—this is where Foxhound sits, and it is critical, I think, to secure policy making in the future. That is one that is well on its way.

When it comes to the PSN—

Chair: The Public Services Network?

Paddy McGuinness: Forgive me, yes, the Public Services Network. That, again, is a very different project, which, I think, was put on to the right track by the Government Digital Service's engagement. I note that the discussion now on PSN is to work out whether actually you need to have a Government-managed—if not actually physically run—network, or whether actually commercial provision is the best option. So it seems to me—I think that is a long way of saying no, I don't think there is a thing that is common between them.

Q49 **Bridget Phillipson:** It struck me on reading the Report that all three projects seem to have in common either unrealistic targets around what they could achieve, or they are not delivering what they could achieve, or we could not be clear in the first place whether they could ever achieve what they set out to achieve.

Paddy McGuinness: That certainly is not true of Foxhound, so that does not fit in that category. Nor is it true, I think, of the Government's new security classification policy. It may be true of the PSN.

Q50 **Bridget Phillipson:** Coming to Foxhound, on page 30, paragraph 2.41: "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." You said it is on track, but it has had problems, hasn't it?

Paddy McGuinness: It has had problems, I think, but it has changed as a programme and it is now on track—

Q51 **Chair:** I think Ms Phillipson's first point that there are some similarities among the projects is a fair point, and you said "No, no, no, not at all, Foxhound is fine." So just to be clear for the record—

Paddy McGuinness: I suppose what I am doing is thinking of where we are now, as opposed to where we may have been previously.

Chair: We do tend to look backwards; we look to learn and help Government learn from the mistakes of the past.

Q52 **Bridget Phillipson:** Turning to the Public Services Network, the original plan was to deliver at least £500 million of savings by 2014, I think every year, but that was then revised down to between £200 million and £400 million per year. In total it has delivered £400 million over the duration of the project, which is the upper end of the projected annual savings. Again, was that unrealistic to begin with, or have we not driven out the full value? I know you talked a bit about this, but it is striking that it has not achieved what it set out to achieve.

Paddy McGuinness: I think that is certainly true of the Public Services Network, and you can see that in the way it has evolved over time. So its original conception from a team, I think the Crown Commercial Services team, which was running this—

Q53 **Chair:** Do you agree with Ms Phillipson?

Paddy McGuinness: I think on the PSN I absolutely do.

Q54 **Bridget Phillipson:** On the Government's security classification system, which you also talked about, the strategic business case estimated savings against industry comparators. I appreciate that, as you said, it is a very different kind of project, but there must be comparators. There was no detailed financial business case done for the savings. Do you know why that was?

Ben Aung: The outline business case that you just referenced was never issued. We had the work done by a consultancy to look at whether or not it was achievable to create a financial case for what was to all intents and purposes an enabling change—so changing the labels at the top and bottom of a piece of paper, or applied to an email, whether or not we can extrapolate from that to the efficiencies we might see in commodity IT or cloud services. It was a very finger-in-the-air assessment that was made.

We could not find accurate data within Government for security spend across all aspects of security, and nor could we find it in industry. We did not find a benchmark that we could use, although the key thing to

reference about the security classifications policy is that it is a security policy, of which we have many; we change frequently. This is just a particularly totemic one, because it extended back for generations. It was never built on the fact that it would achieve efficiencies, other than being a system designed for paper-based files that we needed to modernise for 21st century government. That is it in a nutshell.

Q55 **Bridget Phillipson:** So again, we can't say whether it has delivered the financial benefits that were initially identified.

Ben Aung: I do not have detailed facts and figures, as I said, because most of the benefits are several steps away from changing the classification system, but the efficiencies that Departments can now make through adopting commodity IT cloud services—those are significantly cheaper than the systems that they were on. In the Cabinet Office we were using a bespoke desktop system that cost in the region of £7,000 per user per annum. We have now moved to a cloud service, in part enabled by the new classification system, that costs less than a quarter of that per user per annum.

Q56 **Chair:** So there are figures that you could identify in response to Ms Phillipson's question.

Ben Aung: The classification change is just a component of that change, which also includes the ICT and digital strategy and other things, so I wouldn't want to lay claim to all those benefits just because we changed the classification system, but it was a key component in that.

Q57 **Bridget Phillipson:** On page 28 of the Report, in paragraph 2.32, it says that those industry comparators from the initial assessment estimated savings of between £110 million and £150 million each year. What you are saying is, "We couldn't ever really have known that that would be the case, and we don't really know what's been delivered."

Ben Aung: The consultancy that derived those figures tried to establish how much Departments were spending on security every year and then compared that with comparable industry sectors for similar provisions of security—the way that we were doing accreditation of IT systems, penetration testing and those sorts of things. That is where they drew those numbers from. We never felt we could stand behind those numbers, because there were so many variables that we did not have a huge amount of confidence in. That is why we did not issue the business case. Although that was written down, we did not formally issue that business case or those numbers anywhere because, as I said, we did not have confidence in them.

Q58 **Bridget Phillipson:** Across the three projects, there would appear to be the common theme that they just are not delivering what they set out to deliver in some respects—the financial case, the savings, the timetabling. What are we going to do to stop this happening? It seems to happen time and again in Government projects, particularly when it comes to IT. What can we do to avoid this happening in future projects?

Paddy McGuinness: I think there are a couple of things that we can do. One of them is to be in the middle of the pack on what is delivered by commercial services rather than always trying to be at the front of it and generating innovative approaches. We want to be slightly behind that, because that way you get more mature models and you can be more accurate in your forecasting. That is certainly one area.

The second one, evidently, is to review quite closely your aspirations within a project. We have a set of projects here that are doing a range of very different things and were developed in a period when there was understandably a very heavy emphasis on maximising the efficiency return, and there is something about just scrubbing over that and checking the deliverability of it over time. I have often thought that one of the things to do was to make the person who wrote that document come back—a bit like share trading—three years later to see if they did the right thing, so that they can be held to account.

Chair: That's our job. You will be back, Mr McGuinness.

Paddy McGuinness: Thank you very much.

Q59 **Bridget Phillipson:** I will move on to the next area, if that is okay, which is about how Government Departments themselves perform on protecting data. First, are you confident that Departments are doing enough to keep pace with the changing nature of cyber-attacks?

Paddy McGuinness: Government Departments are doing a great deal. There is some variable geometry, so there are some Departments—the Department for Work and Pensions, for instance, or indeed HMRC, not least because of past experience—where absolutely central to their business is the delivery of services through digital means. Therefore, absolutely, and their partnerships with the bodies that were originally in the alphabet soup and now with the National Cyber Security Centre are extremely tight—also with industry.

There is something about maturity in a Department that you also see in commerce. One of the joys in commerce is when someone comes, for instance, to CERT-UK, now the National Cyber Security Centre—I could cite a number of businesses that have done this, but I suspect they would not want me to speak publicly about it—and says, "This happened to us. We resolved it this way. We thought you should know about it. You might be interested." That is quite interesting, and we are beginning to get that from the more mature Government Departments.

For other Departments that are far smaller and far less focused on delivery of services by digital means, these clusters that we are building will help them with their maturity, because they will get access to a larger Department with critical mass, with expertise both on what you can get from the market and on the interface, with the skills that the Government have to offer.

Q60 **Bridget Phillipson:** That takes us back to the Government's approach and what can be done centrally—and what cannot be done centrally, but

where there could be an impact on the delivery of public services. For example, to take the recent incident at the Northern Lincolnshire and Goole Hospitals NHS Foundation Trust, the attack there appears, purely from the media coverage, to have been dealt with quite effectively. How do we ensure that other bodies dealing with personal data and handling information, or where there are vulnerabilities, know where to come and how to access the right response that they need? I read that that case was not so much a cyber-attack as a malware or ransom attack—whatever you want to call it. How do we make sure that they know where to come and how to respond?

Paddy McGuinness: That kind of ransomware attack is absolutely a cyber-attack; it is a really good example.

Bridget Phillipson: I appreciate that it is an attack; I am just trying to get the terminology right.

Paddy McGuinness: Indeed. The answer is that that was dealt with in the stack—so down here, among the many things that the National Cyber Security Centre was doing, that is one of the things that it supported, along with others looking at the criminal aspects. That happens regularly and does not get a particularly high profile. That case clearly had an impact on services to the public, and therefore it got a different profile. So that is going on and, absolutely, we need to keep working on our interfaces, our products—

Q61 **Chair:** How often is an incident like that happening?

Paddy McGuinness: I don't have the numbers available to me here, but with a degree of regularity.

Q62 **Chair:** Do you mean monthly, weekly or daily?

Paddy McGuinness: I would mislead you. Let me go away and get the National Cyber Security Centre to let you know the kind of rate, but they classify—

Q63 **Chair:** I think it is quite important for people to realise, when providing their information to organisations such as their doctor and hospital, what the risk is.

Paddy McGuinness: Yes. This is about how often we have such an incident, though not necessarily in the health service. The National Cyber Security Centre deals with incidents of that kind of level with a degree of regularity.

Chair: Write to us with some information about the regularity of such incidents.

Q64 **Bridget Phillipson:** Do you think that across the NHS, for example, the culture is catching up with the reality of where we are? For a long time, data was held on hard-copy records—it still is, in many cases—and we had gatekeepers for that hard-copy material. Now that we have moved towards digital, do you think there has been enough of a culture change

in organisations such as the NHS to understand the risks that can be posed by such attacks?

Paddy McGuinness: No. We had investment under the previous national cyber-security programme, and under this one, including with the NHS, to stimulate that. I think that events such as the one you described help with that, but no—but that is true across society. I think it is true for all of us in this room and for every business—we are on a journey where we are having to learn about this. Particularly as we go towards the internet of things, it is going to become ever more true.

Q65 **Bridget Phillipson:** Previously, there was the annual information security return, when Departments submitted returns with information of variable quality—the NAO notes—and often quite late. It appears that that process is moving on, but what work will be done to bring together those risks, to analyse trends, rather than taking Departments in isolation?

Paddy McGuinness: Maybe Ben Aung could answer that.

Ben Aung: We replaced the process you just described with something called the departmental security health check. One of the reasons to replace it was that the previous system relied on Departments and Department security officers expressing their security concerns and risks in a consistent way—specifically, we allowed them a free text form to fill out and provide us with annually. That meant it was very challenging for us to compare different Departments and different sorts of risks.

The new process is much more binary in many cases, and much more enabling for statistical assessment and evaluation. The report we have just produced off the back of last year's returns has graphs. We can see trends and we can understand where risks are burgeoning in different parts of the system and where we are doing better in other areas. So we are on that journey. In general terms, our approach is to be far more data-driven than we have previously been in terms of understanding risks and trends, but it is very challenging, if not unrealistic sometimes, to expect Departments to be able to understand their systems and security approaches in a very consistent way, but we are much better at it.

Q66 **Bridget Phillipson:** Could we just look at figure 6 on page 22, which shows the data incidents reported to the Information Commissioner from the largest Government Departments? Mr McGuinness, what would you say about that data? What does that chart, as presented, say to you?

Paddy McGuinness: It says to me that we don't have sufficiently specific guidance from the Information Commissioner's Office on what should and should not be reported, so we are doing some work with them to think about how we should set that. There is some exact language—I looked at it just before I came out—in the terminology used by the Information Commissioner, and you will see that it is very broad. The latest guidance states, "If a large number of people are affected or there are very serious consequences, you should inform the ICO." That is open to interpretation if one delivers services.

Q67 **Bridget Phillipson:** It is, but is it not incumbent on the Department in question to consider what impact that would have and have discussions with the Information Commissioner? Why has that not happened already?

Paddy McGuinness: Indeed, they do that.

Q68 **Bridget Phillipson:** They are either brilliant or they are awful, looking at the numbers. Some are reporting en masse. Potentially their performance is appalling, or maybe they are just very good at picking up on incidents and reporting them. In other cases, I find it wholly incredible that the Cabinet Office could report only one incident in one year and that the Department for Work and Pensions, which handles a considerable volume of data, reported only two incidents to the Information Commissioner, with incidents recorded but not reported at zero. That is surely not credible.

Paddy McGuinness: That is why we are going with the Information Commissioner to work for clearer standards so that it is more straightforward for Departments, and frankly to improve the conduct—

Q69 **Chair:** Mr McGuinness, I think Ms Phillipson was trying to point you to a culture issue. You have got more than 6,000 incidents recorded but not reported by HMRC, and on data handled by DWP there is nothing at all. It is not just about guidance from the Information Commissioner, is it? A bit of common sense applied might suggest that there must be some issues sometimes.

Maybe DWP is working perfectly and there is never a breach, but I have had letters, as have other colleagues. I am not picking on that Department particularly. We get it all the time. The Department writes "Re: Ms Smith" and then tells me all about Ms Jones's circumstances in the letter. These things happen. We have all got them. Round this table we have got more than zero from that one Department, and the same goes for other Departments. I just worry that you are a bit complacent here, saying it is all down to the ICO.

Paddy McGuinness: I should that hope I am not. I am a great believer; given my security function, I like breach reports.

Q70 **Chair:** So, in response to Ms Phillipson's question, figure 6 is actually bad news because not enough of them are reporting breaches. Is that how you read it, or am I putting words into your mouth?

Paddy McGuinness: I think you are, because I think it is in the specifics of each case, and I can't speak to those. In principle, I like the idea of having a clarity about what should be reported and it being reported and us being able to look at it. That is what I like.

Q71 **Bridget Phillipson:** What is the timescale for that?

Ben Aung: It is ongoing. We have begun those discussions.

Q72 **Bridget Phillipson:** With an end point that might arrive?

Ben Aung: The difficulty is that those definitions and thresholds that the ICO publish are to cover all organisations in the United Kingdom, not just Government, so for us to interpret their published guidance in a way that is more meaningful for Departments will require them to balance whether they are consistent.

Q73 **Chair:** I am still puzzled as to why it waits for the ICO. You could suggest guidance that says, "This is what the ICO says. We interpret this to mean that if you send Meg Hillier MP a letter about Ms Smith but include the details for Ms Jones, you need to record that as an incident." You could provide that information without waiting for the ICO. I am just using my initials; I am obviously not the Information Commissioner's Office.

Ben Aung: One point I will make on the figures in the NAO Report is that there is a consistency between numbers of incidents reported to the ICO. They are in very low numbers, if not zero. Probably what this sort of report and even our own reports cannot capture is the amount of informal engagement and discussions that go on between Departments. Most of these Departments, if not all of them, will have an established relationship with the Information Commissioner's Office and will speak to them very regularly. They will test their assumptions on whether they should report something and whether it warrants it and meets the threshold.

That said, when I look at the other column, the right column, I see an organisation in HMRC that has an online reporting tool where every individual who works there can report with the click of a button when they feel unsure or nervous about something. It could be a lost pass or someone who has tailgated them, or any number of security incidents, and that, as Paddy says, is what we want in the system. We want an amnesty of reporting. Beyond that, I see Departments that have less maturity or less capability for collecting that data. To sit the two ICO reports against the breach reports is useful, but it is not the entire story. As I said, there is a consistency with reporting to the ICO between Departments; what we see on the right column is Departments that are better than others at collecting all of their breach data.

Q74 **Bridget Phillipson:** But if we were to compare, say, HM Revenue and Customs with the Department for Work and Pensions, we see that HM Revenue and Customs had more than 6,000 incidents. That could be because it has a good culture of reporting breaches. The Department for Work and Pensions had zero. What would that suggest: that it is an incredibly effective Department, or that it does not have the right culture?

Ben Aung: There is obviously something that needs addressing there. I would not for one minute say that DWP has had zero incidents in that period compared with HMRC. It obviously is comparable in many ways in terms of business. There are other variables here. It is whether DWP has recorded that.

Q75 **Chair:** So what are you doing about it?

Ben Aung: This Report has given us an insight that we did not previously have into that disparity in reporting, so we will address it.

Q76 **Chair:** So this is the first time that you have thought about this—since the NAO came in to look at it?

Ben Aung: It is the first time that we have thought about the fact that Departments are recording breach incidents in such significantly different ways. We know that Departments face those security incidents in fairly consistent ways. There is an issue about the way they are recording them in the data that the NAO has pulled out from their annual reports and their websites. I am not saying that it is the first time we know there is a disparity between Departments in the number of breaches. What is highlighted to us is the disparity in the way that they are recording them and then reporting them publicly on their websites.

Q77 **Bridget Phillipson:** On a separate issue about the Information Commissioner and the guidance and which incidents should be reported and which should not, there must be a better mechanism for Departments themselves to know which incidents to record. Even if you are unsure as to whether it merits reporting to the Information Commissioner, if you take the example that you gave of a lost pass or someone tailgating you through a security door, surely someone in the Department for Work and Pensions would be just as aware as someone in Revenue and Customs that that might be worthy of reporting. If we assume that Revenue and Customs have simply got a good reporting culture, how do we support other Departments to learn from that culture and share that practice across Government?

Ben Aung: A really good example is the fact that HMRC are the lead organisation in our new trial cluster. Their reporting system, the incident management system, is now being rolled out across every organisation in that cluster. Every other Department in that cluster, which includes the Cabinet Office, DCMS, HM Treasury and some other organisations joining a bit later, will benefit from that system because we now know about it and it has been socialised and understood through the cluster work. There is an ongoing question that we have already raised about whether that system should be Government-wide. I appreciate that what this is highlighting and what we have highlighted through the cluster work is very good practice when compared with other Departments. The work that is under way at the moment is an opportunity to spread that across Departments without negotiating individually, but through the mechanism of clustering Departments.

Q78 **Bridget Phillipson:** There is an argument that if Government Departments are not very good at doing this, why would anybody else be good at it? There does seem to be a problem with Government Departments, yet it is Government that the wider public will look to for advice, best practice and guidance. They cannot have a great deal of confidence at the moment when they view the Government's approach to the reporting of data incidents.

Ben Aung: To go back, I work very closely with DWP on a daily or weekly basis, who have a very capable, very well resourced security team there. So although these figures are very stark in what they represent in terms of numbers, I know that the reality of the capability in DWP to address its own internal security issues for a range of breaches and also the very significant online services that it hosts is not represented in these figures. So there is an issue about the figures and the presentation that does not necessarily correspond to my understanding of how the Department manages security.

Q79 **Bridget Phillipson:** There is an example in the Report of the good work the DWP does in staff and supporting them around training. I understand that, but the wider public will think, "Government should surely be setting the standard." Are Government setting the standard?

Ben Aung: We set the standard in terms of security. These figures I think misrepresent that standard and are something that we will need to think very hard about.

Q80 **Philip Boswell:** Further to Ms Phillipson's questions around figure 6, I refer you to figure 7 on page 24 of the NAO Report. This is a question about resources, which my colleagues and I have all touched on at one point or another. Figure 7 is a somewhat chaotic chart, which is hard to follow at times. The vagaries there may be are more about poor metrics or changing metrics than about actual changes in cyber-security breaches, reported or otherwise. If you look at the figure around Q1 of 2015 and the coloured code below, it shows that "Lost or stolen paperwork", "Other—Principle 7 failure", "Data posted or faxed to incorrect recipient", data passed to incorrect recipient, insecure websites and so on, which are predominantly human error-oriented data security incidents, are all seen to rise sharply, just at the time—Q1, 2015—when Government cuts were ramped up after about five years of austerity. Do you recognise that cutting Government Department resources, putting more pressure on existing staff, as most efficiency drives tend to do, has contributed to the spike in human error-driven data security incidents by the UK Government's staff?

Chair: It is a complicated chart, but Mr Boswell's point about human error is quite clear from it.

Paddy McGuinness: Clearly there is an issue with human error. What is not clear to me is whether that is to do with reductions in staffing or morale or indeed just simply reporting patterns—

Q81 **Philip Boswell:** Or restructuring, which has been ongoing.

Paddy McGuinness: Or restructuring—that is not clear to me. I do not think I can answer your question. I do not know, and it would perhaps be placing too much weight upon the data that we have here to take it that way.

Q82 **Philip Boswell:** Okay. Would you agree that if targets slip again, now you have readjusted or recalibrated, that is more likely to do with you

remaining short of adequately qualified and trained staff? Can the Government compete with the private sector in attracting the best in industry?

Paddy McGuinness: It is a challenge for Government to draw in the very high end of experts in information security, cyber-security and the like. It is a challenge because there is a shortage of people with those skills in the United Kingdom and one of the strands in the work of the National Cyber Security Strategy is to build up that and do all we can. Industry are also focused on it and we are in partnership with them and academia, with apprenticeships and so on.

There is a difficulty with the high end. There are still attractive careers to be in for the kind of work that the majority of people are doing at interface-level, working with networked systems. That is not things like high-end security, systems architecture and data scientists. We are able to attract those. We have got an intensive training programme and we have got an e-learning package called "Protecting Information", which has been taken by 1 million people across central Government and the wider public services to improve their performance.

Q83 **Philip Boswell:** Just one last point, which goes back to Ms Phillipson's well-made point on figure 6 and the vagaries therein. Is one of the reasons why certain Departments do not report because a negative score could affect managers' bonuses, performance contracts and promotions? Would that be one of the reasons why certain Departments are reluctant to report?

Paddy McGuinness: Personally, I would quite like it if there were significant consequences to a failure in security in a Department, but I don't think that that is what this represents. I don't think that is the factor in play here. I have no specific example of that. I don't know whether you do.

Q84 **Chair:** You can imagine that someone could put their head down and think, "I won't report this. No one will realise it was me", and the incident then doesn't affect their career path. Are you sure that has got absolutely nothing to do with it?

Paddy McGuinness: I couldn't say in every single case, but that isn't the culture that I find. I find a culture of sincere work in the public interest. When something goes wrong, there is a wish to put it right. On the whole, people put their hands up and say, "Something has gone wrong here; we need to put it right."

Q85 **Chair:** We won't talk about whistleblowing here, but if everything was always that fine, that would be great. I will bring in the Comptroller and Auditor General before I bring back Bridget Phillipson.

Sir Amyas Morse: I am sure everyone is working in the public interest, but some of these areas—areas where you know there are massive communication interactions with the general public and things like that—predispose risks of some kind, and it would be quite possible to do some predictive modelling on that, where you would expect that there would be

a certain number of breaches, not because anyone is behaving badly, but because of the nature of the operations that they are carrying out. If they are not reporting according to that, it is a reasonable question as to why not. If you really want to know what's going on, either they or you could take that sort of view.

Paddy McGuinness: I agree. I don't know whether you want to comment.

Ben Aung: There's a really important point in there about the maturity of an organisation in terms of not measuring how many breaches it does not report, but measuring how well it responds when breaches do occur. The very fast-paced nature of cyber-security and the threat means that we will never have absolute protection. Being able to respond is critical, and the Government and industry generally are not in the mature place that we need them to be. We need them not to be preoccupied with trying to prevent everything, but to be ensuring that the processes and capabilities are in place to respond effectively. That is a leadership point, a technical point and a skills point. These figures in HMRC and others are the beginning of that recognition in some organisations that it is not about sweeping things under the carpet or sticking your head in the sand. Instead, it is about thinking, "We are going to deliver this online service. We will have some vulnerabilities inherent in delivering an online service. Our ability to respond to a breach is critical."

Q86 **Bridget Phillipson:** Moving on to a slightly separate point on the EU general data protections regulations, are you still working on the basis that they will be introduced in the UK?

Paddy McGuinness: The GDPR are due for introduction in May 2018. We are working on the assumption that at that point we will still be members of the European Union and will introduce them. I note that we were major contributors to their design and development, and it would be eccentric of us to now say that they were not an appropriate body of regulation, given that we were so much a part of developing them.

Q87 **Bridget Phillipson:** How will central Government deal with the impact, not only centrally, but in terms of the support for the wider public sector and others affected by how the regulations will apply?

Ben Aung: As with other regulatory frameworks and other rules and legislation that we must apply, there is a role for the centre to ensure that it has sufficiently interpreted the new regulations for the very specific contexts that Government Departments find themselves in. We will certainly do that. We have done that with the existing Data Protection Act. We have information assurance and information security standards that exist solely for that purpose. I have no doubt that we will have those again in the future.

There is a point there: Government previously was a very different, bespoke creature, but over the past few years we have tried to converge the way that we think about data, IT and systems to make it generally much closer to the industry model and commercial good practice. That

means that we now have to do less reinterpretation of things such as Data Protection Act regulations and so on that are now UK-wide, because actually we are not so very different. Some of the IT programmes we have done previously were very Government-special. We now try to adopt commodity technologies, where lots of these things are baked in from when we buy them off the shelf.

Q88 **Bridget Phillipson:** As you say, Mr McGuinness, as we will still be members of the European Union then, those regulations will be introduced. Will they therefore have to be part of carry-over legislation to ensure their continued applicability at the point of departure from the European Union?

Paddy McGuinness: They will remain in force unless they are removed, in practice.

Q89 **Chair:** Are they going to be in the Digital Economy Bill?

Paddy McGuinness: I am not certain; I had better come back to you with the specifics.

Q90 **Chair:** I just want to quickly pick up on that point. If you look at figure 8 on page 25 of the Report, the red line at the top shows what happened when automatic reporting of health sector breaches happened. It is much higher than the cluster of breaches in any other area. Presumably, with mandatory reporting, as under the EU general data provision, you would expect to see a similar jump in data breach reporting? You are not sure between you.

Paddy McGuinness: There are particular factors that have created that spike that I do not think have been discussed.

Q91 **Chair:** It is not so much the spike but the differential overall. The spike itself is interesting but, in simple terms, there is a gap between the red line and all of the other lines. That is the bit I am interested in.

Paddy McGuinness: And specifically whether it is better to have mandatory reporting or not?

Chair: Yes.

Paddy McGuinness: We have worked on the assumption that we need to lead organisations to maturity. Mandatory reporting, if they don't understand what is happening on their systems, isn't going to particularly help them. It will drive it some way.

Q92 **Chair:** Is that talking about all organisations or just Government Departments at this point, just to be clear?

Paddy McGuinness: There are some sectors that choose to have or have mandatory reporting; others do not. We have chosen to work with those in Government that do not. We've discussed it with them and within Government to consider whether or not mandatory reporting would materially change what we are able to do and we have concluded at this point that it would not.

Q93 **Chair:** What about private businesses, with the malware and so on that is going on? Tesco is still rumbling on. If you are being held ransom as a company, because of the damage to your reputation and the damage to a chief executive officer, for them personally and the threat that they could lose their job if it is revealed to the public, and with the public scare that that might create, there could be a big temptation not to report it immediately.

Paddy McGuinness: We focus very much on this in the GDPR and the provision within the GDPR for the right to know when you've been hacked, which creates an obligation. Rather than creating a separate obligation, we have relied on that.

Q94 **Chair:** How quickly? Let's say I am a private company running a health business. I've got access to very sensitive personal information about patients and there's a breach. I'm tempted just to sit on it, because it might be embarrassing or I might not get my contract renewed with the NHS in future. That could be a real scenario. How quickly will the new EU requirement require me to report that breach, so that patients—the people whose data I've got—are aware?

Paddy McGuinness: I don't have that detail in front of me. I will have to get it and write to the Committee to let you know.

Q95 **Chair:** Do you know if it's a matter of hours? Days?

Paddy McGuinness: I literally do not have that data available to me.

Q96 **Chair:** That's the key thing. Automatic reporting sounds like it is fairly instant or fairly quick, and that is obviously historic data. It seems to us looking at this that if you have got real-time information, the citizen is protected because they know what is happening; breaches will happen but we need to know about it. Do you agree that if breaches happen, citizens should know about it?

Paddy McGuinness: I think what is important is that measures are taken to counter them. There may be reasons to make them public or not, depending on the nature of the breach.

Ben Aung: I will just add that having seen a lot of these things play out I can say there is often a high degree of ambiguity around a cyber-breach, well into the recovery and response process, about whether or not you have indeed been attacked or it is just a failure of another IT system. With hindsight, when you look back at attacks such as TalkTalk and other incidents in recent years, you can sometimes see the exact point at which the breach occurred, and then you can measure on when the public should have been informed, but when you are in the midst of one of these issues it is very unclear as to whether or not there has been an attack. You have to balance and weigh up whether informing people pre-emptively or too early could be counterproductive.

Q97 **Chair:** You say counterproductive, but if it was my bank account details with TalkTalk, or my personal details with the NHS, I would want to know pretty quickly so that I could keep an eye out in case something was

going wrong and I could change a password or whatever.

Ben Aung: If there is a meaningful step that can be taken by the consumer of that service or the customer, that is quite different, but if you're not sure—

Q98 **Chair:** So what would your recommendation be? If there is a meaningful step that a citizen can take to protect their data or limit the damage, how quickly should an organisation tell them?

Paddy McGuinness: Classically, if you have an interaction with an organisation in, let's say, the financial sector, you would expect that the financial authorities—the Treasury and the Financial Conduct Authority—would be in dialogue with the bank, or possibly the National Cyber Security Centre would be in dialogue with them, if that is where the breach was. You would expect them to immediately talk about what they did with their customers. On the whole, banks, if they have this happen to them, immediately act with customers, and they find a way of acting as fast as possible.

Q99 **Chair:** So you are saying that customers are built into the National Cyber Security Centre's planning? Your focus is on customers from the moment of a breach.

Paddy McGuinness: Our focus is on recovering the breach and understanding what has happened, which often takes time. We encourage people to fulfil their responsibilities. If they have breaches of customer accounts, for instance, we say to them, "You must act with your customers." Usually, though, they are already on their way.

Q100 **Chair:** Before I bring in Mr Bacon, you talked earlier about the processes that people go through to get information and online support and so on. Say there is a big data breach—like the hospital one that happened recently, or Tesco Bank—that involves a lot of very personal information. If I was running Tesco Bank and rang you to tell you that we had had a breach, is there a blueprint for that first hour or two after the breach? Can the National Cyber Security Centre take certain steps to limit the damage?

Paddy McGuinness: I should be careful here. I hold the National Cyber Security Centre to account. What exactly happens or happened in that first hour—

Q101 **Chair:** What do you think would be good practice to happen in that first hour or two? Is there a blueprint—is there a standard approach or a checklist of some sort? When the riots happened, there was a gold group in each borough and certain actions were taken, including on publicity.

Paddy McGuinness: There is a triage process, but the point that Ben Aung makes, which is very significant, is that there is great variable geometry to the way these things come about. They are often spoken about publicly—I am not referring to Tesco; I am just speaking generally—before what has happened is understood. It often takes until quite long

into the recovery phase to fully understand what has happened in the network system and put it right.

Q102 **Chair:** Do you think it is wise to send out a warning to people saying, for example, "We don't yet fully know what is happening, but you need to be aware. Keep an eye on your bank account for any suspicious behaviour"? Would you consider that to be good practice?

Paddy McGuinness: I am not sure whether that is necessarily good practice in and of itself. It is good practice if a set of things happens for the customer. That might include communication with them, or I can think of one example in which a particular way in which a service was delivered, which was the source of fraudulent transactions, was removed. In other words, they just said, "We will no longer tolerate these kinds of transactions on our system." So they immediately protected their customers and then got in touch with those who had previously been affected. That was a good way of doing things, but I don't want to say to the Committee—or, indeed, to someone who is watching—"You should do this," because it may not be right in that particular incident. What is vital is that when it happens to them the institutions who hold the data—financial institutions tend to be very good at this—must act, and they must act in an appropriate way to protect the interests of the customer.

Q103 **Chair:** If you are a public-facing or customer-facing organisation, announcing a breach of data is a big reputational risk. It can hit share prices and individuals' bonuses and affect whether they keep their job. No one wants to lose their job, but a senior person might be worried about that, and the temptation might be not to say anything. Are you telling me that you cannot tell us how quickly someone would have to report it under the new European legislation, because you don't know?

Paddy McGuinness: Simply because I did not bring that with me today. I shall have it sent to you.

Ben Aung: I would just make the point that although we do not have a response blueprint because all systems, companies and organisations operate differently, we do invest in, promote and advise that the Departments exercise these issues as much as they can, because that is the learning that an organisation needs to go through. Who do you call when it happens? How do you bring in a press team? That is the critical experience.

Q104 **Chair:** How convinced are you that people now know who to call? Who do you call? Not ghostbusters, but the National Cyber Security Centre. Is that written in now—that all those organisations that you are worried about there being breaches in know where to go?

Ben Aung: That knowledge and awareness will scale up.

Q105 **Chair:** So what is the penetration at the moment—50% of small companies, all Government Departments? Have you any idea? Have you got any targets for how fast you will get people understanding, so that they say, "We've got a problem; we've got to call these guys who are

attached to GCHQ. We've got a phone number; we know where to find it"?

Ben Aung: Every breach that has occurred since they launched, that we were aware of as a Government, they have been a significant party to. There is now, I think, a more common understanding that there is a commercial imperative to be publicly responsive to a breach, because to be seen to bury it proves more damaging in the long term.

Q106 **Chair:** You say "now".

Ben Aung: As Paddy McGuiness said earlier, company boards have seen other company boards go through these things. They speak about these things. There are forums where they discuss these issues. I think we now have an evidence base that says, that if you try to hide it, it comes out six months later and you get a hammering in the press. If you are seen to be on the front foot—you hold your hands up, put in place measures and communicate to your customers—that is one of the best mitigation and response measures that you can employ.

Q107 **Chair:** Do you think the same is true in Government, if a Department admits something early? Do you think there is an impact on the Minister's career?

Ben Aung: It is a very different dynamic. Often, the sorts of issues we have in Government we are not able to disclose publicly, because we are following them up and investigating and responding in certain ways, but I think the same applies.

Chair: I think we are a bit of a way from the open culture yet.

Q108 **Mr Bacon:** Mr McGuiness, you said earlier that there were big leadership challenges for Departments, and that there was a need in Departments to understand and to live up to their accountabilities, yet from listening to you this afternoon, I have detected a certain reluctance to tell Departments what they should do. There is no mandatory reporting. There is no mandatory training. There is no mandatory certification. There is no mandatory regulation. Somehow, by some process of learning and osmosis—and if Mr Jackson were here I am sure he would throw in "sitting around in a circle on beanbags"—this information will get to the people who need it. What is wrong with mandating what is required in terms of regulation, certification and training?

Paddy McGuinness: In terms of training and board familiarity, I think it is right that you can mandate it, but it bears a bit of examination. Let me give you three examples. There is a difference between the Department for Work and Pensions, which generates a significant proportion—a third perhaps—of BACS transfers in the United Kingdom and therefore is facing the public and working with the banking sector; the Foreign and Commonwealth Office, with its presence overseas, including in category A espionage posts, where people are trying to break into our systems and steal our secrets; and the Ministry of Defence, which is running the nuclear firing chain. Those are all very different organisations and, frankly,

we had not thought that it was useful to try to write an overarching standard that you would apply to all of them. What we have tried to do—

Q109 **Mr Bacon:** There must be common minima that one would expect to adhere to. When I first worked in an investment bank, before I was allowed to speak to a customer I had to take a stock exchange exam and become a registered representative of the stock exchange. It did not matter whether I was in commercial banking or corporate finance or asset management, or writing speeches for the chairman or the chief executive about why integrated investment banking was such a good thing or not—all of which were extremely different domains—or foreign currencies or sterling money markets, all of which I did, apart from asset management. I had to do the exam regardless. What is wrong with setting a minimum standard, from which, for sure, you can branch out and add things, depending on whether you are in the Foreign Office or in the Department for Work and Pensions? What is wrong with doing that?

Paddy McGuinness: There is value in having a commonly available set of courses—

Q110 **Mr Bacon:** Not just available. My question is: what is wrong with mandating a minimum?

Paddy McGuinness: We could do that, but we would still fall a long way short in those Departments of what was required. What we need is something that is bespoke to that category of—

Q111 **Mr Bacon:** Paragraph 3.29 on page 37 says, "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)". You have said there is a big leadership challenge in Departments. You have said that Departments all need to understand and live up to their accountabilities. If there were certain absolute minima before someone could be a senior information risk owner or a departmental security officer—if, before you could even fulfil that role, you had to get your ticket, as it were—it would, among other things, raise awareness inside Departments of the importance of this, would it not?

Paddy McGuinness: If I may, I will get Mr Aung to comment on the question of how we generate skills, but on that particular point—

Mr Bacon: I didn't ask you about how you generate skills. I asked you whether it would raise awareness.

Paddy McGuinness: It may well raise awareness.

Q112 **Mr Bacon:** You think that if it were mandatory to have an exam, and if you had to get your ticket or certification before you could be a senior information risk owner or a departmental security officer, that may raise awareness in Departments. Is that your evidence?

Paddy McGuinness: My evidence is that paragraph 3.29 refers to a system that no longer exists; we have removed it because it did not work, and we have put in place a different way of doing it, which is—

Q113 **Mr Bacon:** But you are still not going to mandate it.

Paddy McGuinness: We are going to have skilled Government security officers or chief security officers for each Department, and we are going to raise the standard for each of those. Depending on the nature of the Department or the clusters they are in, they are going to have particular emphases in their skills.

Ben Aung: A few years ago, we had a very prescriptive set of policies and mandation, quite similar to the one you described. We found that it was highest common denominator and did not account for the high degree of variance in departmental business. The knock-on effect was inhibited technology adoption and business generally, so we moved away from that to a more flexible description of the requirement, with an overarching mandatory regime that was outcome-focused. We didn't tell you how you had to achieve a particular security outcome. All that was required was that the accounting officer or permanent secretary committed to it and then signed off the fact that it had been achieved.

Q114 **Mr Bacon:** So they have to attest that it has been done, without saying how it has been done.

Ben Aung: They did tell us, but we didn't tell them how they had to do it in every instance. It was for them to tell us how they had achieved the aim we had set out in our policy framework. With things like senior information risk owners, we defined the role and the responsibilities, and again the accounting officer would attest or sign off the fact that they had implemented the senior information risk owner role as written. We found that over time, the standard and application of those policies and frameworks drifted. What we were expecting to get was no longer what was happening on the ground, which is why we have reviewed the space. We now have a standards board, which we have just established, to do exactly the thing you referenced.

Q115 **Mr Bacon:** Why don't you just have someone whose job it is to be responsible for it?

Ben Aung: It is very challenging to strike the right balance across the multitude of Government Departments.

Q116 **Mr Bacon:** Why? I know that the actual business of delivery will vary hugely. You have explained that, and plainly we know that different Departments do very different things, but why is it not possible to point at one person—a man or a woman—in a particular Department and say, "This is your job. This is your responsibility"?

Ben Aung: That is exactly what we have done. It is the chief security officer who is writing the job role description centrally. We have not worked out the exact dynamics in terms of reporting lines, but there will

be a smaller number of accountable full-time professional individuals of the right seniority.

Q117 **Mr Bacon:** When you say chief security officer, are you referring to the chief security officer at the centre following these reforms? Will each Department have its own chief security officer?

Ben Aung: Each cluster will.

Q118 **Mr Bacon:** And how many of those are in place now?

Ben Aung: We have just launched one trial cluster, with a chief security officer at the head of it.

Q119 **Mr Bacon:** When will each cluster have a chief security officer?

Ben Aung: The roll-out of clusters—these are, in many ways, machinery of government changes—while we are consolidating security teams will run until late 2018/early 2019.

Q120 **Mr Bacon:** So by the end of 2018/early 2019, each cluster should have in place an appointed chief security officer?

Ben Aung: Yes.

Q121 **Mr Bacon:** And will that person be trained and certificated?

Ben Aung: Yes.

Q122 **Mr Bacon:** I will just go back to Mr McGuinness's raspberry ripple analogy. I have never worked in an ice-cream factory, but I have done many things, and it seems to me that if you had a bloke or a woman whose job was to make sure that the raspberry went into the ice-cream, so that when it came out the other end it didn't look like vanilla but raspberry ripple, you could point to that person and say, "This is the reason there's no raspberry. You didn't put any raspberry in." Are you saying that's essentially what is going to happen with these clusters?

Paddy McGuinness: These clusters will provide that expertise, not least commissioning expertise, for the highest-end security capability— for instance in cyber, but possibly in other areas too—that will run across the whole of the business of that Department, or of the Departments within that cluster. I regret using the raspberry ripple analogy; I think orthogonal is a better word. This will lay across the whole thing—

Q123 **Mr Bacon:** What's a better word?

Paddy McGuinness: Forgive me—it will lie across the whole of the set of Departments that are there. They will be security professionals responsible for the delivery of security in that cluster.

Q124 **Mr Bacon:** Right. Two more questions. I was at a seminar—a round-table—on data and security a while ago at a party conference, and the word GAFTA came up, which I'd never come across before; it stands for Google, Apple, Facebook, Twitter and Amazon, and everyone around the table except me seemed to know about it. Are you content that you've

got the policy environment and the legal framework you need to do what you need to do to get the co-operation of these major players and holders of data in the globalised economy?

Paddy McGuinness: In terms of the delivery of services through Government—Government access to the cloud, for instance?

Q125 **Mr Bacon:** In terms of protecting the United Kingdom.

Paddy McGuinness: That is a very, very broad question. We have the Investigatory Powers Bill, of course, which is still on its way—

Q126 **Mr Bacon:** So the answer is, "Not yet"?

Paddy McGuinness: No. Forgive me; let me say two things. One is—this is a very interesting hinge for us—that on the one hand, in the provision of the kinds of services that Ben Aung has described when referring, for instance, to what the Cabinet Office has done, where we have made use of Google's cloud and access to Google's cloud, but in a way where the security of it was certified by the emanations of GCHQ, which are now embodied in the National Cyber Security Centre, I am very satisfied with that co-operation; they are a fantastic partner.

I would like, if and when the Bill becomes law, to see Google, if it is served by a warrant, provide unencrypted data to enable law enforcement and Security Service work. I'd also like the company to take a responsible position themselves in relation to the removal of pernicious content that is on their networks, whether that be about child sexual exploitation, modern slavery or indeed the use of their networks—if they are being used—by Islamic State in Syria and Iraq, for instance.

Q127 **Mr Bacon:** Would you say that those companies still have some way to go to meet legitimate Government expectations in that regard?

Paddy McGuinness: Absolutely, I would.

Q128 **Mr Bacon:** Good. One more question—final question. It was reported three years ago that the Kremlin had started to use typewriters for the most confidential material, on the basis that the most primitive methods are preferable. Not only can you identify one typewriter uniquely but of course they are rather difficult to hack.

Now, paragraph 1.8 of the NAO Report says, "Historically, government's information was largely paper-based and did not need to be immediately accessible or easily shared between departments, businesses or citizens." Now, we take it as read, or we seem to take it as read, that everything has to be online, it has to be in the cloud, it has to be electronic and it has to be available to everybody all the time, and yet surely the most secure way to keep something safe is to have it not being accessible to very many people, and if there is a slight price to be paid in terms of the immediacy with which it can be accessed in different places, then, in terms of maintaining a high threshold of security, that might be a price worth paying, mightn't it?

Paddy McGuinness: Yes, I would agree with that. In terms of securing the material that is of the very highest concern, I think that when we laid out the changes that were made to the Government security classifications, we laid out three categories, broadly speaking: one that allows the use of commodity IT; one that is sovereign, so that Government itself, in partnership with trusted industry, generates the protection; and one that is hybrid, in other words it allows you to work between those two areas, and that's what Foxhound falls into. Clearly, one of your options, when you are talking about the highest level, if you do not need to use a network in order to achieve the task, is to do it in hard copy, but I do not really want to discuss in a public forum how we put all those elements together to be secure.

Q129 **Mr Bacon:** No, but it is just striking that no government system has yet been devised—including the highest classifications in the Pentagon—that does not seem to be capable of being penetrated by a 15-year-old in his dressing gown in his bedroom somewhere in Neasden. This seems to happen quite regularly.

Paddy McGuinness: I must confess that with my intelligence title and in helping to oversee the single intelligence account, I wish that were true, because life would be much more straightforward. Sadly, it isn't. I would reflect, though—it is a point that Mr Evans made earlier—that in running all these systems, we are building with what I think Kant called the crooked timber of humanity, and it is difficult to make things straight. When you really restrict access and train highly, you can get to the point where you have a degree of confidence about the ability to really control information. It is almost more about the human culture than the network systems.

Mr Bacon: It is nice to finish on Immanuel Kant.

Paddy McGuinness: I thought you would like that.

Chair: Mr Bacon has published a book and is therefore very into paper-based things.

Q130 **Philip Boswell:** Further to Mr Bacon's interesting point, given that there is no minimum standard, or no intention to mandatorily implement one, looking back at figure 6 on page 22 as an indication of the levels of engagement by the various Departments, how keen are those Departments that seem to be less engaged in compliance awareness—that is most Departments, according to figure 6—to take your advice to raise standards and standardise?

Paddy McGuinness: My sense is that they are keen to do it. We have in the recent past brigaded them to engage them at various levels. Mr Aung does it all the time. We have done it from permanent secretary down. We have interacted with their boards, I think. There is a significant change in the attitude of Departments to this responsibility.

Q131 **Philip Boswell:** Is it a significant change? Let us go back to where Mr Bacon was previously: item 3.28 on page 36. It is the last sentence

specifically, but I will go through 3.28 anyway: "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." That is one thing: it is optional for Departments. Secondly, "Organisations with the weakest information assurance procedures are, in its view"—this is according to the NAO Report—"less receptive to suggested improvements." Has something changed? If it is an opt-in/out, how can you standardise across Departments that are allowed to choose how much or little they engage?

Ben Aung: It does not necessarily hold that the National Archives' experience of its engagement with those Departments is the same as our engagement with those Departments. When I look down the list of organisations in figure 6 on page 22, I see a high degree of engagement from all those organisations. It is different, because they have different capabilities, wants and needs. The National Archives was offering an optional training package, which the numbers attest was taken up heavily over the lifespan of the programme. All those Departments will have been trained by the National Archives in one form or another. I am sure that at one point, all the SIROs from those organisations were trained by the National Archives. Some of those organisations are very capable and have little need to look outside their own perimeter for advice and can get it on tap from GCHQ if they need to, given the prominence of the work. The experience of the National Archives does not necessarily correspond to the experience that we would have or speak to the engagement of those Departments in security generally.

Q132 **Philip Boswell:** What about the rest of the Departments? It seems that the majority are not engaging, so how do you standardise, and what have you done to change their tune? Have they changed their tune? Are they compliant? It says here that they have not been, but now you say they are.

Ben Aung: The National Archives experience is that they have not been as engaged, or consistently engaged. As I said, our experience in the Cabinet Office is different. There is always a balance that we have to strike with standardisation, because if we land a central policy or rule badly with a Department and it does not feel like it corresponds to their business or the threats or risks that they face, there is a risk that they will be disengaged by it. We have got much better at it and we are much more consultative. There all sorts of forums where we join these organisations up with one another and ourselves. I disagree: I think they are all equally engaged, but in different ways, and not necessarily with the National Archives or any other body.

Q133 **Chair:** I just want to mop up a few quick points. In paragraph 3.12 on page 33, the NAO reports that there is quite a lot of confusion. This goes back to the point that Mr Evans raised about the different guidance coming out of the Government. Mr Aung, I guess this falls to you. It seems like you have gone from the alphabet soup to a central cyber-

security body, but you have still got a lot of guidance out there if you are a lowly civil servant just trying to do your best to protect data from data breaches. Have you got any plans to simplify that guidance and make it easier for people to find out what they need to do, how they need to do it and when by, and will you do that quickly?

Ben Aung: Absolutely. This Report recognises the proliferation of guidance. As a centre, we have tried to account for every risk and every new technology that has come along, and we are now in a period of consolidation, clean-up and streamlining. The National Cyber Security Centre has got a new website, where they have got a brand new taxonomy for their guidance. It is much more straightforward to find. We will mirror that with our central policy so they mesh in with one another.

Q134 **Chair:** So effectively it will be a website or something on the internet.

Ben Aung: We reach the biggest audiences via gov.uk, the NCSC website and CPNI's website.

Q135 **Chair:** We haven't touched so far on local government. With all the interconnection between different public bodies, there is a lot of information flowing between health and local government, and between local government and national Government. Who has responsibility for making sure local government is complying with the standards and guidance you issue? Who is going to jump in on that?

Ben Aung: My team doesn't have a mandate over local government or the wider public sector. Ours is over central Government and their agencies.

Q136 **Chair:** Even with the interfaces?

Ben Aung: For industry or the wider public sector, where central Government information is being held by other parties, we expect it to be handled in accordance with our rules and regulations and the standards we set. That is for Departments to enforce.

Q137 **Chair:** So they have to do an audit to ensure that is happening.

Ben Aung: Yes.

Q138 **Chair:** Do you do an audit of their audit, so to speak, so you can check it?

Ben Aung: Yes, we do.

Q139 **Chair:** Have you got any concerns about how local government or other third parties are doing things? Are there any areas of risk in that sector?

Ben Aung: The supply chain, whether it is a wider public-sector supply chain or industry, is an exceptionally challenging prospect for us in the centre, because it stretches out so far. Yes, I have concerns about both the ability of those organisations to meet our standards and the ability of Departments to assess and evaluate whether those standards are being met, discriminate between different parties and know when they should apply a particular mandation. It is a very varied picture.

At the National Cyber Security Centre, as we move to more commodity IT and more of a commercial best-practice model—we are not so bespoke and different in central Government—if a local authority were to use the Google cloud or the Microsoft cloud because it is the most cost-effective option for them, we know that that has the security we expect baked into it when they buy it off the shelf. We do not expect them to buy the very expensive bespoke system that central Government might have bought a few years ago. That is our route to market.

Paddy McGuinness: The strapline for that in the national cyber-security strategy is "secure by default". In other words, rather than relying on individual network owners to do all they need to do to make their networks secure, you get the providers to provide something. You raise the standard of what is delivered to them to the point at which you have a degree of confidence.

Q140 **Chair:** That's on the cyber side, but there is also the human side, which we have heard about.

Paddy McGuinness: The human side is obviously the larger cultural challenge that we've discussed.

Q141 **Chair:** Have you done a risk-based assessment of where the biggest risks lie, both in protecting information generally and in the cyber-sphere?

Paddy McGuinness: What we have done in three different ways is to press those responsible for the data in a Government Department—and, if it is a lead Government Department, those responsible for the Government's interaction with a sector of critical national infrastructure—to do the work to determine an order of priority for what matters to them most. One of the critical things one needs to do to create the right kind of protection is to understand which data sets or systems are absolutely critical and need the most protection.

Chair: So they do that, and then do you amalgamate it?

Paddy McGuinness: To amalgamate it, because it comes in various ways, would be quite complex.

Q142 **Chair:** Let's dream up an unusual scenario. The new Prime Minister came into office a few months ago. If I had been her and asked you, "What's the biggest risk to the UK in your area, Mr McGuiness?", what would you have said?

Paddy McGuinness: In terms of cyber?

Q143 **Chair:** Both. Information generally and cyber.

Paddy McGuinness: My area covers everything from space weather to a marauding terrorist firearms attack. I have quite a range to choose from. I think I would say to her that, almost not a risk but an issue, is natural hazard because, while we have some success through suppressive action at addressing terrorism, for instance, or cyber threats, natural hazards, if you look, just happen every 18 months, but that may be a facetious answer.

Q144 **Chair:** On the cyber side?

Paddy McGuinness: On the cyber side, I wouldn't have been able to give her a single asset that was saying our biggest risk is this here. There is a system problem. If one were briefing on defence capabilities, we would say, "The last thing you want to have compromised is this one", and then you would work your way out. That is certainly true sector by sector, but I don't think I could have said—

Q145 **Chair:** So who does have a risk register of what could go wrong. Is there someone in Government who is absolutely sighted on the risk, or are you just leaving it to every Department?

Paddy McGuinness: To amalgamate it and for it to be meaningful is really problematic across all the Government do. What we need is for us to have confidence in the individual Departments' understanding of their risk and the individual Secretaries of State understanding their risk. They are accountable to Parliament, but also they are delivering the business.

Q146 **Chair:** Part of the reason I am asking about the risk register is also about the data the NAO highlighted in paragraph 3.14 and following: some of the issues around you not having a great handle on the amount of money being spent, the number of staff and so on. If you don't have a risk-based assessment any Department could bid in to the spending review saying, "If you don't give us money, Sellafield will blow up"; "If you don't give us money, we'll have a breach in terrorism here"; "If you don't give us money we won't have a warship for self-defence"; or whatever. If you don't know about the money and the people, how do you know the risk?

Paddy McGuinness: May I segment risk and money? On risk, we have a national risk register and a national risk assessment that is the basis of planning. That is just reaching a conclusion. We are about to go out to response planners with a national risk assessment. Subject to ministerial agreement—I am reasonably confident that this will be true—we will publish the national risk register, which leaves this out. This gives a little more detail from the tiered risks you described from the national security strategy. So in that sense, we have a risk mechanism—absolutely, we do—but what we do not have is a centralised register of cyber risk, because to do that meaningfully is problematic. We could talk about intrusion capability at very high classification—that might be something we would do—but I don't think so. So there is cyber risk inherent in the national risk register and in the national risk assessment, and that runs through, but there is not a single risk register on a page that I can show you today.

On the question of money applied for security, in particular, I think it is important to recognise that in the way in which we talked about this when we were interviewed by NAO colleagues, we had to reflect that—Mr Aung has touched on this as we have gone along today—picking out which spend has a security effect from a composite spend on a network system is a very difficult thing to do and highly unscientific. You design your architecture and you build in security—I suppose a certain amount of your spend is for it to be secure when you set it up—but you are buying architecture that delivers a service, and you are paying for that.

Chair: You say that, but if you are buying architecture—there are certain things like some of the security stuff around counter-terrorism—there would be a particular level of security compared with much more minor information in a Government Department. So it is not the same level of security you need in every system. There will be differences of expenditure, surely, and you can extrapolate from that some approximation at least—we never, as a Committee, want people to go and do a huge bureaucratic exercise, but there must be some method of getting an approximation of whether Departments like the DWP and HMRC, which are equivalent in terms of some of the data they handle, are spending the same amount. Maybe one is spending less and getting more bang for their buck. Maybe another is spending more but quite rightly doing so, and another is lagging behind. Do you have any idea?

Paddy McGuinness: I don't.

Ben Aung: We do. The difference of experience that Departments have from maybe the NAO—we often get told we ask too many questions too frequently of Departments about what they are doing, how they are spending their money and what risks they have. Even though HMRC and DWP have very comparable businesses in many ways, building and securing universal credit over the last few years and securing a decades-old VAT mainframe system are fundamentally different and will have very different spend profiles and requirements.

We do know broadly what Departments spend that is over and above the composite spend that Paddy mentioned, but the utility of it in terms of informing our policy making, rules and regulations and strategies is limited. We know where Departments are feeling their keenest risks around protection of aggregate or bulk data, particularly when they are connected to online systems, the ability to monitor their networks successfully or properly and skills. We are constantly hearing and responding to those at a working level, and our policy, spend and resourcing correspond with those.

Q147 **Chair:** The Chancellor is going to make the autumn statement shortly. Every year there is the Budget. He will be being lobbied by every Department, possibly on this issue, and if he comes to you and says, "This Department's bidding for this much to make their systems secure, and that Department's bidding for that much. Do I believe these figures?" you could not give him any advice. Is that what you are saying?

Ben Aung: No, we absolutely could, but that would be a case-by-case decision that we would respond to, rather than, "Does HMRC need to spend as much as DWP?" It would depend on what they are both doing and what security outcomes they must achieve.

Chair: Okay. I will ask the Comptroller and Auditor General to chip in on this point.

Sir Amyas Morse: I am struck, as I listen to you, by a theme of not being very keen to push things at people. I detect a quite pervasive

philosophy in a lot of your answers—I am not saying that it's bad; I am just making sure I have understood it. You think that's better. I also detect a tendency to think that things cannot be evaluated or terribly readily prioritised based on number-type information. I was interested in one of your answers, Mr Aung. You said that Departments tend to tell you you're asking too many questions. All of this has a slightly voluntary feel. For something of this seriousness, it sounds a bit like you are on sufferance. Is that really what it feels like? Is this really okay? You are telling us this is all great—jolly good, chaps—but I am slightly uneasy about it. This was classified as a tier 1 threat, whether with any information or on any real basis, and you are operating on a fairly voluntary and not particularly pressing approach. I may have just picked that mood up wrong, but it sounds a little bit like that.

Paddy McGuinness: I think you have picked the mood up wrong, if you are talking about the tier 1 side of it. You are conflating a set of things. It is absolutely the case that we are not trying to drive information technology decisions and data-holding decisions of themselves from the centre. We are trying to provide a framework within which they can deliver. That is because it would not work, we would fall over and I would be in here all the time.

Chair: I think we've got that point.

Paddy McGuinness: But also because we get a tremendous return from Departments—this is part of the Government Digital Service revolution, in terms of the approach of Government—riding the new technologies and the relationship with the companies and realising what can be realised for their business delivery as opposed to designing bespoke Government systems to do so. We get a tremendous return from that. There is a thing about the limits of what we want to do centrally, first. In terms of the tiered risks, the reason why cyber was a tier 1 risk is that—not at this classification—we have multiple examples of action by states and by criminal groups that could have pernicious effect; and actually when we briefed Ministers originally in 2010, prior to the drawing up of the 2011 strategy—which Mr Evans has quoted from quite extensively—we talked about a set of risks. What we found over the life of that five-year programme on the back of that strategy was that those risks eventuated, and things that we had said, "Oh, this might happen"—they happened.

That is even more true in the last 12 months. One can point at a number of cyber events in the United Kingdom—but elsewhere, as well, in the media—and you can see the extent. So I do not think we have a difficulty categorising risk. What is difficult is to come up with a macro picture of what spend has what effect where, because of the complexity of Government business. It is not useful for us, as I think Mr Aung has said, to try and bring this together to the point where we have a kind of wonderful central view where we have clarity. It has to be done system by system and Department by Department. We absolutely can support the Chancellor as he makes his judgments. If he asks me about the sectors for

which I am responsible I absolutely can take him through the judgments that might be made around elements of spending on systems.

Sir Amyas Morse: And yet you said to us—or another part of your evidence was—that you do not insist on mandatory reporting of breaches. So that is not a question of philosophy or mandating systems from the centre. That is quite basic stuff you are not asking for.

Paddy McGuinness: We are asking to know about breaches. What we are not doing is mandating it in the way that some people might think because—

Sir Amyas Morse: Or nothing else very much—or not much.

Paddy McGuinness: No, I am not sure that is right. We are requiring a great deal from Departments to tell us about what happens on their systems. Absolutely we are, and we are in constant dialogue with them.

Q148 **Mr Bacon:** Apart from training, certification, regulation and reporting anything.

Paddy McGuinness: We do have a model for doing that through these security clusters.

Q149 **Mr Bacon:** We will probably have you back at some point to see how it is going.

Paddy McGuinness: I look forward to it.

Q150 **Mr Bacon:** Are you aware, by the way, that the NHS today inadvertently launched a denial of service attack on itself, after a—let me get this right—senior ICT delivery facilitator in Croydon accidentally added everyone to a mailing list and sent them a test email. The NHS has admitted today that as many as 840,000 staff were subsequently locked out of NHS mail, the organisation's in-house email service. As you said, there is nothing you can do to cope with the crooked timber of humanity, I suppose. Are you responsible—you mentioned you have a very broad remit: do you cover the NHS as well?

Paddy McGuinness: Only for the contribution that the national cyber security programme can make to its wellbeing, and the contribution that it makes in our preparedness for dealing with natural hazards and threats.

Q151 **Mr Bacon:** So not medical records?

Paddy McGuinness: No, I can't help with medical records.

Q152 **Mr Bacon:** They could be traded in the secondary market quite happily, and you would know nothing about it.

Paddy McGuinness: I may not know about it; I would hope someone would, and I would certainly pay for someone to know about it with money that was put in my possession, if it were. But, if I may, I think you have hit on a really important point—that we have a tendency, there is a risk, in

particular when talking about cyber-security, or generally about security, to start at the hardest end. We tend to talk about state intrusions, or—

Chair: Well actually, to be fair, we haven't today. We have a lot on human error, patient records, citizen information.

Paddy McGuinness: Absolutely, and I think that is the critical message in terms of our national standards and preparedness—that quite a lot of the public discourse is about the much more sophisticated end, of which there is little. An effort to raise, relatively simply, information assurance standards, patching and the rest, at quite a low level, would materially improve the experience of the citizen, whether it be from Government or from the—

Q153 **Chair:** I am aware that we are now at quarter past 6, which is longer than we intended to carry on, but can I just ask, for clarity, to both of you, actually, just to be clear about your reporting line. So, Mr McGuinness, who do you report in to—senior officials, and which Minister, ultimately?

Paddy McGuinness: Certainly. It depends on the subject area, but broadly speaking I advise the Prime Minister as the Chair of the National Security Council. My line manager is the National Security Adviser. His line manager, I suppose, is Sir Jeremy Heywood. So I am accountable for a whole set of things to the Prime Minister. In the field of security, the Minister for cyber-security is Mr Gummer, and I am accountable to him. Certainly the national cyber-security programme goes on that route.

Q154 **Chair:** I just wanted to be clear. I knew that you had slightly unusual reporting. Straight to the Prime Minister is quite unusual, so it is always good to get it on the record. Mr Aung?

Ben Aung: I report to the Government's chief security officer, who is the director of the Cyber and Government Security Directorate in the Cabinet Office. I head up the Government security team in that directorate, and he reports to Paddy.

Q155 **Chair:** How long have you been in post in your job?

Ben Aung: I have been in my job for just over a year. I have been in the team for three years before that and I have been in Government cyber-security for 10 years.

Q156 **Chair:** So there is a career path in Government cyber-security.

Ben Aung: Yes. I am living it.

Q157 **Chair:** It's not like you just pitch in having dealt with policy in another area.

Ben Aung: No. I have a technical background.

Q158 **Chair:** And that is expected in your role.

Ben Aung: At the moment, I think it would be.

Chair: I would hope so.

Ben Aung: In previous years my role has had more of a policy focus. Given all the things that we have talked about today, it would not be tenable not to have a technical background.

Mr Bacon: Would that more people said that about other areas of Government.

Chair: Thank you very much for your patience and time today. An uncorrected transcript of the sitting will be up on the website in the next couple of days. If you have any corrections, let us know. We cannot be sure that the report will be out before Christmas. It may just be on the cusp of recess. We look forward to getting responses on the things we mentioned, and we will send you a letter about that.