Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's response to the Culture, Media and Sport Committee's inquiry into Cyber security: protection of personal data online

1. The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations 2003, as amended (PECR). The Information Commissioner also has a more limited supervisory role under the Data Retention Regulations 2014 (DRR) created under the Data Retention and Investigatory Powers Act 2014 (DRIPA).

2. The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

Introduction

3. The Information Commissioner welcomes the opportunity to respond to this inquiry into cyber security following on from the recent Talk Talk incident. Cyber security is integral to the protection of personal data and his role encompasses oversight of security measures put in place by communication service providers (CSPs) in specific circumstances.

4. The DPA governs the processing of personal data by all organisations, and includes an obligation for those organisations to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (principle 7). This obligation applies to all organisations processing personal data and not just telecommunications and internet service providers. The Information Commissioner has the power to take enforcement action where this principle is contravened, including the power to issue monetary penalties of up to £500,000 for serious contraventions.

5. In addition, PECR require that providers of public electronic communications services (which would include telecommunications and internet service providers) take appropriate technical and organisational measures to safeguard the security of the service that they provide. PECR also require notification of personal data breaches both to ICO and, in some cases, to individual users/subscribers. Failure to meet these requirements can be met with enforcement action varying from a fixed monetary penalty of £1,000 for failure to report personal data breaches to a monetary penalty of up to £500,000 for more significant breaches.

6. The DRIPA and DRR impose duties on CSPs around the retention of communications data for third party investigatory purposes where they have been served with a notice by the Secretary of State. Under the DRR the Information Commissioner has a duty to audit the security, integrity and destruction of that retained data. A Retention of Communications Data Code of Practice issued under the Regulation of Investigatory Powers Act 2000 as amended by the DRR (the Retention Code) governs the arrangements relating to the retention of data by CSPs including arrangements to allow the Information Commissioner to undertake his audit duties.

Specific questions

The nature of the cyber-attacks on TalkTalk's website and TalkTalk's response to the latest incident

7. We are investigating the recent Talk Talk incident within our regulatory remit and it is not appropriate comment on what has occurred in that specific context whilst that investigation is still underway. We can however confirm that Talk Talk did submit a breach notification as required by PECR and we are in contact with them as part of investigating that breach.

8. We issued the following statement:

   "*The ICO is aware of this incident, which was reported to us on Thursday afternoon. We will be making enquiries and liaising with the Police.*

   "Any time personal data is lost there can be a risk of identity theft. There are measures you can take to guard against identity theft, for instance being vigilant around items on your credit card statements or checking your credit ratings. There are tips and information about identity theft available on our website. "

The robustness of measures that telecoms and internet service providers are putting in place to maintain the security of their customers' personal data and the level of investment being made to ensure their systems remain secure and anticipate future threats

9. The Information Commissioner was given the power to carry out audits of the security of personal data held within the networks of CSPs under regulation 5 of PECR in 2011. Since 2013 we have carried out consensual audits with all the major CSPs and have found all to provide some level of assurance, with the majority providing a reasonable level of assurance that security procedures are in place to protect the personal data held. It is our experience that CSPs do devote resources to the security of their systems and personal data, however we could not quantify the adequacy of that investment.

10. It is worth pointing out that even where assurance has been assessed as 'reasonable' or 'high', we have always been able to make recommendations for improvement. This can at least in part be attributed to the nature of the industry which is subject to ever-evolving threats.

11. The DRR further extended the audit role of the Commissioner in respect of some CSPs. Where CSPs are required by notice to retain certain communications data for investigatory purposes, the Commissioner has a role to audit the security, integrity and destruction of that specific data. Since being given this duty we have recruited and established a dedicated team with the necessary skills to undertake this work. We have already commenced initial desk based reviews under this power, and are about to begin a programme of site visits.

12. Regulation 7 of the DRR requires CSPs to hold data securely and specific security arrangements for the retention of data by CSPs are set out in chapter 6 of the Retention Code. This also provides for the Home Office to include specific security requirements in data retention notices and to provide security advice and guidance to all CSPs who are retaining data. The Retention Code envisages retained data being kept in a dedicated retention and disclosure system which is securely separated from a CSP's business system. However the Retention Code does recognise that it may not be practicable for all CSPs to do this and data may be retained in business or shared systems and that specific security safeguards will need to be agreed with the Home Office.

13. Whilst it may be possible to ensure that data retained in normal business systems does have the necessary safeguards in place to

ensure appropriate security, such systems, aimed as they are at facilitating wider business use, may pose more of a challenge not only for CSPs to secure but also for the Information Commissioner to audit.

The nature, role and importance of encryption in protecting personal data

14. Encryption is a vital cybersecurity tool for protecting personal data but it is one which cannot be relied on to the exclusion of other security measures. The Information Commissioner has, for a number of years, strongly recommended the use of encryption as a security measure to protect personal data, particularly in the event of loss or theft of a physical device. The Information Commissioner is producing guidance about the use of encryption for organisations, which will be available in early 2016.

15. Strong encryption, properly configured and used, is an effective security measure which guards against unauthorised access to data in many scenarios but must not be regarded as a perfect solution as it can only provide effective protection against a specific set of security risks. Encryption can be used for storing data at rest or when it is in transit across a network. However encrypted data eventually needs to be decrypted in order to make use of it, even though this may only be done temporarily. Hence any potential attacker is likely to try and target the data in its decrypted form if possible.

16. The existence of security vulnerabilities which allow attackers to gain unauthorised access to this decrypted data illustrates the importance of not relying solely on encryption as a defensive measure. Vulnerabilities can arise when the data is at rest or in transit.

17. A good example is SQL injection: SQL is a computer language commonly used to interact with databases. It is common for applications, such as modern websites, to make use of SQL to interact with a database. Where such an application has been poorly coded, instructions written in SQL can be passed directly to the database. This means that an attacker can easily read, modify or delete data irrespective of any encryption in use. In some cases automated tools can be used to scan a website searching for such vulnerabilities. SQL injection is made possible because by design, an application such as a website has already been granted access to the database and the attacker has hijacked this authorised access to the underlying data. If data were to be stored in an encrypted form and be decrypted in response to a request from the web application it would similarly be returned to an attacker in a decrypted form.

18. Similarly, encryption of data in transit is vital in many cases, yet this encryption must be combined with further security measures. For example, a customer connecting to an internet banking service would typically use an encrypted HTTPS connection to protect their financial data whilst it is sent between the server and web browser. An attacker attempting to obtain this customer's financial data would typically avoid trying to compromise the encryption itself, and instead attempt to compromise the endpoint (the device which the customer is using such as a desktop computer, laptop or mobile device) using malware such as a keystroke logger. If the endpoint is not secured using further security measures, the attacker might be able to compromise it and gain access to the financial data while it is being processed in its decrypted form.

19. The need for good key management should also not be underestimated. Should an attacker be able to gain access to the encrypted data and the decryption key then the high level of protection that encryption could offer is no more than an illusion.

20. A simple example would be the loss or theft of an encrypted laptop. Provided that the laptop was switched off and access credentials remain secret there is a strong likelihood that an attacker could not gain access to any personal data stored on the disk. However if that same laptop was left unattended whilst the user was logged in or the device was infected by malware the personal data stored on that device could be subject to unauthorised access.

21. Encryption can play a role in protecting data in a wide variety of circumstances – and there are plenty of effective encryption methods readily available. The best methods are those that are openly published and have been widely tested by cryptographic experts.

The adequacy of the supervisory, regulatory and enforcement regimes currently in place to ensure companies are responding sufficiently to cyber-crime

22. As set out in the introductory paragraphs above, there are legally enforceable security requirements on all those who process personal data with additional requirements, such as around security breach notification, being focused on CSPs. The Information Commissioner has a number of regulatory tools to use in tackling security breaches involving personal data, held by CSPs or otherwise. Some of those powers are intended to be punitive, whilst others such as the audit and reporting obligations are instead intended to proactively identify areas of weakness. Since the power to impose a Civil Monetary Penalty came into force in April 2010, the Information Commissioner

has levied fines amounting to £783,500 in relation to cyber security incidents.

23. The nature of the breach, including the impact on individuals – whether preventable or otherwise - is a key factor to take into account in considering what action to take. The Information Commissioner also has duties to promote compliance and has issued a range of guidance aimed at helping organisations avoid security breaches in the first place. This includes guidance aimed at learning from previous security breaches. The "Protecting personal data in online services: Learning from the mistakes of others" report mentioned some of the most common security mistakes encountered during his enforcement work.[1]

24. There is a distinction to be made between breaches which occur as a result of a known, preventable vulnerability and those which occur as a result of new or novel criminal attacks. The former are known risks (as illustrated by the SQL injection example at paragraph 17 above) which organisations should be able to prevent or mitigate via their security measures. The latter are the result of operating within a dynamic environment and, whilst they cannot be individually anticipated and dealt with, sensible precautions and keeping security under constant review will help to mitigate these.

25. That security breaches resulting from known vulnerabilities (such as loss of unencrypted drives, exploitation of SQL injection) still regularly occur is of concern as the Commissioner's 'Learning from the mistakes of others' report shows. It is also particularly of concern that some organisations are repeatedly subject to security breaches. Whether this is the result of organisational failures to institute improved procedures and practices, or as a result of having been identified by criminals as an easy target, is not easy to determine. Given the high profile which has been given to these incidents over the past few years, we would hope to find information security high on all organisations' agendas, not just CSPs'.

26. The additional security requirements which PECR and DRIPA place upon CSPs are a recognition of the inherent importance of that sector's effective functioning in everyday life. Those requirements do mean we have additional powers in respect of that sector than we have in respect of other sectors.

27. Mandatory breach notification reporting by CSPs means that we receive significant additional intelligence about that sector's failures

[1]Report "Protecting personal data in online services: Learning from the mistakes of others" is available at: www.ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf

compared to other sectors where no comparable obligation exists. Under regulation 5A of PECR CSPs must notify the Information Commissioner of personal data breaches. During 2015/16 to date[2] 143 breaches have been reported under this mandatory requirement. 21 of these breaches (15%) related to insecure webpages or hacking. Of breaches reported across all sectors under the DPA for the same period, 7% related to insecure webpages or hacking (87 out of 1287). However it is important to highlight the different breach reporting requirements, which make it difficult to meaningfully compare these figures. It is also worth noting that the reporting shows great variation in volume of reported incidents between CSPs and it is not clear whether this is due to significantly differing security standards or different interpretations of the threshold for reporting. It is however our view that the function of reporting should be a useful review tool for the CSPs, pushing them to keep their security measures under constant review.

28. It is also important to bear in mind that the European Union's General Data Protection Regulation (the GDPR) is currently going through the EU's legislative process and will replace the regime set by existing European Directive 95/46EC. This will impact significantly on all who process personal data including CSPs. The legislative process is expected to be concluded during the first half of 2016 and there will then be a two year period for implementation meaning that the GDPR is likely to be in force at some point in 2018.

29. Although the wording can be subject to change during the legislative process it will build on existing requirements to ensure appropriate security. Key elements are likely to include mandatory breach notification reporting for **all** data controllers, significantly increased penalties for breaching organisations, which may include the ability to fine a percentage of annual global turnover, and improved powers for data protection authorities. All of these should help to focus organisations' attention on protecting individuals' personal data. The Information Commissioner has been supportive of these elements of the proposed GDPR.

30. Following on from the implementation of the GDPR it is expected that the E-Privacy Directive on which PECR is based will be reviewed, and if the direction of travel with the GDPR is followed the provisions relating to security and breach notification will be reinforced.

31. Although there is already a substantial body of legally enforceable requirements around ensuring appropriate security there is one significant outstanding area where a further strengthening of the penalties is required to improve the overall regime. At present there is

[2] Figures correct as of 19 November 2015

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[3] 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. Whilst the Criminal Justice and Immigration Act 2008 includes a provision for introducing custodial sentences for the DPA section 55 offence[4], this has not been commenced. The replacement of the existing fines-only regime with the possibility of custodial sentences would also open up a range of lesser penalties which are not currently available but which might be an effective deterrent such as community service orders, curfews and tagging. The need for this has also been recognised by parliamentary committees considering this issue who have made recommendations that this provision should be triggered without further delay.[5]

The adequacy of the redress mechanisms and compensatory measures for consumers when security breaches occur and individuals' personal data are compromised

32. The DPA makes provision for individuals to seek compensation where they have suffered damage, and attendant distress, as a result of a data protection breach. Similar provisions apply where the requirements of PECR have been breached. However, the position under the DPA may be about to change. Depending on the outcome of the Vidal-Hall v Google appeal case currently pending in the Supreme Court, individuals may be able to claim compensation under the DPA for distress without having to provide accompanying evidence of pecuniary loss. This would represent a significant strengthening of individuals' right to seek compensation under the DPA.

33. Section 5A of PECR also requires that where a personal data breach has occurred which may adversely affect a subscriber or user, the CSP should notify the individual concerned without delay. This obligation may well be replicated for victims of data protection breaches in the finalised GDPR. However the effect of notification upon individuals is likely to depend on the extent to which the recipients know what steps to take to protect themselves – such as signing up to active fraud prevention alerting schemes and changing relevant passwords and

[3] Most recently the ICO's response to the PACAC inquiry into charity fundraising.

[4] The offence of knowingly or recklessly, and without the consent of the data controller, obtaining, disclosing or procuring the disclosure of personal data

[5] Lord Justice Leveson recommended in his report that the necessary steps should be taken to bring the provisions into force. Since the publication of his report, the Parliamentary Joint Committee on the Draft Communications Data Bill has added its voice to those of the House of Commons Justice and Home Affairs Committees in calling for sections 77 and 78 of the Criminal Justice and Immigration Act 2008 to be brought into effect.

login prompts. In the absence of that sort of practical knowledge, being informed of breaches is likely to have a more negative impact and may result in additional distress and/or confusion being caused.

Likely future trends in hacking, technology and security

34. We are seeing an upward trend of breaches from both mandatory and voluntary reporting. Whilst it is true that the breaches reported to us may represent only a fraction of the total number of breaches occurring it is our view that this will continue to rise in future years, as more and more personal data is stored online and an increasing number of services operate online. As organisations and individuals make use of growing number of electronic devices the potential attack surface will also increase. The so-called 'Internet of Things' presents security challenges which will need to be addressed by device manufacturers and service providers in order to deliver a safe and secure online environment.

35. It is also likely that those individuals attacking systems will continue to evolve their methods and make use of more sophisticated tools in order to gain unauthorised access to data controllers' systems. Whilst it is true that no system can be 100% secure, in our experience it is often the data controllers who fail to undertake the most basic of IT security tasks (such as updating their systems regularly or protecting against SQL injection attacks) which will be subject to the majority of cyber attacks.

Information Commissioner
23 November 2015