House of Commons

Culture, Media and Sport Committee

Cyber Security: Protection of Personal Data Online

First Report of Session 2016–17

HC 148

House of Commons

Culture, Media and Sport Committee

Cyber Security: Protection of Personal Data Online

First Report of Session 2016–17

Report, together with formal minutes relating to the report

Ordered by the House of Commons to be printed 15 June 2016

HC 148
Incorporating HC 587, session 2015-16
Published on 20 June 2016
by authority of the House of Commons

The Culture, Media and Sport Committee

The Culture, Media and Sport Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Department for Culture, Media and Sport and its associated public bodies.

Current membership

Jesse Norman MP (*Conservative, Hereford and South Herefordshire*) (Chair)

Nigel Adams MP (*Conservative, Selby and Ainsty*)

Andrew Bingham MP (*Conservative, High Peak*)

Damian Collins MP (*Conservative, Folkestone and Hythe*)

Julie Elliott MP (*Labour, Sunderland Central*)

Paul Farrelly MP (*Labour, Newcastle-under-Lyme*)

Nigel Huddleston MP (*Conservative, Mid Worcestershire*)

Ian C. Lucas MP (*Labour, Wrexham*)

Christian Matheson MP (*Labour, City of Chester*)

Jason McCartney MP (*Conservative, Colne Valley*)

John Nicolson MP (*Scottish National Party, East Dunbartonshire*)

The following Member was also a member of the Committee during the Parliament:

Steve Rotheram MP (*Labour, Liverpool, Walton*)

Powers

The committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/cmscom 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 Elizabeth Flood (Clerk), Katy Reid (Second Clerk), Kevin Candy (Inquiry Manager), Johnnet Hamilton, (Inquiry Manager), Hannah Wentworth (Senior Committee Assistant), Keely Bishop (Committee Assistant) and Jessica Bridges-Palmer (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Culture, Media and Sport Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 6188; the Committee's email address is cmscom@parliament.uk

Contents

Introduction

1. On Wednesday 21 October 2015, there was a cyber-attack on telecommunications and internet provider TalkTalk, which resulted in the company taking down its consumer website the same day.[1] On Thursday 22 October, TalkTalk began notifying customers and the CEO, Dido Harding began a number of press interviews, in order to tell customers about the attack as quickly as possible.[2] On Friday 23 October, TalkTalk said that the "significant and sustained cyberattack" was under investigation by the Metropolitan Police Cyber Crime Unit (because there had been a cyber-ransom demand) and that there was a chance that customer names, addresses, dates of birth, phone numbers, email addresses, TalkTalk account information, credit card details and/or bank details had been compromised.

2. On Monday 26 October, the TalkTalk data breach was the subject of an Urgent Question in the House of Commons. The Chair of this Committee said that the Committee would be following developments related to the cyber-attack closely. Ed Vaizey, the Minister of State for Culture and the Digital Economy, welcomed our inquiry.

3. The inquiry was formally launched on Tuesday 3 November. We heard oral evidence from TalkTalk CEO, Dido Harding, on 15 December 2015, and from the Information Commissioner, Christopher Graham, on 27 January 2016. The inquiry received 32 written submissions.

4. We wish to express our thanks to those who gave oral evidence, to those who submitted written evidence and to our specialist advisor, Philip Virgo.

1 Dido Harding oral evidence Q104

2 TalkTalk supplementary evidence CYB0030 - section 2

1 Background

5. Although the TalkTalk cyber-attack in October 2015 was the trigger for this inquiry, it is essential to put this attack in context.[3] Cyber-crime is a significant and growing problem and affects all sectors with an on-line platform or service. As the British Business Federation Authority said in their evidence to the Committee:

> The TalkTalk incident is one of many that have happened and continue to happen. To consider it in isolation of others would be misleading. The overall context is complex and changing fast... The problem space is international.[4]

6. According to evidence submitted by the Federation of Small Businesses (FSB), a third of their members had been the subject of cyber-crime.[5] The FSB also cited the PricewaterhouseCoopers (PwC) 2015 Information Security Breaches Survey, conducted on behalf of the Department for Business, Innovation and Skills, which found that 90% of large organisations had experienced a security breach. The recently published Cyber Security Breaches Survey 2016 commissioned by the Department for Culture, Media and Sport (DCMS) found that 25% of companies experience a cyber-breach at least once a month.[6]

7. The Internet Telephony Services Providers' Association emphasised that data breaches are not unique to the telecommunications sector,[7] and indeed the latest research from the Information Commissioner's Office (ICO) shows that the health sector has the most data breaches, followed by local government.[8] Furthermore, it is also important to make clear that not all threats to cyber security or data protection are from external actors. Research from Intel showed that 43% were caused by internal actors (employees, contractors and third party suppliers) and half of these were accidental.[9]

8. Companies and organisations are responding to the cyber-threat in different ways. The 2015 PwC Information Security Breaches survey found that 49% of companies are accredited to the Government's Cyber Essentials and Cyber Essentials Plus scheme, or are on their way to accreditation.[10] The 2016 Cyber Breaches Survey found that 51% of companies had completed five or more of the Government's Ten steps to Cyber Security.[11] In evidence, Dido Harding underlined that TalkTalk used the 'Ten Steps to Cyber Security' and was going through the accreditation process to the Cyber Essentials programme.[12]

9. It is also essential to put this attack in the context of the regulatory framework. As the end result of the TalkTalk cyber-attack was a personal data breach, the lead regulator here is the Information Commissioner's Office (ICO), which is responsible for compliance

3 TechUK CYB0024 Introduction
4 BBFA CYB0005 - overall comment
5 FSB CYB0004
6 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf
7 ITSPA CYB0018 - Introduction
8 https://ico.org.uk/action-weve-taken/data-security-incident-trends/
9 Intel Security CYB0020 - paragraph 12
10 http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-digital.pdf
11 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf
12 Dido Harding oral evidence Q77

with data protection law.[13] As the regulator for electronic communications networks and services, however, Ofcom was also involved. In the year to March 2015, the ICO received 14,368 "concerns" under the Data Protection Act and around 180,000 under the Privacy and Electronic Communications Regime.[14] In the same period the ICO received 285 reports from communications service providers, who are required to notify the ICO of any security breach within 24 hours, under the Privacy and Electronic Communications Regulations (PECR). The ICO's enforcement section of 30 staff are dealing with approximately 1,000 cases at any given time.

10. The ICO conducted an audit of TalkTalk in September 2014, which resulted in a number of suggestions but did not give the ICO any reason to put TalkTalk on a 'watch list'.[15] In written supplementary evidence, TalkTalk stated that they had reported 14 data breaches to the ICO over the previous two years, including two separate internal data breaches involving third party suppliers in September 2014 and December 2015.[16]

13 Ofcom written evidence CYB0029 paragraph 3.2
14 https://ico.org.uk/media/about-the-ico/documents/1431982/annual-report-2014-15.pdf
15 ICO oral evidence Q169
16 Talk Talk supplementary evidence CYB0031 - paragraph 1

2 TalkTalk cyber-attack and response

11. The ICO has yet to produce a final verdict on the TalkTalk cyber-attack and data breaches. **We await the outcome of the ICO investigation into the TalkTalk cyber-attack and data breach, and note the comment from the ICO that the time taken for the investigation is partly due to the international dimension to the investigation.**[17] **We accept this, but regret that, some eight months after the breach, customers are no closer to a clear understanding of what happened. Although the Information Commissioner did not complain about lack of capacity, it seems evident that 30 enforcement staff are not enough to handle 1,000 cases and almost 200,000 public concerns a year, even if the vast majority of cases are found not to warrant detailed investigation. We suggest that the new Information Commissioner make an assessment of resources and priorities as soon as possible.**

12. We note that an unusual feature of the TalkTalk cyber-attack was that the Board took a decision to go public within a day of the attack, knowing that it would take at least several days (in fact it took two weeks) to work out how many customers were affected.[18] TalkTalk also commissioned PWC to review TalkTalk's systems as part of their follow-up into the cyber-attack. Although final judgement as to how the breach occurred must await this report, we recognise the strong crisis management response by TalkTalk and the prompt response and leadership shown by Dido Harding. **However, it is important that TalkTalk publish as much of the PWC investigation as commercially possible without delay, and set out how they will implement any necessary changes.**

13. We received evidence from a number of individuals who had suffered financial losses after scam calls following the data breaches at third party suppliers to TalkTalk[19] and also from individuals suffering from nuisance calls after third party data breaches.[20] We did not receive any evidence of financial loss directly attributed to the cyber-attack itself. In oral evidence, Dido Harding underlined that TalkTalk had regularly written to customers in the 12 months preceding the cyber-attack informing them what information customer service agents would and would not seek if calling on behalf of the company[21]. Following the cyber-attack, TalkTalk also contacted banks to monitor customer accounts and provided advice to consumer groups like Which? and Citizens Advice Bureau[22]. Financial Fraud Action UK told us that

> As fraudsters increasingly concentrate their attacks on customers, a major part of the response must be through awareness-raising about how customers can identify fraudulent approaches and protect themselves….FFA UK is calling for a landmark public awareness campaign to achieve a genuine step change in prevention.[23]

14. We believe it is essential to increase customer awareness of on-line and telephone fraud and scams, but consumers also have a responsibility to protect themselves on line. **There needs to be a step change in consumer awareness of on-line and telephone**

17 ICO oral evidence Q151
18 Dido Harding oral evidence Q104
19 CYB0007, CYB0008
20 CYB0032
21 Dido Harding oral evidence Q22
22 Talk Talk supplementary evidence CYB0030 paragraph 2.6
23 CYB0028

scams. The Government should initiate a public awareness-raising campaign, on a par with its campaign to promote smoke alarm testing. All relevant companies should provide well-publicised guidance to existing and new customers on how they will contact customers and how to make contact to verify that communications from the company are genuine. This verification mechanism should be clearly signposted and readily accessible, as with existing customer contact and complaints mechanisms. The Information Commissioner should check that data controllers have put easy-to-use verification guidance and measures in place. We think that these recommendations should apply not only to the telecommunications sector but also more widely to all who hold customer personal data.

15. The inquiry also considered how the TalkTalk Board members took responsibility for cyber security and data breaches. During oral evidence, Dido Harding confirmed that she saw herself as "accountable and responsible"[24] for security within the company, and in further probing, she elaborated that

> line responsibility for keeping our customers' data safe is split across a number of teams, so the accountability for security policies, the accountability for security audit, the accountability for security best practice, knowledge and dissemination within the organisation sits with the security function. The implementation of systems and processes that comply with those policies sits with my technology function. The implementation of the human elements of security—safe passwords, usage, complying with call centre policies—sits within my operations function. So it is impossible in a telecoms company to say that security only sits with the director of security. [25]

16. Although ultimate responsibility for cyber security within a company lies with the CEO, it would be highly unusual for the CEO of a company to have to resign over an attack, and it is important that this is not used as a means to diffuse or avoid responsibility elsewhere. The day to day responsibility in any company should therefore be clearly allocated to a specific person, for example, the Chief Information Officer or the Head of Security. **It is appropriate for the CEO to lead a crisis response, should a major attack arise. But cyber security should sit with someone able to take full day-to-day responsibility, with Board oversight, and who can be fully sanctioned if the company has not taken sufficient steps to protect itself from a cyber-attack. To ensure this issue receives sufficient CEO attention before a crisis strikes, a portion of CEO compensation should be linked to effective cyber security, in a way to be decided by the Board.**

17. We were keen to understand the level of technical sophistication behind the TalkTalk cyber-attack. Some commentators suggested that the cyber-attack was a product of SQL (Structured Query Language) attack.[26] We note that there had already been three occasions when the ICO had issued a fine following an SQL attack (the largest of which was £200,000)[27] and these cases should have served as a warning to others, including TalkTalk. According to written evidence from Infosec, SQL susceptibility is "one of the most prevalent vulnerabilities in web applications."[28] JISC (the higher education not-for-profit organisation for digital services and solutions) told us that

24 Dido Harding oral evidence Q1
25 Dido Harding oral evidence Q9
26 A SQL attack is a code injection technique which exploits a security vulnerability.
27 ICO oral evidence Q170
28 Infosec CYB0009 paragraph 1

> the vulnerabilities such as SQL injection most often exploited to create this kind of breach of customer data are not limited to telecoms and Internet service providers. Any organisation participating in e-commerce, in any industry, should be taking appropriate and continuing measures to ensure their systems are not vulnerable to similar attacks.[29]

18. It is no longer a defence, for a company using an e-commerce platform, to say that it was not aware of the risk of SQL injection based attacks, or similarly established and in some cases routine forms of cyber-penetration. **The ICO should introduce a series of escalating fines, based on the lack of attention to threats and vulnerabilities which have led to previous breaches. A data breach facilitated by a 'plain vanilla' SQL attack, for example, or continued vulnerabilities and repeated attacks, could thus trigger a significant fine. We were also surprised that there is no requirement to make security a major consideration in the design of new IT systems and apps. We therefore recommend that security by design should be a core principle for new system and apps development and a mandatory part of developer training, with existing development staff retrained as necessary.**

19. Given the prevalence of cyber-attacks, it is important that companies and entities do not just focus their efforts on trying to prevent such attacks, but they also prepare themselves for the eventuality. As Symantec said in written evidence,

> despite increased levels of investment, organisations should still expect to be attacked and sometimes breached, and they should be prepared to respond.[30]

The Institute of Chartered *Accountants* in England and Wales concurred, arguing that business needed to see security breaches as an inevitable part of being in the digital economy today.[31]

20. Although TalkTalk had run various business continuity exercises, including potential risks like cyber-breaches, TalkTalk had not exercised and planned on how to handle a cyber-attack on this scale.[32] In the 2016 Cyber Breach Survey for DCMS, it was striking that only 29% of companies had formal written cyber-security policies, and on average 10% of companies surveyed had a cyber-incident management plan, although 42% of large companies did have one. Other submissions stressed the importance of "*scenario-exercising to build organisational and national resilience*"[33] and BT saw testing and monitoring as an "*essential part*" of doing business in the digital economy.[34] In written evidence, TechUK emphasised the importance of managing communications with customers, pointing out that an email after a breach can give cyber-criminals "*an opportunity to spoof the affected company and dupe customers.*"[35] **In major organisations, where the risks of attack are significant, the person responsible for cyber-security should be fully supported in organising realistic incident management plans and exercises, including planned communications with customers and those who might be affected, whether or not there has an actual breach.**

29 JISC CYB0006 paragraph 5
30 Symantec CYB0025
31 ICAEW CYB0017
32 Dido Harding oral evidence Q75-76
33 Dr Mils Hills CYB0026 paragraph 6
34 BT CYB0015 section 2
35 TechUK CYB0024 section 1

21. We note the announcement by TalkTalk in March 2016, that it would introduce voice biometric passwords for customers to access their accounts, the first UK Internet Service Provider (ISP) to do so. We await the impact of this change with interest.

3 Consumer compensation and contracts

22. We received written evidence from TalkTalk customers who had been affected by data breaches, but not directly affected by the 2015 cyber-attack. One customer told us that it had taken TalkTalk over 100 days to inform customers about a third party data breach that occurred in 2014. This customer believes that the delay in informing customers left them vulnerable to scams and they suffered financially as a consequence.[36] In further written evidence, another TalkTalk customer complained that they had not been informed at all about a 2014 data breach and they subsequently lost money when scammers pretended to be from TalkTalk and claimed to be following up on a hack.[37]

23. We welcome Dido Harding's assurances that TalkTalk wishes to hear from any customer who has directly lost money as a direct consequence of the cyber-attack[38] and that any customer who suffered financial losses as a result of the cyber-attack would be able to terminate their contact early.[39] Mobile and telecoms contracts often do not make it clear if financial losses as a result of a data breach would be sufficient grounds to terminate a contract early; written evidence from consumers confirmed this.[40] **Telecoms companies should clarify this point in simple language for consumers, so that they can make an informed choice when choosing a service or product.**

24. We remain concerned that consumer redress following a data breach is still too difficult. At present an individual can claim for compensation for damages caused as a result of a breach only by going to court. As the Information Commissioner stated in oral evidence:

> I have responsibilities to deal with the company as a whole. What I cannot do is to act on behalf of individual constituents and award compensation. At the moment, that involves going to law and that will involve lawyers.[41]

25. Compensation for distress without evidence of financial loss under the Data Protection Act is currently one area under consideration by the Supreme Court, in the Google v Vidal Hall case. [42] **We believe it should be easier for consumers to claim compensation if they have been the victim of a data breach. There are a number of entities (for example the Citizens Advice Bureau, ICO and police victim support units) that could in principle provide further advice to consumers on seeking redress through the small claims process. It would be useful for the Law Society to provide guidance to its members on assisting individuals to seek compensation following a data breach. The ICO should assess if adequate redress is being provided by the small claims process.**

36 CYB0007
37 CYB0008
38 Dido Harding oral evidence Q40 and Q45
39 Dido Harding oral evidence Q49
40 CYB0010
41 ICO oral evidence Q179
42 https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/compensation/

4 Data protection in third party suppliers

26. In addition to the data breach that followed the cyber-attack, we are also concerned by the data breaches that affected third party suppliers to TalkTalk in September 2014 and December 2015.[43] Several of these cases were highlighted by the radio programme *Moneybox* in February 2016; scammers were able to access detailed customer records within 24 hours of an engineer's visit and use that information to persuade customers to grant access to their personal computers, leading to financial losses. Experiences like this are not limited to TalkTalk but have also affected banking and on-line retail customers.[44] In evidence, the Institute of Chartered Accountants in England and Wales argued that many businesses are struggling to get control of their supply chain, and get assurance from suppliers with the highest associated cyber risk.[45] We note that in the 2016 Cyber Security Breaches survey, only 34% of large companies set cyber-security standards for their suppliers. **All telecommunications companies and on-line retailers, and other cyber-vulnerable organisations, should take steps to ensure that compliance with data protection rules and Cyber Essentials are key criteria when selecting third party suppliers.**

43 Talk Talk CYB0031 paragraph 1
44 Tim Coote CYB0011 point 1
45 ICAEW CYB0017 point 5

5 Cyber Essentials and improving cyber-security

27. One of the key areas of the inquiry was to examine the adequacy of the supervisory, regulatory and enforcement regimes currently in place to ensure companies are responding sufficiently to cyber-crime. We received evidence from the DCMS which stated:

> The Cyber Essentials scheme sets out the technical controls organisations should have in place to demonstrate that they are following a basic level of "good practice" in terms of their cyber security. Once implemented, the scheme provides a base level of readiness for the organisation to defend itself from internet-based attacks. However the Government's expectation is that larger organisations and those that hold large amounts of data would need to undertake other measures above and beyond those included in the Cyber Essentials scheme. One such measure is the Ten Steps to Cyber Security, which is a more comprehensive piece of guidance that assists companies take the appropriate steps they need.[46]

28. Not all of our witnesses were convinced about the effectiveness of Cyber Essentials. The British Business Federation Authority (BBFA) highlighted divisions within the security community, stating

> All agree it sets a low bar; some believe it is better than nothing, but others believe that it provides a false sense of security. This issue would be ok if the UK Government were working with industry to develop cyber-security methodologies at higher levels of assurance, but it is not.[47]

29. In written evidence, the Federation of Small Business supported Cyber Essentials but voiced a number of concerns, particularly concerning "*how it establishes and implements security controls without first identifying the assets, vulnerabilities and risks an organisation faces…the human factor is also a major consideration.*"[48] Dido Harding told us that she was not sure if Cyber Essentials was a good enough benchmark[49]. In written evidence, TechUK highlighted that neither Cyber Essentials nor the 10 Steps make any reference to encryption, or the hashing and salting of passwords.[50] The Cyber Essentials scheme was established in 2014 and has not been updated since then to take account of emerging technology and new hacking approaches.

30. We note the evidence from Federation of Small Businesses and BBFA concerning the weaknesses of the Cyber Essentials scheme[51] and the comments from DCMS that other measures beyond Cyber Essentials would be expected for larger organisations. We support the aim of the UK Cyber Essentials scheme and we recognise that no certification can provide 100% guarantee to prevent cyber-attacks. We think that Cyber Essentials provides a good check list for small and medium sized firms but needs revision in light of the recent experience of cyber-attacks, particularly the probability that 90% of large

46 DCMS CYB0027 points 3-5
47 BBFA CYB0005
48 FSB CYB0004
49 Dido Harding oral evidence Q94
50 TechUK CYB0024 section 2. This means applying algorithms to passwords
51 CYB0004 and CYB0005

organisations will experience a cyber-attack and the growing problem of cyber-ransom demands. We note that *Get Safe On Line*, supported by the Government, includes guidance on developing business security and recovery plans, and that current advice is to update the business security plan within 6-12 months of the first test.[52] **Cyber Essentials should be regularly updated to take account of more recent attacks, including the need for security, incident management and recovery plans and processes for responding to cyber-ransom demands.**

52 https://www.getsafeonline.org/index.php/businesses/business-security-plan/

6 The tensions between informing the authorities, criminal investigation and informing those potentially affected

31. The ICO set out reporting requirements following data breaches in his supplementary written evidence. Under the Data Protection Act (DPA), there is no general obligation to report data breaches to the ICO, but the ICO would expect serious breaches to be reported. Under the Privacy and Electronic Communications Regulations 2003 (PECR), telecoms companies and ISPs must notify the ICO of personal data breaches, and in some cases, also inform individual users and subscribers.[53] Under the EU General Data Protection Regulation (EU GDPR), agreed in December 2015 and due to be implemented by 2018, the obligation to report and inform following a data breach will be widened. The European Commission said "*companies and organisations must notify the national supervisory authority [in the case of the UK, the ICO] of data breaches which put individuals at risk and communicate to the data subject all high risk breaches as soon as possible so that users can take appropriate measures.*"[54]

32. In the evidence given to the Committee, a clear tension emerged between the need to inform the police, who may wish to keep details about the attack restricted to allow criminal investigation, and the duty to inform those affected. We note the evidence given by TechUK cautioning that emailing consumers after a breach may expose them to tailored 'phishing' attempts.[55] As Dido Harding said, on the day following the initial cyber-attack

> The advice we received from the Metropolitan Police was not to tell our customers. I totally understand why the police wanted us to stay quiet, because they have a different objective. They want to catch the criminals. We had some constructive discussion with them … on how to marry the conflicting objectives of a company wanting to look after their customers and the police force rightly wanting to catch the criminals.[56]

33. We welcome the close collaboration that TalkTalk established with the Metropolitan Police immediately after the October 2015 cyber-attack.[57] We recognise that the TalkTalk Board decided to notify all customers potentially affected, and subsequently established that the number actually affected was much smaller. However, the tension between police investigation priorities and informing those affected may be further complicated by situations where it may take weeks or months from finding evidence of a possible breach (e.g. customers being contacted by fraudsters) to finding the source of the breach (in the organisation or its supply chain). **The ICO and Cyber Essentials should publish further guidance on informing the relevant authorities and include best-practice examples of how to inform in an appropriate way those affected, in order to strike the best possible balance between protecting information that is sensitive to police investigations, whilst recognising consumer/customer requirements to be made aware of a breach that may**

53 Information Commissioner CYB0016 paragraph 4-5
54 http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm
55 TechUK CYB0024 section 1
56 Dido Harding evidence Q105
57 Dido Harding oral evidence Q104

affect them. This is particularly relevant as the EU GDPR will extend the obligation to inform consumers to all companies and organisation, not just telecommunications companies and ISPs.

7 ICO powers and remit

34. The ICO has a number of tools and powers at its disposal to support data protection and enforce the laws and regulations that underpin it. Given the importance of the digital economy and the increasing amount of personal data held on line, as the ICO said in written evidence, cyber security is "integral" to the protection of personal data.[58] Apart from any tension between informing the authorities and informing those affected, there may also be an incentive to cover up cyber-attacks or data breaches, due to the potential damage to corporate reputation they may cause. **The ICO should introduce an incentive structure that inhibits delays, for example escalating fines for delays in reporting a breach. At present the ICO can only issue a fixed fine of £1,000 for failure to report a data breach. There should also be scope to levy higher fines if the organisation has not already provided guidance to all customers on how to verify communications.**

35. We note that the maximum fine that can be imposed by the ICO is currently £500,000, which may not be a significant deterrent for a large company. The forthcoming EU GDPR strengthens consumer rights and extends the requirement to report data breaches to all entities that handle personal data. All companies and organisations will be required to inform national data protection authorities within 72 hours of a breach, and if there is a high risk to individuals/consumers, those people must also be informed. The EU GDPR also significantly increases the fines available to the ICO, from £500,000 maximum at present to a maximum of 4% of global turnover or €20 million. In oral evidence, the Information Commissioner said:

> In the GDPR that is coming down the track, the potential fines are much bigger[59]….the figures are eye-watering and will make the big players sit up and take notice…a fine of £500,000 when deployed against a really big player, like Sony for example, does not amount to very much whereas a percentage of global turnover becomes very serious.[60]

36. The ICO has begun producing guidance to help UK data controllers to prepare for the Regulation's entry into force.[61] However, the attention of individuals within the organisation may be better engaged by the threat of a custodial sentence, rather than a fine for their employer. As the ICO said in his written evidence:

> At present there is no option for a court to impose a custodial sentence for someone who contravenes section 55 of the DPA. Previous parliamentary evidence which we have submitted has called for more effective deterrent sentences, including the threat of prison in the most serious cases, to be available to the courts to stop the unlawful use of personal information[62]

37. The Direct Marketing Association also agreed that the use of criminal sanctions would be a greater deterrent[63], as did Big Brother Watch.[64] **We concur with the ICO, that whilst the implementation of the EU GDPR will help focus attention on data protection,**

58 Information Commissioner CYB0016 paragraph 3
59 ICO oral evidence Q187
60 ICO oral evidence Q198
61 https://dpreformdotorgdotuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf
62 ICO written evidence paragraph 31
63 Direct Marketing Association CYB0019
64 Big Brother Watch CYB0014 section 3

it would be useful to have a full range of sanctions, including custodial sentences. We therefore support the ICO's call to bring into force Sections 77 and 78 of the Criminal Justice and Immigration Act 2008, which would allow a maximum custodial sentence of two years for those convicted of unlawfully obtaining and selling personal data.

38. The digital economy is an increasingly important part of the UK economy. The 2015 UK Digital Strategy said that the UK economy is boosted by around £145 billion a year from digital technology.[65] In written evidence, Fujitsu said that the UK has the largest internet economy in the G20.[66] However, as TechUK underlined, as the digital economy grows, the opportunity for cyber-crime increases, and the challenge to make the UK a safe place to do business becomes ever more important. TechUK estimates that cyber-crime costs the UK economy £34bn a year, having increased from £27bn in 2010.[67] The 'digital by default' agenda also means that public services are increasingly provided digitally, resulting in significant volumes of personal data being held on-line. Increased use of cloud computing also means that more personal data is held on line.[68] Given the importance of e-commerce to the British economy and the prevalence of e-services, coupled with the mounting threat of cyber-attacks, we consider that companies need to continually invest in cyber-defences and ensure that they are keeping ahead of criminals and hackers. NCC Group highlighted a widespread diversity in cyber awareness at Board level, expressed through a variable level of committed investment.[69] **Companies and other organisations need to demonstrate not just how much they are spending to improve their security but that they are spending it effectively. We therefore recommend that organisations holding large amounts of personal data (on staff, customers, patients, taxpayers etc.) should report annually to the ICO on:**

i) **Staff cyber-awareness training;**

ii) **When their security processes were last audited, by whom and to what standard(s);**

iii) **Whether they have an incident management plan in place and when it was last tested;**

iv) **What guidance and channels they provide to current and prospective customers and suppliers on how to check that communications from them are genuine;**

v) **The number of enquiries they process from customers to verify authenticity of communications;**

vi) **The number of attacks of which they are aware and whether any were successful (i.e. actual breaches).**

Such reporting should be designed to help ensure more proactive monitoring of security processes (both people and cyber) at Board level, rather than reporting breaches after they have happened. Those submitting reports should also be encouraged to include such data in their own annual accounts to help give confidence to customers, shareholders and suppliers that they take security seriously and have effective processes in place.

65 https://www.gov.uk/government/news/uk-digital-strategy-the-next-frontier-in-our-digital-revolution
66 Fujitsu CYB0003 objective 1
67 TechUK CYB0024 Introduction
68 Federation Against Software Theft CYB0023 section 2
69 NCC Group CYB0012

39. Consumers are increasingly concerned about data protection and cyber-security. In written evidence, the Institute of Customer Service said that 43% are concerned that cyber-attacks might compromise their personal information and financial loss is the principal concern.[70] Consumers need to be able to identify which suppliers and retailers are implementing effective data protection and security (personnel and cyber) defences. **There is an urgent need for a mechanism that is easily understood by consumers in order to maintain consumer confidence and inform consumer choices. We therefore support the ICO's plan to create a privacy seal, to be launched later this year, which would be awarded to entities which demonstrate good privacy practice and high data protection compliance standards. It would be useful if the privacy seal could also incorporate a traffic light system to help consumers understand which companies are compliant, which are making progress, and which have yet to take the issue seriously.**

40. At present, the ICO has limited powers of non-consensual audit. Such audits cannot provide complete assurance: as noted above, the ICO had undertaken a consensual audit of TalkTalk in September 2015. **Nevertheless, the ICO should have additional powers of non-consensual audit, notably for health, local government and potentially for other sectors.**

70 Institute of Customer Service CYB0013 section 1.1

8 Investigatory Powers Bill

41. During the oral evidence session, the ICO issued a stark warning about the Investigatory Powers Bill, currently before Parliament. The ICO said that it creates a "haystack of potential problems" given the huge pools of personal data that it would create and their vulnerability to attack and theft leading to personal data breaches[71]. We also received evidence from academics who agreed on this point.[72]**The vulnerability of additional pooled data is an important concern that needs to be addressed urgently by the Government**. Part of the response could be to require enhanced security requirements and background checks for those with access to large pools of personal data. Data controllers should seek to control and limit access to such pooled data.

71 ICO oral evidence Q282-3

72 Professor Paul Bradshaw, Birmingham City University CYB0022 points 19-20

Conclusions and recommendations

1. We await the outcome of the ICO investigation into the TalkTalk cyber-attack and data breach, and note the comment from the ICO that the time taken for the investigation is partly due to the international dimension to the investigation. We accept this, but regret that, some eight months after the breach, customers are no closer to a clear understanding of what happened. Although the Information Commissioner did not complain about lack of capacity, it seems evident that 30 enforcement staff are not enough to handle 1,000 cases and almost 200,000 public concerns a year, even if the vast majority of cases are found not to warrant detailed investigation. We suggest that the new Information Commissioner make an assessment of resources and priorities as soon as possible. (Paragraph 11)

2. However, it is important that TalkTalk publish as much of the PWC investigation as commercially possible without delay, and set out how they will implement any necessary changes. (Paragraph 12)

3. There needs to be a step change in consumer awareness of on-line and telephone scams. The Government should initiate a public awareness-raising campaign, on a par with its campaign to promote smoke alarm testing. All relevant companies should provide well-publicised guidance to existing and new customers on how they will contact customers and how to make contact to verify that communications from the company are genuine. This verification mechanism should be clearly signposted and readily accessible, as with existing customer contact and complaints mechanisms. (Paragraph 14)

4. It is appropriate for the CEO to lead a crisis response, should a major attack arise. But cyber security should sit with someone able to take full day-to-day responsibility, with Board oversight, and who can be fully sanctioned if the company has not taken sufficient steps to protect itself from a cyber-attack. To ensure this issue receives sufficient CEO attention before a crisis strikes, a portion of CEO compensation should be linked to effective cyber security, in a way to be decided by the Board. (Paragraph 16)

5. The ICO should introduce a series of escalating fines, based on the lack of attention to threats and vulnerabilities which have led to previous breaches. A data breach facilitated by a 'plain vanilla' SQL attack, for example, or continued vulnerabilities and repeated attacks, could thus trigger a significant fine. We were also surprised that there is no requirement to make security a major consideration in the design of new IT systems and apps. We therefore recommend that security by design should be a core principle for new system and apps development and a mandatory part of developer training, with existing development staff retrained as necessary. (Paragraph 18)

6. In major organisations, where the risks of attack are significant, the person responsible for cyber-security should be fully supported in organising realistic incident management plans and exercises, including planned communications with customers and those who might be affected, whether or not there has an actual breach. (Paragraph 20)

7. Telecoms companies should clarify this point in simple language for consumers, so that they can make an informed choice when choosing a service or product. (Paragraph 23)

8. We believe it should be easier for consumers to claim compensation if they have been the victim of a data breach. There are a number of entities (for example the Citizens Advice Bureau, ICO and police victim support units) that could in principle provide further advice to consumers on seeking redress through the small claims process. It would be useful for the Law Society to provide guidance to its members on assisting individuals to seek compensation following a data breach. The ICO should assess if adequate redress is being provided by the small claims process. (Paragraph 25)

9. All telecommunications companies and on-line retailers, and other cyber-vulnerable organisations, should take steps to ensure that compliance with data protection rules and Cyber Essentials are key criteria when selecting third party suppliers. (Paragraph 26)

10. Cyber Essentials should be regularly updated to take account of more recent attacks, including the need for security, incident management and recovery plans and processes for responding to cyber-ransom demands. (Paragraph 30)

11. The ICO and Cyber Essentials should publish further guidance on informing the relevant authorities and include best-practice examples of how to inform in an appropriate way those affected, in order to strike the best possible balance between protecting information that is sensitive to police investigations, whilst recognising consumer/customer requirements to be made aware of a breach that may affect them. This is particularly relevant as the EU GDPR will extend the obligation to inform consumers to all companies and organisation, not just telecommunications companies and ISPs. (Paragraph 33)

12. The ICO should introduce an incentive structure that inhibits delays, for example escalating fines for delays in reporting a breach. At present the ICO can only issue a fixed fine of £1,000 for failure to report a data breach. There should also be scope to levy higher fines if the organisation has not already provided guidance to all customers on how to verify communications. (Paragraph 34)

13. We concur with the ICO, that whilst the implementation of the EU GDPR will help focus attention on data protection, it would be useful to have a full range of sanctions, including custodial sentences. We therefore support the ICO's call to bring into force Sections 77 and 78 of the Criminal Justice and Immigration Act 2008, which would allow a maximum custodial sentence of two years for those convicted of unlawfully obtaining and selling personal data. (Paragraph 37)

14. Companies and other organisations need to demonstrate not just how much they are spending to improve their security but that they are spending it effectively. We therefore recommend that organisations holding large amounts of personal data (on staff, customers, patients, taxpayers etc.) should report annually to the ICO on: (i) Staff cyber-awareness training; (ii) When their security processes were last audited, by whom and to what standard(s); (iii) Whether they have an incident management plan in place and when it was last tested; (iv) What guidance and channels they provide to current and prospective customers and suppliers on how to check that

communications from them are genuine; (v) The number of enquiries they process from customers to verify authenticity of communications; (vi) The number of attacks of which they are aware and whether any were successful (i.e. actual breaches). Such reporting should be designed to help ensure more proactive monitoring of security processes (both people and cyber) at Board level, rather than reporting breaches after they have happened. Those submitting reports should also be encouraged to include such data in their own annual accounts to help give confidence to customers, shareholders and suppliers that they take security seriously and have effective processes in place. (Paragraph 38)

15. There is an urgent need for a mechanism that is easily understood by consumers in order to maintain consumer confidence and inform consumer choices. We therefore support the ICO's plan to create a privacy seal, to be launched later this year, which would be awarded to entities which demonstrate good privacy practice and high data protection compliance standards. It would be useful if the privacy seal could also incorporate a traffic light system to help consumers understand which companies are compliant, which are making progress, and which have yet to take the issue seriously. (Paragraph 39)

16. Nevertheless, the ICO should have additional powers of non-consensual audit, notably for health, local government and potentially for other sectors. (Paragraph 40)

17. The vulnerability of additional pooled data is an important concern that needs to be addressed urgently by the Government (Paragraph 41)

Formal Minutes

Wednesday 15 June 2016

Members present:

Jesse Norman, in the Chair

Nigel Adams	Nigel Huddleston
Andrew Bingham	Ian C. Lucas
Damian Collins	Chris Matheson
Paul Farrelly	

Draft Report (*Cyber Security: Protection of Personal Data Online*), proposed by the Chair, brought up and read.

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

Paragraphs 1 to 41 read and agreed to.

Resolved, That the Report be the First Report of the Committee to the House.

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

[Adjourned till Tuesday 28 June at 10.00 am

Witnesses

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

Tuesday 15 December 2015

Question number

Dido Harding, Chief Executive, TalkTalk — Q1-145

Wednesday 27 January 2016

Christopher Graham, Information Commissioner and **Dr Simon Rice**, Group Manager (Technology), Information Commissioner's Office — Q146-288

Published written evidence

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

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

1 BBFA Ltd (CYB0005)

2 Big Brother Watch (CYB0014)

3 British Standards Institution (CYB0021)

4 BT (CYB0015)

5 Department for Culture, Media and Sport (CYB0027)

6 Direct Marketing Association (CYB0019)

7 Dr Mils Hills (CYB0026)

8 Federation Against Software Theft (CYB0023)

9 Federation of Small Businesses (CYB0004)

10 Financial Fraud Action UK (CYB0028)

11 Fujitsu (CYB0003)

12 ICAEW (CYB0017)

13 Information Commissioner's Office (CYB0016)

14 Integrated Infosec (CYB0009)

15 Intel Security (CYB0020)

16 ITSPA (CYB0018)

17 James Johnson (CYB0032)

18 Jisc (CYB0006)

19 Mr Roger Webster (CYB0010)

20 Mr Tim Coote (CYB0011)

21 Mr David Westwood (CYB0007)

22 Mr Graeme Smith (CYB0008)

23 NCC Group plc (CYB0012)

24 Ofcom (CYB0029)

25 Professor Paul Bradshaw (CYB0022)

26 Symantec (CYB0025)

27 TalkTalk (CYB0030), (CYB0031)

28 TechUK (CYB0024)

29 The Institute of Customer Service (CYB0013)

List of Reports from the Committee during the current Parliament

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 2015–16

First Special Report	Tourism: Government response to the Committee's Sixth Report of Session 2014-15	HC 382
Second Special Report	Society Lotteries: Government response to the Committee's Fifth Report of Session 2014-15	HC 415
First Report	BBC Charter Review	HC 398
Second Report	Appointment of the Information Commissioner	HC 990