Reprinted with permission of PDP Journals

Information security and lessons from HMRC — an overview of the Poynter and IPCC reports

Bridget Treacy, Partner at Hunton & Williams, *suggests there are wider lessons to be learned from Poynter*

Bridget Treacy is chairing the 7th Annual Data Protection Compliance Conference in London.

For more information on this Conference, which takes place on the 2nd and 3rd October 2008, please visit www.pdpconferences.com

When a junior employee at Her Majesty's Revenue and Customs ('HMRC') lost two unencrypted CDs containing the entire child benefit database in October last year, it shook the world. Data Protection and information security became headline news, rather than merely the preserve of the geeky few. We even began to characterise events as being either 'pre-HMRC' or 'post-HMRC.' Having settled into the new world order in which information security has assumed greater significance as a corporate risk, and in which our regulators have become more proactive in enforcing data breaches, the recent publication of two key reports into what actually happened at HMRC has attracted remarkably little comment. Yet the reports provide many useful insights for both the private and public sectors.

In this article, we distil some of the key themes of the Poynter Report and the Independent Police Complaints Commission ('IPCC') Report.

The Poynter report

Following the loss of the child benefit database by HMRC in October 2007, Keiran Poynter, Chairman of PricewaterhouseCoopers, was appointed to undertake a review of information security within HMRC.

Divided into two distinct parts, the report provides a factual account of the background leading up to the data loss, and comments in broader terms on information security across HMRC as a whole, making numerous recommendations for improvement.

In terms of overall conclusions, the report identifies two major deficiencies which were key to the data loss:

(i) information security was not a management priority; and

(ii) the organisation did not focus on management accountability.

Of course, the position at HMRC was more complex than the identification of these two key deficiencies might suggest. However, it is the likelihood that these deficiencies are not unique to HMRC, or even unique to the public sector. Indeed, the report generates a certain amount of sympathy for HMRC, and a sense that information security procedures at many other organisations are likely to suffer from many of the same shortcomings.

The investigation

The forensic examination of events leading up to the data breach concludes that, contrary to some of the early reports in the media, no single event led to the decision at HMRC to download the child benefit database onto two CDs, and to send them unencrypted by post to the National Audit Office ('NAO.') Rather, a number of factors contributed to the breach, and a number of people were involved in the events which led to the breach.

Key amongst the factors which led to the breach, were the informal nature of some of the internal procedures at HMRC, which were not documented in any detail and not generally known by staff, and decisions which focused on operational issues at the expense of security risks. The series of decisions which led to the database being made available to the NAO was made informally and incrementally, by emails exchanged over a period of time, and without reference to senior management.

The report also points to several 'institutional' factors which contributed to the data loss. It is in this context that HMRC's policies and guidelines are particularly criticised as being too generic to offer any real guidance to staff in particular circumstances. Indeed, some of the 'policies' appear to have been guidance for developing a policy, rather than a description of the actual procedures to be followed.

It appears that few HMRC staff were aware of the existence of the policies, which were disseminated via HMRC's intranet. Most of those interviewed did not know where to locate the security policies on the intranet. These criticisms are similar to criticisms made by the Financial Services Authority (the 'FSA') during some of its investigations into data breaches, particularly in the context

(Continued on page 8)

(Continued from page 7)

of Nationwide's data breach in early 2007. In that case, the FSA observed that staff did not know where to find the policies, the policies themselves were piecemeal, and staff did not have access to training. Nationwide was fined £980,000, in part to serve as an example to others. At HMRC there was no single person or group with responsibility for the data. A data guardian or data owner can play a crucial role in acting as a focal point for data protection and data security issues within an organisation.

Wider issues at HMRC

In addition to investigating the specific facts which led to the data loss at HMRC, the Poynter report examines information management within HMRC more generally.

In this section of his report, Poynter recommends the implementation of an information management strategy which is more in line with strategies created within the private sector. Perhaps somewhat radically for the public sector, Poynter recommends that HMRC moves from merely accepting responsibility for collecting and managing customer data, to a strategy which encourages customers to entrust their data to HMRC, on the understanding that they will be responsible for keeping the data secure, and customers retain responsibility for updating their information. Further, HMRC will move away from paper-based records to digital records structured, in the case of individual taxpayers, as single customer records.

Poynter argues that such a strategy will address the fragmented nature of the data currently held by HMRC which, in turn, will make it easier to keep data synchronised and current. He states that the internet banking model (which is broadly similar) demonstrates that people like to retain control over their data and that this, in turn, improves efficiency as less data are held.

A move to a 'trust' based model is perhaps slightly ironic given the very significant breach of trust by HMRC in losing the child benefit database. However, the report acknowledges that the transformational nature of the strategy is the long term goal. In its early stages, the objective will be to ensure HMRC regains control of data security in the context of existing processes and consolidates that control. These tasks will, no doubt, focus on rebuilding trust with individuals.

To implement such a strategy, HMRC will need to address criticism that information security was not a management priority, and that there was no clear mechanism for creating accountability. Part of the explanation for these shortcomings appears to be incremental growth over a period, and little real focus on integrating new functions into the existing organisational structure. There appears to have been a 'silo' mentality with little communication outside individual silos.

IPCC Report

Concurrently with the Poynter investigation and report, the IPCC investigated whether there had been any criminal conduct or disciplinary offences committed by HMRC staff. The focus of the IPCC report is therefore different and more factually based. It does not seek to recommend changes to organisational and management structures in the way that the Poynter report does.

The criticisms of the IPCC are expressed in fairly robust terms, but the report is clear in its conclusion that there was no evidence of criminality in connection with the disclosure of the data to the NAO.

In essence, the report concludes that there was no coherent strategy for mass data handling. Specifically, the IPCC criticises the absence of meaningful systems, the failure to appreciate the importance of data handling and a 'muddle through' ethos.

It considers that there were probably breaches of the Third Data Protection Principle (data must be adequate, relevant and not excessive) and the Seventh Data Protection Principle (data must be afforded appropriate technical and organisational security), but that these breaches were caused by a lack of understanding and the absence of procedures concerning data security.

Next steps at HMRC

The Commissioner has now served an Enforcement Notice on HMRC. Unsurprisingly, in his Notice to HMRC, the Commissioner identifies a breach of both the Third and the Seventh Data Protection Principles. He also notes that the likelihood of distress caused by the breach is self evident, and he refers to the right to respect for private and family life, home and correspondence contained in the European Convention on Human Rights.

The Commissioner has required HMRC to use its best endeavours to implement, within 36 months, the 45 recommendations contained in the Poynter Report, and to provide annual reports to the Commissioner. Pre-Notice, HMRC had already started down the path towards implementing the 45 specific recommendations; the Poynter Report contains a table indicating that each recommendation had been accepted by HMRC, and has either been implemented or is in the process of implementation.

Wider lessons

The essential criticisms made by the Poynter and IPCC reports could equally be made of many organisations in the private sector. Yet too often we see organisations unwilling to deal proactively, or thoroughly, with information management issues. When an organisation suffers a data breach, a significant part of the overall cost of dealing with the breach is the cost of reassuring existing customers and rebuilding their trust.

How many companies can state that information security is a management priority and that management is held accountable for information security? As the Information Commissioner's new power to fine companies for serious breach of the DPA takes effect, we are likely to see more examples of companies who continue to ignore information security risks.

Bridget Treacy
Hunton & Williams
btreacy@hunton.com