

Panic stations over security

The government shuts up shop but, asks Jane Dudman, is it too little too late?

The recent fiasco over missing personal data may yet have catastrophic implications if the information ends up in the wrong hands, but in the meantime it has had a remarkable effect across government.

One striking thing about the crisis has been the absence of an identity champion for government. No one in the public sector has stepped forward to affirm the principles on which the government's transformational agenda, of which datasharing is the largest pillar, rests. Instead, there has been the unedifying sight of civil servants ordering reviews of their data-handling processes as though no one had ever given a thought to this matter before.

Some think this is a missed opportunity for government to conduct a debate about both the technicalities and the underlying philosophy of the relationship between state and citizen over personal information. "The whole ID debate is couched in the 20th century debate about a big brother state, but there is in fact a new trade-off between the state knowing more about you and the public services it provides," says Ian Kearns, deputy director of the Institute for Public Policy Research.

Kearns believes the HM Revenue & Customs debacle should prompt a rethink of this relationship. "If the state knows more about you and me in the 21st century, then we should probably have more to do with the state," he comments. While citizen engagement is often confined to small, local participatory budgeting projects, Kearns thinks there might be far larger movement towards people being more involved in democratic accountability.

Wave of fear

Instead, a wave of fear and defensive reaction is running through government. Richard Thomas, the information commissioner, is riding the crest of that wave, in intense discussions with, it seems, almost every department and agency, on how they handle data. Describing the privacy breach as shocking, Thomas also said it was a serious wake-up call to the whole

of government, pointing out that the public was not aware that the records and bank accounts of 25 million citizens could be so easily downloaded on to a couple of computer discs.

Thomas's department is to gain greater powers as a result of the fiasco: a result for Thomas himself, but part of a general trend that runs counter to lifting the burden of regulation.

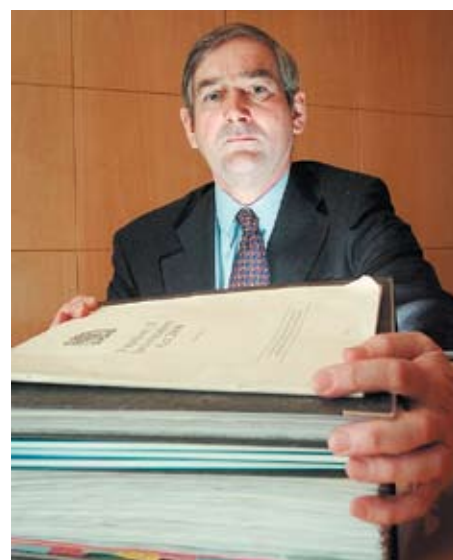
Natalie Ceeney, chief executive of the National Archives, who is also head of profession across government for knowledge and information management, prefers not to comment on whether the fiasco will enhance or otherwise the professional standing of those involved in her profession (see pages 38-39). Part of the problem is that information management staff still tend to be relatively junior and have little sway over policies.

Identity

Concerns over security are likely to impact development of the national identity scheme, which will be supported by a single, logical database holding the biographical information of all individuals registered. Academics from the London School of Economics have argued that holding this information in this way is inherently insecure, saying the Home Office and Cabinet Office should hold open meetings with industry and experts to discuss the challenges for transformational government that arise from the widespread use of centralised databases.

Suppliers, on the back foot over their own handling of information, seem to be keeping fairly quiet, too, as they watch how this issue works itself out. The private sector has little room for complacency; doubtless there are as many reviews of information security going on in private companies as in government right now. The difference is that the private sector conducts such reviews behind closed doors.

But some firms think the government should make more of its own successes. Eran Farajun, executive vice president of software firm Asigra, which has several public sector customers, says the government "needs to prove to



Richard Thomas, information commissioner

the world that it is keeping up with the rest of the UK as a leader in the field of technological advancement and make full use of the technology it has". Farajun says many people have lost confidence in the ability of the government to protect sensitive information about its citizens, but rather than step back, defensively, the government needs to announce its successes, and should not be shy of continuing to focus on rethinking the way it shares data between departments, particularly in terms of ensuring processes are stringent enough to prevent such an incident from happening again.

At least this has prompted far more of a debate about some basic principles. Until now, it's been too easy to assume that information security and data protection are rather arcane, geeky issues. Only the diehard libertarians, it has been assumed, have been involved in any kind of debate, even over such major schemes as the national identity scheme. Now, that no longer holds true. With every parent in the country potentially at risk of fraud, information security has stepped into the limelight.