Disciplinary action for data breaches

06/10/2015

Local Government analysis: Are local authorities doing enough to tackle and sanction data breaches? David Bowden, freelance independent consultant, examines the findings of the Big Brother Watch report and considers the action local authorities can take in this area.

Original news

Fewer than one in ten council workers punished for privacy breaches, LNB News 11/08/2015 44

Daily Telegraph, 11 August 2015: Fewer than 10% of council workers are punished for breaches of privacy, including one instance in which CCTV cameras were used to watch a colleague's wedding.

What is the background to the report?

On 11 August 2015 the Big Brother Watch portal published 'A Breach of Trust--How local authorities commit 4 data breaches every day'.

The report notes that we are handing over more of our personal data than ever before to local authorities in exchange for more efficient and better targeted service. As part of this deal we expect that the information will be kept secure and those who have access to the information are properly trained. Its survey shows that between April 2011 and April 2014 there have been at least 4,236 data breaches. 'Local Authority Data Loss', a previous Big Brother Watch report found that between July 2008 and July 2011 personal data had been lost 1,035 times.

It is not just the number of the breaches which raise concerns, but the lack of proper punishment. Despite more than 400 instances of loss or theft, including 197 mobile phones, computers, tablets and USBs and 600 cases where information was inappropriately shared, just one single person has faced criminal sanctions and only 50 employees have been dismissed.

What is the methodology of the report?

A freedom of information request was sent by the Big Brother Watch Foundation (BBWF) to all 434 local authorities in the UK on the 9 June 2014. BBWF received a 98% response rate. It asked for these individual number totals:

- convicted for breaking the Data Protection Act 1998 (DPA 1998)
- had had their employment terminated as the result of a DPA 1998 breach
- disciplined internally
- resigned during proceedings, and
- where no action was taken

The BBWF report sets out the reported breaches in some detail. A few authorities declined to provide any data, but it is notable that 36% of local authorities reported no issues at all with data protection. This is not just limited to smaller local authorities but it is notable that some large authorities have a good track record in this field too such as Westminster, Reading, Derry City, Sheffield and Dundee.

What are the conclusions of the report?

The report makes these six recommendations:

- a custodial sentence should be an available punishment for serious data breaches
- serious data breaches should result in a criminal record
- data protection training within local government should be mandatory
- the mandatory reporting of a breach that concerns a member of the public

- standardised report systems and approaches to handling a breach, and
- the extension of the Information Commissioner (ICO) assessment notice powers to cover local authorities

BBWF says that current penalties for serious data breaches do not deter individuals who are seriously considering breaking the law. Judges presented with serious data breaches should be able to hand out custodial sentences if the perpetrator is found guilty of a serious breach. The legislation to make breaching DPA 1998, s 55 punishable with a custodial sentence already exists in the Criminal Justice and Immigration Act 2008, s 77 (CJIA 2008). If this part of CJIA 2008 is brought into force, BBWF says that this would show that the government is serious about safeguarding the privacy of individuals.

BBWF says that individuals who commit a serious data breach are rarely prosecuted and correspondingly do not get a criminal record. An individual could therefore resign or be dismissed by an organisation only to seek employment elsewhere and potentially commit a similar breach. In organisations which deal with highly sensitive data, knowing the background of an employee is critical.

What sorts of privacy breaches does this report cover?

The report notes a whole range of things that have gone wrong. Many of the instances reported are inadvertent and many of them are quite trivial. There are instances of emails being sent to the wrong distribution lists but such errors are not limited to public authorities. The report lists the thefts or losses of laptops and mobile phones. Any impacts of such losses could be minimised if the data was encrypted. There are instances of the wrong report being sent out in error and some cases of data being given out without prior adequate verification. Finally, there are some comical confessions including the one from Cheshire where a member of the authority's CCTV team had used it to watch the wedding of someone else on the team.

What are the report's findings on more serious data privacy breaches?

There are around 20 serious breaches in the report in relation to English local authorities. In just over a quarter of these cases, a warning was issued. In one case no action was taken and in others formal disciplinary proceedings have been taken or are ongoing. In one quarter of cases, an employee resigned and in another quarter the employee was dismissed. Only Lewisham and Portsmouth councils indicated that this may not be the end of the matter having either referred the matter to ICO or said that it was 'now a legal matter'.

These more serious breaches included instances of the following:

- accessing confidential council data regarding family members or for personal use
- accessing child reports and offering to provide copies to a relative
- extracting electronic social care record files for use in an employment tribunal claim
- falsification of residential address for personal gain
- accessing and amending council data for personal reasons, and
- accessing confidential information on Department for Work and Pensions and/or HMRC data bases without a legitimate business reason or appropriate authorisation

What are the current sanctions for data protection breaches?

There are four groups of sanctions that can be applied where breaches of data protection are identified:

- unlawful data obtaining under DPA 1998, s 55
- computer misuse under the Computer Misuse Act 1990 (CMA 1990)
- misconduct or misfeasance in public office, and
- offences under the Fraud Act 2006 (FA 2006)

Unlawful data obtaining under DPA 1998, s 55

Prosecutions for unlawful obtaining can only be initiated by the ICO or by or with the consent of the Director of Public Prosecutions. The DPA 1998, s 55 offence was initially designed to address the growth in private investigation agencies

offering services based on the acquisition of such information. There is a £5,000 maximum fine on conviction in a magistrate's court and the potential for an unlimited fine if a case reaches a crown court.

Although CJIA 2008, s 77 empowers the Secretary of State for Justice to increase the maximum penalty by statutory instrument to a sentence of up to two years prison in the crown court, to date no such order has been made. The first prosecution in November 2002 at Kingston Crown Court related to a benefits agency employee who had offered to sell personal data that had been unlawfully obtained. In *R v Rooney* [2006] EWCA Crim 1841, [2006] All ER (D) 158 (Jul), Bean J approved a fine of £700 on appeal for a DPA 1998, s 55 offence where data had been obtained from the Police National Computer. This related to two offences of unlawful obtaining and one of unlawful disclosure. The offending, while in breach of the employer's rules, was relatively trivial as details were obtained about the appellant's sister and a police officer she was having a relationship with after a planned wedding had been called off. Some of the instances noted in the BBWF report are of this nature and some authorities have made referrals onwards to the ICO.

The ICO publishes details of DPA 1998, s 55 convictions and penalties. These include:

- £200 fine to estate agent who attempted to access the account of a benefit claimant over the telephone
- £800 fine and £400 costs for bank cashier who accessed the bank account details of woman who had accused her husband of sexual assault, and
- £1050 fine and £1,160 costs for NHS worker who passed on patient details to her boyfriend who worked for a personal injury claims management company

Computer misuse under the CMA 1990

There are four principal CMA 1990 offences:

- CMA 1990, s 1--unlawful access or hacking
- CMA 1990, s 2--unauthorised access with intent to commit further offences
- CMA 1990, s 3--unauthorised acts with intent to impair the operation of a computer, and
- CMA 1990, s 3A--making, supplying or obtaining articles for use in offences under CMA 1990, 1 or 2

The BBWF report notes a number of cases where council workers have accessed confidential data and this would appear to engage the CMA 1990, s 1 offence. The BBWF report notes that in Tower Hamlets a staff member falsified a residential address for personal gain which would appear to engage the CMA 1990, s 3 offence. While the maximum sentences under CMA 1990 range from two to ten years' imprisonment or an unlimited fine where they are tried in a crown court, sentences handed down are lower.

In *R v Baker* [2011] EWCA Crim 928 where a CMA 1990, s 1 offence was charged the sentence was four months in jail. It should be noted here that this offending was against a public authority, the Welsh Assembly Government, but these sort of bodies were not in scope for the BBWF report. For a CMA 1990, s 2 offence, where a bank employee had sold confidential details of two bank account holders, a four-month prison sentence was upheld on appeal (*R v Delamare* [2003] EWCA Crim 424, [2003] All ER (D) 127 (Feb))

Despite all this, it does not appear from the responses to the BBWF that any local authority is considering let alone prosecuting serious misuse of their computer systems under CMA 1990.

Misfeasance in public office

The reported cases on misfeasance in public office have to date involved police officers who have used data on the Police National Computer for their own purposes. What all the cases have in common is that these sorts of data breaches invariably result in an immediate prison sentence for the offender whatever mitigation is presented. The prison sentences on cases which have reached the Court of Appeal have ranged from nine months to three-and-a-half years. Where Police National Computer data has been sold or used for commercial gain or where safety of members of the public has been put in jeopardy, then this tilts the sentence towards the upper end of the scale. In *R v O'Leary* [2007] EWCA Crim 186, Longmore LJ in the Court of Appeal said the starting point for a sentence (subject to mitigation) was an immediate prison sentence of four years.

A few of the most serious breaches identified in the BBWF report would on their face appear to amount to misfeasance in public office. However, it does not appear that any local authority has sought to prosecute any member of their staff for this.

Offences under FA 2006

This seems to be appropriate for offending at the higher end of the scale. The maximum penalty is ten years in prison or an unlimited fine or both. However, unlike CMA 1990, detailed sentencing guidelines have been issued which took effect on 1 October 2014.

The main FA 2006, s 1 offence provides that it can be committed in three ways:

- FA 2006, s 2--false representation
- FA 2006, s 3--failing to disclose information, and
- FA 2006, s 4--fraud by abuse of position

In *Skelton* (unreported, Bradford Crown Court, 17 July 2015), the charge and conviction was for FA 2006, s 4 offence which resulted in an overall prison sentence of eight years. While not a case involving data theft but rather systematically forged documents in a people smuggling scheme, the Court of Appeal upheld a sentence of nine years for charges including an FA 2006, s 2 offence (*R v Bina* [2014] EWCA Crim 1444). It does not seem from the BBWF report that systematic fraud was identified as an issue by any local authority that responded.

Is this a reflection on budget cuts?

Matthew Cooper at the Local Government Association (LGA) does not believe this to be the case:

> 'Councils take data protection extremely seriously and staff are given ongoing training in handling confidential data. Given the huge volume of data councils handle, breaches are proportionately rare. When they do occur, robust investigations and reviews are immediately undertaken to ensure processes are tightened.'

The LGA qualifies this by saying it can't comment on individual councils' policies regarding disciplinary action.

What can explain the low level of disciplinary action following a breach?

From the responses to BBWF, one or more of these 14 sanctions have been applied. In ascending order of seriousness these are:

- no disciplinary action
- report data loss to the ICO or police
- additional advice and training provided on IT and/or DPA and/or use of CCTV
- investigation
- verbal warning or informal action or counselling or reprimand
- management advice or formal note on supervision file
- final written warning
- suspended pending disciplinary process
- compromise agreement
- demotion
- employee resigned or retired before outcome of disciplinary process
- summary dismissal or termination of employment or agency worker told not to return
- prosecution of local authority worker by ICO, or
- legal action by local authority against employee who committed data breaches

Each local authority will have different terms and conditions that apply to their contracts of employment with their staff. Where a data breach has been identified, then the local authority will need to deal with this according to the contract of employment.

Where a local authority is considering disciplinary action, it will need to comply with the ACAS code of practice 'Disciplinary and Grievance Procedures'. Where an employer does not follow the ACAS code, then they are at risk of a claim for a 25% uplift in compensation if an unfair dismissal case reaches an employment tribunal. Paragraphs 18 and 19 of the ACAS code are quite clear:

'Where misconduct is confirmed or the employee is found to be performing unsatisfactorily it is usual to give the employee a written warning. A further act of misconduct or failure to improve performance within a set period would normally result in a final written warning.'

'If an employee's first misconduct or unsatisfactory performance is sufficiently serious, it may be appropriate to move directly to a final written warning. This might occur where the employee's actions have had, or are liable to have, a serious or harmful impact on the organisation.'

The ACAS code says that some acts of gross misconduct are so serious in themselves or have such serious consequences that they may call for dismissal without notice for a first offence but a fair disciplinary process should always be followed, before dismissing for gross misconduct. ACAS says that disciplinary rules should give examples of acts which the employer regards as acts of gross misconduct. These may vary according to the nature of the organisation and what it does, but might include things such as theft or fraud, physical violence, gross negligence or serious insubordination.

Rather disappointingly, the BBWF report glosses over all this. It is clear from the responses to BBWF that sanctions have been applied including the most serious ones such as dismissal, demotion or legal action. What is more difficult to glean from the BBWF report is whether standards in this area are being enforced in a uniform manner. If individual authorities want to take a different enforcement approach in the future for data breaches then their disciplinary rules will need to make this clear.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor