Editorial

Journal of Database Marketing & Customer Strategy Management (2008) **15**, 135–137.
doi:10.1057/dbm.2008.15

It cannot go on. It really cannot.

In the first editorial of this year, we commented, at length, about the problems potentially facing organisations if they lose public confidence in their ability to look after their data. At the time, we noted:

‘It [the issue of Data Security] is presently very topical in the United Kingdom. If one reads the newspapers, one can hardly escape the issue. The government, in the guise of its taxation arm, the Revenue and Customs division, decided to send two cd’s, containing the personal and banking details of 25 million individuals, from one department to another’.

Nearly nine months on and what has changed? Sadly, not a lot: instead we have been treated to much more of the same. In the week in which I am writing, government, in the shape of the Home Office, has just lost a database of the entire prison population that was left lying around on a laptop. Or maybe data stick.

This crowns a pretty bad year for government, which has reported more data security incidents than ever before. Meanwhile, a leading bank just happened to leave the personal details of maybe a million customers on a laptop, which subsequently washed up on the further shores of eBay; and a hotel chain has been hacked, with the result that possibly anyone who booked in over the last year may be at risk of ID fraud.

It would be comical if it weren’t so serious. A part of the problem, of course, is that the media have their teeth into the issue. That’s a charge to which I must plead guilty myself, as in-between commissioning and writing for the *Journal of Database*

Marketing, I also write for a number of other media. Editors are like hounds who have scented fox: they’re up, they’re off, they’re baying for blood.

They are looking for stories about data insecurity — and by God, major corporations are making them happen. A similar effect may be at work in government, which bleats rather self-consciously that the number of reports of data security breaches are up because they have tightened the reporting rules. There may be some truth in that: the crime figures bear out just how any campaign to combat a particular crime leads at first to an increase in the reporting of that crime.

But still, it will not do. Thus far, the government has just about stayed ahead of the curve. In response to the first inklings that not all was well in the state of UK Data Security, they promised reviews, greater powers for the Information Commissioner and higher penalties for those who deliberately flout the law.

Unfortunately, the above has proven to be mostly a succession of very damp squibs. The main effect of reviewing what went wrong is that the review gives the press a second bite at the cherry. In most instances, the cause of the breach is very simple: in general terms, human error, combined with slightly lax procedures and a desire at the top to cut corners. Although the spectacle of reviews set in motion and reporting months later still sets my teeth on edge.

As someone who has worked at the sharp end of database technology I know that ‘what went wrong’ is rarely complicated — and the root causes can usually be sorted out within 24–48 hours.

Just what government reviews are doing in the weeks they appear to need is something that I cannot understand. Perhaps they are taking the time, because it impresses the public. Perhaps the facts are discovered on day 1 — and the rest of the time is taken up with working out the correct spin to give them.

I digress. Reports and reviews are probably not helping much any more. The Information Commissioner is not getting to get all the powers he asked for. In particular, he is not going to get the powers of increased (pro-active) audit that he felt were necessary to go into organisations and investigate. At the time of writing, although the government has agreed on stiffer penalties for obvious data crimes, it has not yet ratified the level of penalties.

It has also focussed on the sharp end: on those parts of the data chain where individuals within organisations think they can make a fast buck by selling data they are not entitled to send.

Three cheers! Except this is not really the issue. The largest, most upsetting instances of data loss are those that seem to happen with the full connivance of 'standard operating procedure'. Laptops go missing. Data sticks go walkabout. Files are lost in the post.

These are not exactly criminal activities — even if the government could make them so. They are breaches of security which is, unfortunately, just ONE of the 8 Data Protection principles. So while the Information Commissioner remains focussed on taking up issues across each of the eight principles — from fair obtaining to accuracy — the public is far more concerned with what, for them, is the single big one.

Impasse. But I talked about staying ahead of the curve. In terms of spin and public announcements, it feels as though the government has just about managed to do that. So far.

Yet it seems inconceivable that they will continue to do so. To date, many of the

stories about data loss are just that: stories about data loss. Few have yet moved on to stories about consequential loss: for instance, to retail the dire consequences for individuals when fraudsters start to make use of their data.

In fact, in many cases, it is likely that the story never will make that next leap. A recent story of a lost data stick carries the rider that it may simply have been dropped into a bin. That is a feeling we all have had from time to time. We have misplaced something small but essential and, now we come to think about it, we have a vague recollection of seeing it at the edge of the table poised just above the litter bin.

If the refuse collection hasn't been carried out for the week, there follows a mad dash to the dustbin, and a long and smelly sifting through its contents in the hope it will turn up. In the case of a large government department, the task is rather more difficult. A little like looking for a needle in a haystack which, in essence, is exactly what the issue is.

So yes: the government has lost a lot of data over the last 12 months: but just because it is lost, that doesn't mean that the most pessimistic scenario must automatically be true. Sometimes, lost data is just that — lost data. Or in one case that I remember from the days of steam-driven computing: the file that went missing had simply been over-written with something else. The weekend shift had suffered a shortage of back-up tapes — and weren't too fussy about which tapes they seized for the purpose.

Sooner or later, though, there will be evidence of real loss, real pain caused by insecure data and then it seems likely that the government will be quickly trampled beneath the demands that 'something must be done'. At which point, expect spectacular — and badly formulated — legislation that is tough, but does very little to address the real problems.

It truly is inconceivable that we are now on the brink of such knee-jerk law-making.

There is a good deal of serious security advice around. The best advice looks to generate secure processes, while still recognising that systems are operated by humans. Best advice also needs to look very carefully at how companies configure their home-working packages.

If companies allow data to go off their main premises, then sooner or later, it will be lost or stolen. If you give 100 employees a blank data stick, the chances are that half a dozen of them will have lost it within a week. If you give a manager a laptop, then it is an open invitation to them to leave it in a pub or on a train, or to have it removed unceremoniously from their car, while they are doing the weekly shop.

Anything an employee can carry, a thief can carry too.

In fact, often the item does not even need to be removed from the premises. A short interlude looking after security for a department I managed inside one of the UK's largest insurers taught a salutary lesson. At the beginning of my reign as local security chief, our department purchased six laptops. Over the next three months, they appeared to be less and less available because — we believed — more and more staff were making productive use of them and taking them home for work purposes.

Not so. We received our rude awakening when the overall security staff for the company called us in and showed us videotape of cleaning staff relieving the department of one of its laptops. A spot check then revealed that the same gang had removed all but one of the six laptops over the period in question. Our fault: we should have had better procedures for tracking our laptops.

However, the issue is much more fundamental. Put your data on to anything small — whether its laptop, palmtop or data stick — and you significantly increase the risk of its being taken or lost.

It is time for companies to start taking some hard choices. Do they want security? Or flexible working? If the former, then they cannot continue as they do now. Data cannot continue to travel around the corporate environment unchecked. It simply mustn't go onto portable media or if it does, it needs to be encrypted — a recent Tory Party suggestion — and stripped wherever possible of all truly personal content.

I regularly analyse files of millions of records on what are essentially home premises. I never need or request or obtain data that can be tracked back to specific individuals. Leftover data are deleted shortly after it ceases to be required.

If companies don't start to impose simple rules of this kind, then the public will. Senior personnel are likely to be made responsible for breaches. There will be a step change to the level of fines. Home-working — at least using any sensitive data — will become a thing of the past. The message feels simple: clean up, or clear out.

It is almost ironic that this issue begins with such a thundering editorial on the topic of data security. In theory, this was to be an issue dedicated to such issues. Unfortunately, the vagaries of paper production and referrals have made that not possible. All else being well, the next issue will be our data special.

This issue includes a very useful paper on 'What characterises the culture of a market-oriented organisation' by Dr Aihie Osarenkhoe, 'Managing event-driven marketing' by E Xenis and 'Cross-national segments for a food product' by Moskowitz *et al.* A mixed bag — but a relevant one, all covering issues that have been encountered in real-world marketing over the last few months.

JOHN OZIMEK
Managing Editor