Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing

Data Loss in the British Government: A Bounty of Credentials for Organised Crime

Paul A. Watters
Internet Commerce Security Laboratory (ICSL)
University of Ballarat
p.watters@ballarat.edu.au

Abstract

Personal information stored in large government databases is a prime target for criminals because of its potential use in identity theft and associated crime, such as fraud. In 2007-2008, a number of very high-profile cases of data loss within the British Government, its departments and non-departmental bodies raised three pressing issues of public significance: (1) how broad was the loss across agencies; (2) how deep was each loss incident; and (3) what counter-measures (organisational and technical) could be put in place to prevent further loss? This paper provides a chronological review of data loss incidents, and assesses the potential to mitigate risk, given organisational structures and processes, and taking into account current government calls for further medium and long-term acquisition and storage of citizen's private data. The potential use of the "lost" credentials is discussed in the context of identity theft.

1. Introduction

Governments are entrusted with our personal data for good and necessary reasons, such as the planning and provision of public services, determining eligibility for access to public services, and associated accountability of public expenditure.

However, as governments acquire and store more personal data of their citizens, in order to provide better and more accountable services, are they securing our personal data effectively? The question can be posed from two distinct perspectives: (1) a privacy rights perspective, which seeks to enshrine an inherent right to privacy of personal data; and (2) a cybercrime perspective, which is concerned with the potential for misuse of large sets of credentials – if illegally obtained – for identity theft. While the first perspective is important, the focus of this paper is the potential for cybercrime, particularly the potential for identity theft. Given the proposed expansion of personal data holdings by the British government, the focus of this case study will be British government data loss.

Numerous incidents of data loss across all branches of the UK government over the past two years, and several reviews have been initiated to ensure policy and procedure implementation. However, from an outsider's perspective, it appears that each government branch is focused on devising their own reports and potentially their own solutions. This is a shame, since there are common lessons across government which can be learned.

Two clear themes emerge from the chronology and analysis of data loss presented in Section 2: (1) many data loss incidents involved contractors, but there appears to have been little attempt to ensure compatibility of government and private sector policies; and (2) most lost data was not encrypted, there instead being a reliance on "password protection" and "registered mail" for confidentiality. Since cybercriminals are both innovative and opportunistic, ensuring consistency among access policies, as well as end-to-end confidentiality, would provide a basic level of security (but not privacy).

While there was a lot of publicity in late 2007, and during 2008 about British government data loss, unfortunately the situation does not appear to be getting any better – for example, on 2/11/2008, an unencrypted USB memory stick containing passwords for access to the Government Gateway was found in a pub car park in Cannock, Staffordshire. The stick also contained source code for the site and security software. The Government Gateway controls access to 100 services including online tax returns and benefit claims, and has 1.8 million users, so the potential pool of credentials available for identity crime is enormous. The Department of Work and Pensions (DWP) have reportedly found that an employee of Atos Origin – the outsourcing company running Government Gateway – lost the stick [1].

For organised crime, obtaining these large sets of credentials is much easier than going committing resources to the more difficult enterprise of phishing [2].

978-0-7695-3737-5/09 $25.00 © 2009 IEEE
DOI 10.1109/UIC-ATC.2009.73

IEEE computer society

2. Data Loss Incidents

In this section, I will outline some of the major data loss incidents that occurred during 2007-08, broken down by agency or department. It is useful to examine the practices and strategies from this perspective because of the individual remedies and responses that have been advocated and/or enacted within each branch of government, but not across the whole government.

2.1. HMRC (HM Revenue & Customs)

In September 2007, the personal details of 25 million child benefit claimants were reportedly sent in the post to National Audit Office (NAO) by HMRC, using TNT [3]. The discs never subsequently recovered. The discs contained names, addresses, dates of birth, child benefit numbers, National Insurance numbers and bank or building society account details. This incident has caused created greater public awareness of the handling of sensitive, personal data by the public sector.

The HMRC Chairman Paul Gray was forced to resign over the incident. Apparently, the data were not encrypted. Since this initial data loss – and despite significant adverse publicity - numerous examples of data loss have been reported across departmental and non-departmental government bodies over the past 12 months. The potential for identity theft is enormous. For example, Avivah Litan (Gartner) suggests that bank account numbers sell for the highest price on the black market, somewhere between $30 and $400 [4].

Multiply this by 25 million customers, and the value on the black market is staggering. One possible remedy would be to rekey account numbers, but this would be a massive undertaking.

While data breach notifications are mandatory in some US states (e.g., California), they are mandatory in the UK, so customers may not even know that their credentials have been lost by an organisation. There is an interim voluntary disclosure code in Australia, which may be modified in any future review of the Privacy Act [5].

Why was such a large download required by the National Audit Office (NAO)? NAO had previously used HMRC's internal sample of 1,500 cases for fraud detection [6]. Larger scale checks were now required by new international auditing standards. The routine disc transfer started in March 07. NAO had suggested to HMRC that it remove the names of parents, their addresses and bank details – to save space, and not to prevent disclosure - but an HMRC official reportedly refused on the following grounds:

"I must stress we must make use of [existing] data we hold and not overburden the business by asking them to run additional data scans/filters that may incur a cost to the department."[1]

In November 2007, 15,000 customers of Standard Life had their banking and pension details lost. HMRC had sent them to Standard Life using a courier [7]. It took 5 weeks for HMRC to notify affected citizens. The courier collected discs but they were never delivered.

2.2. Ministry of Justice

The Ministry is the government department responsible for UK courts, prisons, probation, criminal law and sentencing [8]. In June 2007, three laptops were reportedly stolen which contained details of 14,000 fine defaulters. The data were not encrypted, and there were no physical security measures on the computers within a secured facility. The data comprised names, dates of birth, addresses, offences and, national-insurance numbers.

In December 2007, four CD's were reportedly lost in the post. The discs were sent by "recorded delivery" but never delivered. HM Inspectorate of Court Administration (HMICA) will not confirm whether the data was encrypted [9].

In July 2007, the Ministry lost a portable 500G hard-drive disk containing personal details of 5,000+ jail governors and guards [8]. The disk held names, dates of birth, national insurance, prison service employee numbers and addresses. It was apparently 12 months before contractor EDS realised the disk was missing. The disc was sent to Mitcheldean, Gloucs, for testing in Washington, Wearside, on July 20 last year, subsequently moved to Telford, Shrops.

2.3. National Health Service (NHS)

In December 2007, service provider BT reportedly sent the names and addresses of children registered with the City and Hackney Teaching Primary Care Trust (CHTPCT) in the mail. The records were not delivered to a staff member at the destination hospital, and have never recovered. The records were given to a member of the public counter who was standing near the enquiries counter [10].

In February 2008, Russells Hall Hospital lost a laptop containing personal details of 5,123 patients, which had only password protection [11]. Other NHS

[1] Reported in The Times (http://news.bbc.co.uk/2/hi/uk_news/politics/7106987.stm)

data losses have also been reported during the past year by [10]:

- Bolton Royal Hospital
- Sutton and Merton Trust
- Sefton Merseyside Trust
- Mid-Essex Trust
- Norfolk and Norwich Trust
- Gloucester Partnership Foundation Trust (historical data)
- Maidstone and Tunbridge Wells Trust (2 cases)
- East and North Hertfordshire Trust (recovered)

The total combined annual loss exceeds 168,000 records.

2.3. Department for Work and Pensions (DWP)

In December 2007, personal data of 45,000 people claiming benefits in West Yorkshire were reportedly lost. Data included names, dates of birth and national insurance numbers [12]. A search of the home of a former contractor also revealed personal records relating to thousands of benefit claimants [13].

2.4. Ministry of Defence (MOD)

In January 2008, approximately 600,000 personal records of recruits or potential recruits were reportedly stolen from a laptop running the Training Administration and Financial Management (TAFMIS) system, from a Royal Navy recruiter in Birmingham [14]. In October 2008, a portable hard drive containing names, addresses, passport numbers and driver's license details of 100,000 serving British military personnel was also lost.

Full replication of TAFMIS on laptops is apparently common for off-line recruiters [15].

In September 2008, a disc carrying sensitive personnel information was stolen from a military base. Details of all current and ex-RAF personnel and their children - stored on three USB-connected storage drives - were also stolen from a base in Gloucestershire [16].

2.5. MI-5 and MI6

In October 2008, a palmtop MI-5 computer was reportedly stolen through an open window in Manchester, reportedly containing information on terrorism [17].

In October 2008, an eBay sale of a digital camera revealed data reportedly owned by the SIS. The camera's memory contained details of suspected al-Qaeda members and their fingerprints, as well as other pictorial intelligence [18].

2.5. Crown Prosecution Service (CPS)

In February 2008, the CPS reportedly lost a disc of hundreds of DNA crime scene profiles sent by Dutch authorities, as part of Operation Thread. The disc has since been recovered, but the resulting investigation revealed a series of small errors which together led to the data being misplaced for a significant period of time.

2.6. Driver and Vehicle Licensing Agency (DVLA)

In December 2007, a hard drive in Iowa was reportedly lost containing details of 3,000,000 learner drivers. The data were stored by Pearson Driving Assessments [19]. In a separate incident, the DVLA lost 7,685 records including vehicle keeper name, address, registration mark of the vehicle, chassis number, make and colour, for drivers registered in Northern Ireland [20].

2.7. The Home Office

In February 2008, a Home Office disk was reportedly found hidden in a laptop computer that had been sold on eBay. The CD was found wedged between the keyboard and circuit board of the laptop [21].

Separately, from the J Track offender monitoring system, the names, addresses and dates of birth of around 33,000 offenders in England and Wales were reportedly lost on a memory stick [22].

Also reportedly lost were the names and dates of birth of 10,000 priority offenders. The names, dates of birth and, in some cases, the expected prison release dates of all 84,000 prisoners held in England and Wales [22].

The contractor – PA Consulting - who reportedly lost the data, also worked on the government's new ID card project.

2.8. Cabinet Secretary and Cabinet Office

In June 2008, the Secretary for local government Hazel Blears reportedly had an unencrypted computer stolen from her constituency offices in Salford, which included some restricted, but no top-secret information [23]. Also in June 2008, two documents marked SECRET were reportedly left on a train from Waterloo to Surrey. The documents were stored in a bright orange cardboard envelope, contained details of government actions against al-qaeda in Pakistan and

Iraq, and were marked for UK, US, Canadian and Australian eyes only" [24].

2.9. British Broadcasting Corporation (BBC)

In August 2008, the personal details of around 250 children being stored on a memory stick were reportedly stolen from a car belonging to a member of staff at Objective Productions [25].

2.10. General Teaching Council (GTC)

In September 2008, the personal data of 11,423 teachers reportedly went missing on a disc, en-route to the organisation's office in Birmingham [26].

2.11. Insolvency Service

In September 2008, a laptop containing the personal details of almost 400 former directors of insolvent companies was reportedly stolen during a burglary at the Insolvency Service office in Manchester [27].

2.12. Kirklees Council

In September 2008, a Virtual Private Network (VPN) server reportedly bought from Ebay had links to private council documents. The server contained the necessary passwords to download these documents on council's servers [28].

3. Security Reviews and Countermeasures

As a result of these data loss incidents, a number of policy and procedure changes have been enacted across different government agencies. For example, the Cabinet Office has mandated that no more than 1,000 personally-identifiable records be transported together. In addition, a number of reviews have been conducted to try and identify any systematic failings which may have contributed to the data loss. The two major reviews are the Poynter Review [29] of the HMRC data loss incident, and the Burton Review [15] of the MOD data loss incidents.

Poynter's Review makes interesting reading. He believes that the loss of data was "entirely avoidable" and the result of "serious institutional deficiencies". He notes an "absence of proper training", and "muddled accountability" for the ownership and guardianship of data. There was also "no visible management of data security at any level". HMRC's information security policies were inadequate, and those that they had were unduly complex, and not adequately translated into guidance for employees to actually use.

It's important to note that both organisational and technical failures contributed to the HMRC data loss. HMRC business processes had been designed for paper not computers, and the organisation suffered from low staff morale and complex organisational structures. PAYE, National Insurance, Child Benefit and Tax Credits all had their own systems, each of which contained a separate customer record, and which had separately developed and maintained security policies and procedures which may not have always been consistent.

Poynter made a number of recommendations for change at HMRC. In terms of technical counter-measures, obligatory use of protective measures (such as encryption and penetration testing) and controls (for example on use of mobile devices or on access to records) have been recommended. At the organisational level, a change in culture – with an aim to protect all personal data, and a recognition that some data needs more protection than other data – was suggested. The proper use of personal information includes both service planning and delivery. Mandatory training for those working with or managing protected personal information was also suggested, and appropriate censures and punishments – in response to a failure to apply protective measures – be applied, leading ultimately to dismissal.

Poynter also suggested that approaches to information risk across government be standardised and enhanced, and that security and privacy of government-held data should be based around "information charters". The public should also be made aware of government use and handling of their data.

On examining the data loss incidents in Section 2, it is clear that the attacks have a number of common characteristics which have standard countermeasures. However, others – such as carelessness – are harder to proscribe. Confidential paper files left on trains and USB sticks left in pub car parks are both tricky problems – better physical measures to prevent the removal of paper files from secure premises, and end-to-end confidentiality through encryption would have helped in both cases[2]. Also, where there has been involvement of external contractors, there appears to have been little effort to ensure compliance with government confidentiality requirements. Ensuring that all contractors who handle any identifying information about citizens are compliant with at least a baseline government standard would be a starting point – especially if the requirement for compliance is identified at the pre-tender qualification stage for large

[2] Note that – in the case of countermeasures such as encrypted USB sticks for data transfer – steps should be taken to ensure that data is recoverable in the case of a lost or misremembered password!

government projects. Alternatively, the adoption of Sarbanes-Oxley-style legislation to ensure that CEOs ultimately take responsibility for security breaches would provide a strong incentive for adherence to mandatory security requirements.

In terms of personally identifying data, this should be removed from individual data records, if there is no requirement to identify individuals. For example, aggregated data may be used by local government for planning purposes. Also, the principles of least privilege and separation of duties must be rigorously enforced, and the least amount of data that is necessary to be transferred between parties to fulfil a specific requirement should be estimated in advance.

4. Risk and Vulnerability

There is no evidence that the personal data lost in any of these incidents has resulted in identity theft – but, in the case of HMRC, it would be difficult to attribute theft to this source, since it includes the majority of adults living in Britain.

One of the major concerns arising from the data loss is that the British government is set on greatly expanding the type and quality of data held about individuals. For example, the new £12b e-records system for the NHS will make all patient records accessible from anywhere in the country [30]. A Green record will be available to any legitimate NHS user and to the patient through HealthSpace. An Amber record will only available if patient gives the clinician permission at the time of the consultation and the patient can view it on HealthSpace. A Red record will not be available on the system or on HealthSpace. While this level of access control is admirable, if the security of data handling at the organisational level does not match the technical controls, then data may be exposed or lost. For example, if the clinician actually lets their secretary access their computer system, or if system or database administrators are given free access to underlying file systems or databases, then there is potential for data leakage.

A more ambitious program is GCHQ Interception Modernisation Programme [31], which would provide SIS, MI-5 and police with access to every text, email and website visit to website made by anyone in the UK. Currently, MI-5 must obtain a Regulation of Investigatory Powers Act (RIPA) warrant via the Home Office to collect and access this data. A centralised database would lower the cost of viewing communications traffic/data as required, and make the important task of fighting crime and preventing terrorism easier. However, the same questions about the NHS database could also be asked here.

5. Conclusion

The widespread loss of personal data within the British government – including any identifiers used as primary keys in government databases, or whose contents could be used to satisfy "identity tests" – is worrying. If this data was obtained by organised crime groups, it could clearly be used – in total - to take over the majority of identities of the adult British population, especially the details lost in the HMRC incident. The minimum estimate of the number of lost records of cases reviewed in this paper is 29,586,917. This data could also be used to facilitate various kinds of fraud, since artefacts of the strong proof of identity – such as bank accounts – were also disclosed.

As governments seek to acquire more and more personal data about their citizens – often with the best of intentions – we need to ask what additional safeguards will be put in place to protect our data. If existing technological countermeasures are not sufficient, could newer systems – such as the Trusted Platform Module (TPM) – make a difference?

6. Acknowledgements

The author receives funding from the State Government of Victoria, IBM, Westpac, the Australian Federal Police and the University of Ballarat.

7. References

[1] Daily Mail, Tax website shut down as memory stick with secret personal data of 12million is found in a pub car park, 2/11/2008. Retrieved from http://www.dailymail.co.uk/news/article-1082402/Tax-website-shut-memory-stick-secret-personal-data-12million-pub-car-park.html

[2] Stephen McCombie, Paul Watters, Alex Ng, Brett Watson: Forensic Characteristics of Phishing - Petty Theft or Organized Crime? WEBIST (1) 2008: 149-157.

[3] Vnunet.com, HMRC data loss leaves 25 million exposed, 21/11/07. Retrieved from http://www.vnunet.com/vnunet/news/2203916/hmrc-boss-resigns-loss

[4] Itpro.co.uk, Revenue head quits after massive data breach, 1/12/2007, Retrieved from http://www.itpro.co.uk/140448/revenue-head-quits-after-massive-data-breach

[5] Australian Government, Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988. Retrieved from http://www.pmc.gov.au/privacy/docs/government_response_pcr.pdf.

[6] Computer Weekly, HMRC data loss: NAO request office, 23/11/2007. Retrieved from http://www.computerweekly.com/Articles/2007/11/

23/228261/hmrc-data-loss-nao-request-evidence.htm

[7] Vnunet.com, Red faces as government laptop goes missing, 8/10/2007. Retrieved from http://www.vnunet.com/vnunet/news/2200705/red-faces-government-laptop

[8] ZDnet, Ministry of Justice report nine data breaches, 18/8/2008. Retrieved from http://news.zdnet.co.uk/security/0,1000000189,39462444,00.htm

[9] ZDnet, Ministry of Justice loses four CDs of personal data, 23/1/2008. Retrieved from http://news.zdnet.co.uk/security/0,1000000189,39292348,00.htm

[10] BBC, Nine NHS Trusts lose patient data, 23/12/007. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/7158019.stm

[11] Express and Star, 5,000 patient records stolen, 14/2/2008. Retrieved from BBC, Nine NHS Trusts lose patient data, 23/12/007. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/7158019.stm

[12] Telegraph, Housing benefit details latest to be lost, 3/12/2007. Retrieved from http://www.telegraph.co.uk/news/uknews/1571192/Housing-benefit-details-latest-to-be-lost.html

[13] BBC, Fresh benefit data lapse admitted, 1/12/2007. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/7123285.stm

[14] Herald Tribune, U.K. reports new data loss for 100,000 military staff, 10/10/2008. Retrieved from http://www.iht.com/articles/2008/10/10/europe/britain.php

[15] E. Burton, Report into the Loss of MOD Personal Data, 30/4/2008. Retrieved from http://www.mod.uk/NR/rdonlyres/3E756D20-E762-4FC1-BAB0-08C68FDC2383/0/burton_review_rpt20080430.pdf

[16] The Register, MoD prays RAF disk thieves aren't data savvy, 29/9/08. Retrieved from http://www.theregister.co.uk/2008/09/29/raf_usb_drives_stolen/

[17] Computing.co.uk, MI5 palmtop computer stolen from open window, 3/10/2008. Retrieved from http://www.computing.co.uk/computing/news/2227480/mi5-palmtop-stolen-open-window

[18] Informatics Online, Security probe after MI6 camera sold on Ebay, 1/10/2008. Retrieved from http://www.infomaticsonline.co.uk/vnunet/news/2227214/security-probe-mi6-camera-sold

[19] CNet, UK Government loses data on driving-test candidates, 18/12/2007. Retrieved from http://news.cnet.com/U.K.-government-loses-data-on-driving-test-candidates/2100-1029_3-6223292.html

[20] The Times, Northern Irish driver data discs lost in the post, 11/12/2007. Retrieved from http://www.timesonline.co.uk/tol/news/uk/article3034420.ece

[21] Pocket Lint, Another data loss for government, 29/2/2008. Retrieved from http://www.pocket-lint.co.uk/news/news.phtml/13143/14167/UK-Government-in-CD-scandal.phtml

[22] The Guardian, Data loss: Government like keystone cops, says Clegg, 22/8/2008. Retrieved from http://www.guardian.co.uk/politics/2008/aug/22/justice

[23] Sky News, Hazel Blears Community Secretary's computer is stolen, 19/6/2008. Retrieved from http://www.guardian.co.uk/politics/2008/aug/22/justice

[24] Backup Anytime, UK Cabinet office official to be charged over data loss, 26/5/2008. Retrieved from http://www.backupanytime.com/blog/2008/09/29/uk-cabinet-office-official-to-be-charged-over-data-loss/

[25] Vnunet.com, BBC partner loses children's data, 11/8/2008. Retrieved from http://www.vnunet.com/vnunet/news/2223662/bbc-partner-loses-children-data

[26] Vnunet.com, Data loss exposes teachers' records, 26/9/2008. Retrieved from http://www.vnunet.com/vnunet/news/2227046/gtc-loss-scandal

[27] Computer Weekly, Insolvency Service suffers another government data loss, 18/9/2008. Retrieved from http://www.computerweekly.com/Articles/2008/09/18/232355/insolvency-service-suffers-another-government-data-loss.htm

[28] Pocket Lint, Day of data loss disasters, 30/9/2008. Retrieved from http://www.pocket-lint.co.uk/news/news.phtml/18021/19045/day-of-data-loss-disasters.phtml

[29] K. Poynter, Review of information security at HM Revenue and Customs, 25/6/2008. Retrieved from http://www.hm-treasury.gov.uk/d/poynter_review250608.pdf

[30] Telegraph, The sickening £12 billion NHS fiasco, 4/1/2009. Retrieved from http://www.telegraph.co.uk/comment/3639250/The-sickening-andpound12-billion-NHS-fiasco.html

[31] The Times, There's no hiding place as spy HQ plans to see all, 5/10/2008. Retrieved from http://www.timesonline.co.uk/tol/news/uk/article4882622.ece