

Would you rather lose your business from too little or too much Information Governance?

1. The issue

According to the newspapers, any and all loss of personal data is likely to result in dire consequences to the individuals and organisations concerned (see below for a selection from the last year's headlines). Reactions to these incidents are quite rightly to move to address obvious shortcomings, but in doing so, some over-draconian steps have been taken and there are now some signs of too much or the wrong kind of protection. This paper argues that now more than ever is the time for security professionals to maintain a sense of balance. Managing risks is and always has been about realistic appraisal of risks and appropriate balanced countermeasures.

Realistic appraisal of risks

Newspapers will exaggerate to sensationalise – it's what they do. Of the selection of headlines below, few of the articles analyse the real threat to the individuals, and those that do concentrate on the worst cases. For example, the MOD loss of 100,000 records in an unencrypted laptop was well publicised, but the fact that only 3,500 of those contained bank details was buried in the small print. True, there was serious cause for concern for the 3,500, but not for all of the 100,000 who were worried needlessly, but then why spoil a good scare story with balance?

2. Recent headlines show too little information security and governance in the past:

From Guardian Online 7/4/2008:

HSBC [admitted]... it had lost a disc containing details of 370,000 customers. It contained the names, dates of birth and insurance cover levels of people with life assurance at the bank, generally linked to a mortgage.

From Silicon.com: 30/9/2008:

September 2008: General Teaching Council (GTC) for England loses details on 11,423 members

September 2008: Three hard drives are stolen from a secure RAF facility in Gloucestershire. One report puts the number of [personal] records lost at 50,000.

September 2008: News emerges that the details of 5,000 prison staff were contained on a drive lost by EDS in 2007.

September 2008: Four CDs containing the details of almost 18,000 staff are lost as they are moved between the wages department of Whittington Hospital NHS Trust and payroll company. The CDs are found again later that month.

August 2008: [PA Consulting loses a data stick](#) holding records on 84,000 prisoners.

July 2008: [The Ministry of Justice reveals](#) data on 45,000 people, including criminal records and banking and court information have been lost or compromised in the preceding 12 months, ...

June 2008: A [laptop containing unencrypted details of 21,000 patients](#) stolen from the car of a manager at Colchester University Hospital NHS Foundation Trust.

March 2008: [The Ministry of Defence confesses 11,000 military ID cards](#) have been lost or stolen over the last two years.

February 2008: A laptop bought on eBay is found to originate from the Home Office and arrives containing an encrypted data disc from the government department.

January 2008: Some 600,000 records on members and would-be members of the Royal Navy, Royal Marines and Royal Air Force are lost after [a laptop belonging to the Ministry of Defence is stolen](#).

January 2008: A CD which holds the names and addresses of 160,000 children is lost by the City and Hackney trust.

December 2007: [Northern Ireland's Driver and Vehicle Agency loses data](#) on 7,685 motorists after two CDs containing their details are sent by courier but never turn up.

December 2007: HMRC follows its massive data November breach with the news that [a data cartridge with details on 6,500 pensioners got lost](#) in transit that September.

December 2007: The Driving Standards Agency admits losing more than three million learner drivers' details after a hard disk goes missing from a contractor's secure facility in Iowa City, Iowa.

December 2007: Department for Work and Pensions fails to receive a disk containing the records of 40,000 housing benefit claimants after a West Yorkshire council attempts to courier it to the department clued up.

November 2007: [HM Revenue and Customs admits 25 million records](#) containing the names, addresses, dates of birth and National Insurance numbers of the entire HMRC child benefit database have gone missing...

3. Consequences of breaches:

3.1 Risks are distorted

The effects of this coverage include a distortion of risks – perceived and actual. Perceived risk is increased in the general public by this unbalanced reporting. Actual risk to reputation is now inflated because the media fever-pitch reporting of every data loss causes the general public to believe that organisations have put them at risk. If risks are distorted, then real risks cannot be properly managed.

3.2 Wrong countermeasures applied

Distortion of risks concentrates attention on countermeasures that may actually make us all *less* secure in reality. For example it is now advocated, by the Government amongst others, that physical transfer of data is less secure than electronic transfer and should not be used. But it simply is not true that the risks from physical transfer of data are in all cases lower than any method of electronic transfer of data. It is true that electronic attacks (sniffing, misrouting) are often invisible, whereas loss of physical media leaves a smoking gun for newspapers. So risks to reputation may be reduced by sticking to electronic transfer but real risks to individuals are *increased* if all data is transmitted electronically without due regard to security. And the fact is that measures such as splitting data into two physical parts, use of two randomly chosen, vetted staff as couriers and strong encryption can make physical transfer more secure than many forms of electronic transfer.

4. Too much information governance

Good information governance requires that every countermeasure implemented actually reduces total risks. Here are some myths that show too much governance can lead to increased risks:

- **“Holding less information is more secure”**: This can be true, but is not always true. It is necessary to consider what risks may flow from information not held as well as risks to information held. For example, if a bank lends money without knowing the true total debt of the applicant, then the bank is increasing its overall business risk in order to decrease a smaller information risk.
- **“Keeping tight reign on information increases security”**: There are many examples where this is not true
 - The real need is to balance all kinds of risks – operational, security, debt, fraud etc. Too tight a control over information can make operational processes inefficient or inherently more risky, increasing costs, decreasing profitability and overall increasing total business risk. A tragic example is that of Ian Huntley, where information about his past was held back due to an overzealous application of part of the Data Protection Act, and increased the risks to children in Soham.
 - Too tight a control over information can also lead hard-pressed staff to bypass controls altogether. Better to have some security fully supported and upheld by staff than tight security widely bypassed. An example found its way into the press from the NHS, where South Warwickshire General Hospitals NHS Trust encouraged hospital staff to share login credentials because login times using the high security smart card authentication were too slow and jeopardised the ability of the hospital to look after its patients. So, tight information security increased risks overall.
- **“If I have security breaches, I need to tighten procedures”**: in fact, most of the headlines above are not as a result of poor procedures, they are a result of procedures not being followed. So tightening procedures will incur great expense and not improve security at all. Monitoring and ensuring compliance will often pay higher dividends than tightening procedures and paying for expensive electronic security devices.

5. Better national approach needed

And finally, there has been no real national debate over why loss of names addresses and other details puts any individual at risk in the first place. Even if I know your name, bank account details and date of birth, it just should not be possible for me to withdraw money from your bank account or take out a loan in your name. Because the truth is that many people already know this information about you – your employers past and present, your mortgage company, utilities, children’s schools and many more, never mind any loss of data by Government or banks.



So, we should ask ourselves:

1. What proof of identity and authentication should be used before incurring a debt in the name of a citizen? And what verification processes would be appropriate? If a big loan is to be taken out in your name and using your correct address (thereby making you liable for repayment), shouldn't this at minimum be notified to you at that address for your confirmation, ideally requiring the use of a pre-arranged password, before the loan is granted?
2. If you have a genuine reason to protect your whereabouts from general knowledge, shouldn't *all* of Government, and big business, remove your address details from general access? But at the present time, each and every Government database operates a different policy for shielding personal records. Servicemen's family details are protected in some databases but not others. How does this protect the individuals?

6. Conclusions

Now is not the time to introduce draconian security processes, now more than ever good professional balance is needed to identify real risks realistically and to apply countermeasures that will reduce risks in practice.

Now is a time for everyone to find ways to ensure that disclosure of personal data cannot lead to serious consequences for individuals – by requiring strong authorisation before financial commitments are agreed, and by acting together to ensure that individuals who live their lives under physical threat should have their whereabouts comprehensively protected across Government and other major institutions.

Contact Details

Andrew Cooke
Director - Intelligence and Homeland Security
ATKINS

Tel: 01242 546 211
E-mail: andrew.cooke@atkinglobal.com

Atkins provides professional, management, business and technology-based consultancy and support services. We are the largest multidisciplinary consultancy in Europe and our greatest asset is our rich diversity of skills. Our significant capability has been acknowledged by the Management Consultancies Association (MCA) who rank us as one of the top 20 providers of Management Consultancy services. Atkins is the partner of choice for the successful delivery of challenging business outcomes.

Working with organisations across the public and private sectors, we provide advice and support to enable our clients to deliver their strategic objectives. This can take many forms from working as client friend through to working as partner in the delivery of significant change programmes.