available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Data security: Past, present and future

Marcus Turle

Field Fisher Waterhouse LLP, CLSR Professional Board, London, UK

Keywords:
Data protection
Data security
Privacy enhancing technologies

ABSTRACT

The loss by Her Majesty's Revenue and Customs (HMRC) of two CDs containing 25 million child benefit details has changed the data security landscape forever. No longer is data security the exclusive and rather arcane preserve of spotty technology professionals or data protection lawyers. HMRC has thrust data security onto the front pages of the mainstream media and brought it very suddenly to the top of the political and commercial agendas of senior politicians and boards of directors. In this article, the author will outline the reasons behind the rise of data security as a front line issue and examine the lessons to be learnt from HMRC. He will analyse the different facets of data security risk and explore ways in which organisations can go about managing it. He will outline the attitude of regulators to data security and where regulatory developments are likely to take us. The final part of the article looks into the future, with particular focus on the emergence of privacy enhancing technologies.

1. Background – a short history of data security

While HMRC was the largest and most high profile data security breach of last year, it was not the only significant one. In fact, there have been a series of significant breaches over the last 18 months. What started as a trickle has now become something approaching a torrent as the mainstream press has cottoned on to the political embarrassment of government shortcomings in data security and the fact that revelations about lost data directly affect millions of citizens.

The following is a summary of what might be termed the 'key' events over the last 18 months. Together, they present a clear picture of the enormity of the task which lies ahead for government and business in recognising the significance of, and identifying and managing, data security risks.

- In January 2007, Clive Goodman, royal editor of the *News of the World*, and accomplice Glenn Mulcaire, a private investigator, were convicted under the Regulation of Investigatory Powers Act 2000 for unlawfully hacking into mobile voicemail messages of royal employees and were jailed for four months. Stories were printed about a medical problem of the Prince of Wales, from information gleaned from tapping phones of members of staff of the Prince of Wales' household.[1]
- In February 2007 the Financial Services Authority (FSA) fined the Nationwide Building Society £980,000 following the loss of a laptop which had created a risk of financial crime.[2] A Nationwide employee had put details of nearly 11 million customers onto his laptop which was later stolen from his home. The fine was a penalty for Nationwide failing to have effective systems and controls to manage its information

[1] http://news.bbc.co.uk/1/hi/uk/6301243.stm.

[2] http://news.bbc.co.uk/1/hi/business/6360715.stm, http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml, http://www.fsa.gov.uk/pubs/final/nbs.pdf.

0267-3649/$ – see front matter © 2009 Field Fisher Waterhouse LLP. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2008.11.001

security risks and because it had failed to start an investigation for three weeks after the theft occurred.

- In March 2007 the Information Commissioner named and shamed 12 banks and other financial institutions for failing to dispose of customer information properly. Each was found to have left personal customer information in dustbins outside their premises. HBOS, Alliance & Leicester, Royal Bank of Scotland, Natwest, Barclays, Nationwide and the Post Office (along with five others) were required to sign a formal undertaking to comply with the data protection principles.
- In August 2007 Forensic Telecommunications Services, a company that provides evidence on telephone use for police forces in connection with investigations, was the victim of a theft at its premises in Kent in which a server containing files of forensic evidence used by police in criminal investigations was stolen. The server contained details of who had made calls on mobiles, their exact location and when they were made.[3]
- In October, following an attack on its customer database, the internet service provider FastHosts warned users to change their main account control panel login password, all email passwords, all FTP passwords and all passwords for its hosted MySQL and Microsoft SQL Server databases. It even took the authoritarian step of unilaterally changing passwords of customers who ignored the warning.[4]
- In December, a government wide data security review revealed nine NHS trusts in England had lost the medical records of hundreds of thousands of patients.[5]
- Also in December, the FSA fined Norwich Union Life (NUL) £1.3 million for not having effective systems in place to protect customers' confidential information and failing to manage its financial crime risks. The failures had enabled criminals to impersonate customers by using publicly available information to target NUL policies, and through contact with NUL's call centres criminals had obtained (and in some cases altered) confidential customer information, including customers' contact addresses and full bank account details. Weaknesses in NUL's customer ID procedures had allowed criminals to instruct the company to surrender 74 policies to criminals' bank accounts, resulting in a loss to customers of £3.3m.[6]
- In June of this year, an unnamed Cabinet Office employee was suspended after top secret documents from the Joint Intelligence Committee were found on a Surrey-bound commuter train and handed to the BBC. Cabinet Minister Ed Miliband later admitted to ''a clear breach of well established security rules which forbid the removal of documents of this kind outside secure government premises without clear authorisation and compliance with special security procedures.''

These are just a sample of what has now become a litany of data security breaches involving both government and private sector organisations. The government has responded with a series of pivotal policy announcements, legislative developments and regulatory initiatives:

- In February 2007 the Lord Chancellor announced that consequent upon *What price privacy?*[7] and a Department for Constitutional Affairs consultation,[8] legislation would be introduced to amend the Data Protection Act 1998 (DPA). This amending legislation was introduced in the House of Commons as part of the Criminal Justice and Immigration Bill and was passed in May this year, giving the ICO power to impose substantial fines on organisations which ''deliberately or recklessly'' breach the DPA. It also gives the Secretary of State power to introduce unlimited fines, or imprisonment for up to two years, for data theft offences under s.55 of the DPA.
- In August 2007, the Home Office published its Partial Regulatory Impact Assessment on the licensing of private investigators,[9] which resulted in part from *What price privacy?* Responses were published in May of this year[10] and a Full Impact Assessment is due to be published shortly.
- As part of the response to HMRC, the Prime Minister announced that the Information Commissioner would be given new powers of inspection within the public sector[11] and a consultation on this proposal was launched in July.[12]
- On the regulatory front, at the end of last year the Information Commissioner revealed his new strategy for laptop data security saying that in cases of laptop loss, the absence of encryption will result in enforcement action.[13] This announcement built upon his data security strategy contained in his July 2007 consultation paper.[14] Likewise, the Financial Services Authority made a number of important policy announcements about data security, as part of its fight against financial crime, with Independent Financial Advisors and appointed representatives[15] being identified in particular. The FSA issued a 100-page report and guidance document on Data Security in Financial Services in April this year.
- In July the Walport report, commissioned by the Prime Minister as an independent review of the data protection regime, recommended the introduction of a statutory

[3] http://www.theregister.co.uk/2007/08/15/fts_forensic_data_theft/.
[4] http://www.theregister.co.uk/2007/11/30/fasthost_hack_update/.
[5] http://news.bbc.co.uk/1/hi/uk/7158019.stm.
[6] http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml, http://www.fsa.gov.uk/pubs/final/Norwich_Union_Life.pdf.
[7] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf.
[8] http://www.dca.gov.uk/consult/misuse_data/consultation0906.pdf, http://www.dca.gov.uk/consult/misuse_data/consultation0906resp.pdf.
[9] http://www.the-sia.org.uk/NR/rdonlyres/1FCBCD2E-B3E0-4B61-A0A4-3C33FAB72C41/0/sia_pi_pa_ria.pdf.
[10] http://www.the-sia.org.uk/NR/rdonlyres/8B3F8377-2994-4717-BF8F-3F00642E1508/0/pi_pa_response.pdf.
[11] http://news.bbc.co.uk/1/hi/uk_politics/7106366.stm.
[12] See: *The Information Commissioner's inspection powers and funding arrangements under the Data Protection Act 1998*, available at http://www.justice.gov.uk/publications/cp1508.htm.
[13] http://www.ico.gov.uk/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx.
[14] http://www.ico.gov.uk/upload/documents/library/corporate/notices/ico_dp_strategy_draft.pdf.
[15] http://www.fsa.gov.uk/pubs/newsletters/fc_newsletter9.pdf.