

# HM Revenue and Customs

Large central government agencies such as the Inland Revenue have been subject to considerable computerisation, many such projects being financed by a mix of public and private sector investment over the last twenty years. In the UK, some 4 million people work in local government, central government and public administrations such as the National Health Service. It is therefore not surprising to find much of the rhetoric surrounding the expected benefits of eGovernment within the UK to be focused around efficiency and effectiveness improvements associated with the re-organisation and re-deployment of staff supported by integrated ICT systems.

In April 2000 the UK e-Government Strategic Framework was published requiring all central government departments to produce eBusiness strategies. These were intended to show how each department planned to implement eGovernment and to achieve electronic service delivery targets. The first draft was required in October 2000. From July 2001 departments were required to report progress against eBusiness strategies to the Office of the e-Envoy every six months. The Inland Revenue was until 2005 the UK government department responsible for collecting and administering taxation. This government department has attempted to be at the forefront of eGovernment in the UK by transforming its performance using ICT. This is evident in much of the strategic thinking emanating from the leadership within the organisation.

For instance, at this time the organisation indicated four indicators that it would use to determine how well it has transformed itself. First, the receipt of clean data from customers would allow the Inland Revenue to remove work that added little value to the organisation and consequently release people

to work at the front line of customer care. Second, increasing the organisation's capability to deliver services electronically and increasing the take-up of such services by customers. Third, it intended to increase use of knowledge management so that its staff had better guidance which in turn enhanced its customer service capabilities. Finally, information and data management would enable it to progress towards the 'joined up government' vision of developing seamless, quality services and making best use of the data it receives.

The department set out its first eBusiness strategy in 2000. The key feature of the strategy at this time was the development of a number of access channels for different customer groups with clear incentives to encourage use of such channels. As part of this strategy the organisation intended to offer improved e-services to the UK taxpayer, thus reducing the burden of compliance on individuals and organisations. The revenue also planned use of intermediaries such as the National Association of Citizens Advice Bureau (see case), the Post Office and software suppliers to provide bespoke services to the customers of the organisation. This transformation was predicated upon greater integration of its services with that of other departments and the provision of its services through commercial and government portals. It also required transformation of staff roles to focus around support for the customer through the use of electronic tools.

In 2001 the Inland Revenue revised its strategy, keeping the fundamental principles above but making two additions: first, a transformation of the organisation around a focus on the customer; and second a philosophy based in customer relationship management, creating a technical framework

that would deliver e-services in a modular but integrated fashion. Within this strategy, the Inland Revenue established three targets. First, that 50% of services would be available electronically by 31st December 2002. By this time the organisation aimed to offer basic secure e-services and have developed plans for organisational change based on such services. Second, it intended to have 50% take-up of its services by 2005. Third, all of its services would be available electronically by 31st December 2005. By this date the Inland Revenue aimed to have achieved significant business transformation with most customer transactions being conducted electronically.

However, subsequent to publication of the strategy, the Inland Revenue merged with Customs and Excise in 2006 to form Her Majesty's Revenue and Customs (HMRC). This was part of a wider attempt at improving the efficiency of UK government departments stimulated by a review of activity.

The newly formed HMRC, however, soon came into the spotlight in 2007 for its failings in data management.


In October of 2007 a junior official from Her Majesty's Revenue and Customs (HMRC) based in Washington, Tyne and Wear sent two compact disks (CDs) containing government records to the National Audit Office (NAO) based in London. The data was requested by the NAO in order to enable them to run their own independent survey of child benefit payments. The disks were password-protected but the data was unencrypted. The package was sent unrecorded and un-registered using a courier company. The records on the disks contained the names, addresses, birth dates and national insurance numbers of all 25 million individuals dealt with by the HMRC in relation to child benefits. The records also contained details of partners, the names, sex and ages of

couple's children as well as bank/savings account details for each claimant. This meant that details of 7.25 million bank accounts associated with families were stored on the disks.

The disks failed to arrive at the offices of the NAO and following notification of this a second package was sent by registered post and arrived safely. In November of 2007 senior managers at the HMRC were told that the first package had been lost. A week later the Prime Minister and other government ministers, most notably the Chancellor of the Exchequer were informed of the loss. Initially, government ministers were told that the CDs would probably be found but when HMRC searches for the lost disks failed the Metropolitan Police were called in to investigate.

This data loss led the Chancellor to consult with the Information Commissioner, the person responsible for overseeing the implementation of data protection in the UK, and they agreed that consultation with UK financial institutions was required. At the request of these financial institutions the public was not informed of the data loss for some days in order to allow these institutions to monitor potential suspicious activity. Banks and other financial institutions tracked transactions back to the date at which the data was lost in an attempt to identify suspicious activity.

As a consequence of this data incident the HMRC Chairman resigned and the Chancellor made an announcement to the House of Commons. It was claimed that a junior civil servant at the HMRC had broken data security procedures in downloading the data to disks and sending these via unrecorded postal delivery. The Chancellor reassured the public that the police had no reason to suspect the data had got into the 'wrong hands'.



However, the public was urged to keep a close eye on their bank accounts for any unusual activity.

The possibility of criminals gaining access to the data and hence engaging in mass identity theft and identity fraud was raised in numerous quarters. This included not only criminals using data to gain access to existing bank accounts but also the possibility of such deviant groups using personal identity data to open new bank accounts or other financial products such as credit cards in the name of

individuals. The issue of paedophile rings gaining access to the data on children and using such data for 'grooming' activities was also raised as a possibility.

A report into this incident was published in June 2008. The report concluded that the HMRC was woefully inadequate in its handling and managing of corporate data. It made a series of recommendations for tightening of data security and improving data management practices across UK government.

### **Points for reflection**

- Managing channels of access is a significant issue for eGovernment. How is this issue relevant to the current case?
- In what ways do you think strategy in this area for private sector organisations differs from that for public sector organisations?
- The case highlights the importance of good data security and data management for organisations. With increasing concern over identity theft and data privacy the reputation of organisations is increasingly reliant on good practices in this area. Investigate what the private sector is doing to ensure this.