



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Speech to RSA Conference Europe on data breaches

Richard Thomas, Information Commissioner – 29 October 2008

I turn now to the subject at the heart of today's conference – data security, or should I say data insecurity. Sadly, 2008 has undoubtedly been the year of data breaches and data losses.

Data losses did not start with the loss of 25 million child benefit records by HMRC nearly a year ago. We had been warning of the problems for some time before then, but that was the case that undoubtedly catapulted the issue close to the top of the public and political agenda. Since then many other cases have hit the headlines. I can reveal today that the number of data breaches reported to my office has soared to 277 since November 2007. There have been 28 breaches by central government; 75 within the NHS and other health bodies; with 80 reported in the private sector. We are currently investigating 30 of the most serious cases. We have already taken enforcement action against HMRC, the Ministry of Defence, the Department of Health, the Foreign and Commonwealth Office, Virgin Media Ltd, Skipton Financial Services, Carphone Warehouse, Talk Talk, and Orange Personal Communications Services Ltd.

The number of breaches brought to our attention is serious and worrying. I recognise that some breaches are being discovered because of improved checks and audits as a welcome result of taking data security more seriously. But the number notified to us must still be well short of the total. How many PCs and laptops are junked with live data? How many staff do not tell their managers when they have lost a memory stick, laptop or disc? How many organisations decide not to tell us? Many losses are simply undetected. Much more worrying is where – in an age of ever increasing cyber-crime, illegal access and identity theft – organisations are not even aware that personal information which they hold has been stolen, obtained by fraud or otherwise

fallen into the wrong hands. Worse still, there are still organisations which are not aware of the risks that they face with any collection of data and have not taken adequate steps to deal with those risks. Worst of all, are those organisations who have simply failed to understand just how much personal information they are accumulating through more and more and ever-cheaper technology. Much is said and written about information being a valuable asset. It is also a toxic liability.

Personal information is now the lifeblood of government and business and is central to our work, family and leisure time. The reality of the 21st Century is ever-increasing flows of digital data, revealing and recording almost everything we do, every transaction we undertake, our preferences and sometimes even our innermost hopes, worries and fears. Used properly and intelligently, personal information leads to better customer service, improved efficiency, more effective law enforcement and protection of the vulnerable and a better quality of life for everyone.

But this means that respecting and protecting people's privacy and personal information – data protection – has never been more important. As government, public, private and third sectors harness new technology to collect vast amounts of personal information, the risks of information being abused increases. It is time for the penny to drop. The more databases that are set up and the more information exchanged from one placed to another, the greater the risk of things going wrong. The more you centralise data collection, the greater the risk of multiple records going missing or wrong decisions about real people being made. The more you lose the trust and confidence of customers and the public, the more your prosperity and standing will suffer. Put simply, holding huge collections of personal data brings significant risks.

It is therefore alarming that – despite high profile data losses, the threat of enforcement action, a plethora of reports on data handling and clear ICO guidance – the flow of data breaches and sloppy information handling continues. Of course it is important to recognise that incidents vary from

regrettable one-off and probably unavoidable accidents to wholesale and systematic failure to take information security seriously. But everyone must also recognise that data breaches can cause harm, distress and hassle for the individuals affected, can lead to serious financial losses and can seriously affect the reputation of organisations. We have already seen examples where data loss or abuse (sometimes linked to identity theft) has led to fake credit card transactions, witnesses at risk of physical harm or intimidation, offenders at risk from vigilantes, fake applications for tax credits, falsified Land Registry records and mortgage fraud and exposure of the addresses of service personnel, police and prison officers and battered women. Sometime lives may be at risk. There have already been cases for example where prison staff have had to be relocated because of security concerns.

There must be a wake-up call each time there are headlines about unencrypted laptops which have gone missing, health or financial records found in the streets or memory sticks or hard drives which cannot be accounted for. But are there still too many people asleep at the helm?

This is a central challenge for those who lead all private and public organisations. The custodians of our data must earn and retain our trust and confidence. They have the responsibility to ensure that it is kept safely and in line with the requirements of the Data Protection Act. This is not just a matter of security. It will never be possible to eliminate losses and data breaches entirely. This simply emphasises the importance of data minimisation; collect, use and store no more personal information than is necessary and keep it for no longer than necessary.

All of this must ultimately be a matter of good governance and accountability. There is no single magic bullet, but there will always be three key elements:

- **Clear thinking and paperwork** – Ensuring the right policies, procedures, contracts, compliance arrangements etc.

- **Getting the technology right** – Awareness of the power of technology, the risks of ever-cheaper storage and mobile data and looking to use technology to minimise risks - “Privacy by Design”.
- **Focussing on people and behaviour** – Recognising that the challenge is cultural and psychological - and must be led from the top – with the right approaches to awareness programmes training, managements, and supervision.

Those at the top of organisations – chief executives, permanent secretaries and so on – must be certain that the right framework is in place to address the risks of personal information and must be certain that responsibilities are clear. There must be complete clarity on who, inside each organisation, has responsibility for safeguarding each set of personal data. This is equally important where data is shared, sometimes amongst several sources, and where processing is outsourced to contractors. Given the levels of risk, there is also a role here – as we elaborated in the Thomas/Walport Report on Data Sharing – for reassurance to be provided through Audit Committees and Statements of Internal Control in annual reports. This should be enlightened self-interest and bodies such as the CBI can help to ensure adequate controls and disclosures. But the Financial Reporting Council and others will need to intervene if high-level accountability is not achieved in practice.

There is also an important role for my Office as the regulatory body, with a role to educate, scrutinise and police. As approaches to regulation become less light-touch, the law plays an increasingly important symbolic and substantive role in showing that data protection must be taken seriously. I have already mentioned that we have taken enforcement action in suitable cases, but the current law has limited impact. We (and many others) have long argued that our powers, sanctions and resources – fixed in another era – are now wholly inadequate. The ICO has made clear for some time that a stronger approach is required to help prevent unacceptable information handling. At last there is movement. Earlier this year Parliament decided that the ICO should have the power to impose substantial penalties for deliberate

or reckless breaches. I understand that the government is working to ensure this measure is implemented as soon as possible. The threat and reality of substantial penalties will concentrate minds and act as a real deterrent. The notification fee for the largest organisations needs to be increased to give the ICO the resources we need to do our job properly. We are also looking forward to new powers to undertake inspections and audits of data controllers.

It is unfortunate that it has taken calamity to convince the government that we need stronger powers, resources and sanctions, but we must also take care not to overreact. We do not need laws for their own sake or ill-considered laws. I am very sceptical about the value or viability of laws requiring individuals to be notified when there is a breach. When personal information has been lost, stolen or otherwise compromised, the immediate priority is to manage the security breach and take all necessary steps to reduce the risks to individuals and to the integrity of the organisation's operations. As a matter of good practice, the ICO should be contacted immediately when any significant breach is discovered and, with the benefit of risk assessments applying to the particular situation, we can ensure that individuals who are affected are being told where that is necessary or genuinely useful. But I do not favour placing a statutory duty on organisations to notify people directly whenever a breach occurs and I am doubtful that a satisfactory law could satisfactorily distinguish in advance between situations where notification is needed and those where it is not. Each breach carries different levels of risk and, consequently, requires a different response. Unless written and interpreted with very great care, a mandatory notification requirement would add a significant extra burden for organisations and, more worryingly, could produce 'breach fatigue' if it were to result in frequent and unnecessary notifications of minor incidents. This carries the very real danger that people will ultimately ignore notifications when there is, in fact, significant risk of harm. Notifying people, when there is often not much they can do about the situation wrongly shifts responsibility from the organisation to the individual and diverts attention and resources away from prevention. Put simply, where the risks posed by security breaches are serious, a notification requirement would be too timid. If they are not, it would be excessive.