

Putting privacy on the map

(This article was originally published in The Compliance Institute Gazette, Issue 176, April 2010)

Recent press releases issued by the Information Commissioner's Office, (ICO), indicate that however seriously organisations may take privacy, data protection and information security, human error remains a significant cause of a large proportion of data breaches publicised.

In February, for example, an employee of a mortgage company inadvertently emailed the records of 15,000 clients, including information about individuals' arrears and possession proceedings, to a member of the public whose email address was similar to that of the intended recipient. In the same month, an employee of a professional association lost a laptop and memory stick containing unencrypted data including the names and personal details of more than six thousand professional members whilst his back was turned and he was loading his car.

In January, an NHS Hospital Trust employee left an unencrypted laptop containing the records of 33,000 patients in an unlocked and unattended vehicle. Also in January, the Chief Executive of a county council signed an undertaking to introduce formal procedures for the disposal of office furniture and equipment after social work records containing sensitive personal data relating to several individuals were found in a filing cabinet purchased second-hand by a member of the public.

Which of us, I wonder, can put our hands on our hearts and honestly say that we have never sent an email to the wrong person as a result of misspelling the address of the intended recipient, only to discover our error *after* we have 'hit' send; or who have not put down valuable belongings on the pavement beside our cars as we load the boot. Most of us have been lucky in these circumstances! No loss has occurred, no damage has been done and the worst we have suffered from such lapses in our personal behaviour is embarrassment. Those responsible for the breaches reported above have not been so lucky and as we ponder their fates, and the fates of those who may have fallen victim to financial crime and identity theft, and the deep distress that can be caused when personal information falls into unscrupulous hands, we can probably recollect times when we may ourselves have been responsible for some near misses!

Raising awareness of information security and data protection remains a priority for many privacy practitioners. Two reports published in March 2010 may help information security, risk, compliance and other professionals to prepare business cases which set out for their Chief Executives and Board Directors, the costs and benefits of developing and deploying coherent and cohesive data protection strategies and plans, including the design and delivery of high quality, effective and behaviour changing employee training.

'Business Case for Data Protection',¹ published by The Ponemon Institute, documents the results of primary research carried out in the UK across 16 sectors ranging from financial services to education and from retail to professional services. Ponemon conducted interviews with 115 senior managers, of whom 28 were chief executives. Deliberately, none of the participants in this research were practitioners in privacy. The research listed 22 different data protection efforts, and showed which were regarded as very important or important by chief executives and senior managers allowing comparisons to be made across both participant groups. With an understanding of what is important to CEOs, it is assumed

that managers preparing business cases to develop and execute data protection strategies and plans, will be better able to secure Board approval.

For both CEOs and senior managers, data protection efforts regarded as most important were the need to: reduce potential security flaws within business-critical applications; develop a data protection strategy for the organisation and identify; and respond to data breach (loss or theft of personal information).

CEOs and senior managers placed little importance, however, on the need to perform background checks on employees, temporary employees and contractors. Whilst malicious intent appears to account for very few data breaches, it is costly to firms when small numbers of employees engage in the large scale defrauding of their companies. It is therefore surprising that emphasis on background checks is considered so unimportant.

With technology solutions seemingly more important to CEOs than training, (only 58% regarded training employees, temporary employees and contractors as important), this poses a challenge for privacy professionals at a time when human error remains the cause of such a large proportion of data breaches; how to raise the need for employee training up the agendas of CEOs and their Boards. For Boards requiring robust business cases, (probably the vast majority), before agreeing to investment in data protection efforts in general and training initiatives in particular, turning to hard evidence may help professionals overcome this challenge.

Statistics from the ICO² updated at the end of January 2010 indicate that 56% of all data breaches reported since November 2007 are the result of lost or stolen hardware or data, 23% arise through the erroneous disclosure of personal information, 6.5% arise when data is lost in transit, and 2.5% arise through non-secure disposal of data. This hard evidence is very much in line with Poneman's research results. These revealed that CEOs and senior managers interviewed saw lost or stolen computer and / or flash drives as posing the biggest risks to data protection alongside cyber crime and insecure disposal of storage media. All of which suggests that organisations can baton down the hatches by securing their technology, and raising their guard against cyber crime and malicious e-attacks, but if they do not make people more aware of what they have to do in their jobs to protect personal information they are leaving their defences wide open to breach as employees leave laptops on kerbsides or on trains, or email thousands of clients' records to members of the public!.

With Ponemon's 2009 research in the UK³ indicating that the average cost to an organisation of a reported data breach was £1.73m, (ranging from £160k to £4.8m) and an average cost per record breached of £60, little should serve better to concentrate minds on what seems to be a gaping hole in data protection strategies, ie a general inadequacy in existing raining provision. But there is an upside! According to Ponemon's UK research, the return on investment in data protection is a 'healthy' 5.8:1, (that is, for every £1 spent on data protection, there is a £5.8 value improvement in the business, through, for example, improved brand reputation, improved information flows about people, increased customer trust and reduced churn, etc), a somewhat better return than is the case in the US.

But perhaps before privacy professionals engage in a stakeholder engagement exercise with their top management, we should also note that CEOs in Ponemon's 2010 research did not perceive customer and consumer information as being relatively critical to business operations compared to other data types. Indeed, it was ranked lowest out of six believed to be critical to business operations. The highest priority was felt to be financial information,

closely followed by intellectual property and non-financial confidential information. Employee information was ranked in fourth place, and business customer information in fifth. This, according to Ponemon, is in stark contrast to the findings from similar research conducted amongst US CEOs and senior managers. That research showed US CEOs ranked customer or consumer information as being much more critical to business operations. If the value of customer and employee information is perceived not to be as critical to business operations, little wonder that UK CEOs, according to this research do not place a higher priority on employee training. Placing value on customer and employee information is therefore at the heart of raising their importance in the eyes of CEOs and their Boards.

That is why the second report, published by the Information Commissioner's Office, (ICO), is so important. This report boldly asserts that 'privacy protection is not a project with a start and an end, it is an attitude and approach that needs to be woven into the culture of the organisation and from there to inform and guide all the 'business as usual' activities employees perform on or with personal information. Cultural leadership cannot be driven from anywhere other than the Board.'⁴

This report acknowledges that placing value on personal information is difficult. It has no easy solutions and, because there is data available on financial losses arising from fraud, its worked examples are based on the average loss per victim of 'financial fraud' of £493, (though this relates specifically to online shopping fraud). It's figure may therefore represent an under-estimate. It nevertheless points to a wealth of references, research and data which may help practitioners to convince CEOs of the value of personal information to individuals, to their businesses, to third parties, and to the wider world, (eg regulators, the police, etc), though it does not answer the question, 'how do you place a value on a patient's medical records' or on a family's social work records?' But to be blunt, we should not expect it to!

The ICO document does, however, provide some useful tools and templates that will surely prove helpful to many professionals as they develop their business cases for raising the protection of personal information up their corporate agendas.

What is certain, is that if things remain unchanged and no greater priority is given to training by CEOs, then sadly, much needed investments in technology will no doubt continue, but we are likely to continue to see further press releases from the ICO announcing yet more data breaches caused by human error.

(Ken Cohen is Director of The Fifth Business Experience Limited, which specialises in the design and delivery of innovative training and development solutions and in bringing regulatory training to life. He can be contacted at ken.cohen@fifth-business.co.uk)

¹ 'Business Case for Data Protection: A study of CEOs and other C-Level Executives in the UK', Ponemon Institute LLC, March 2010, http://www.ouncelabs.com/writable//resources/file/ibm_business_case_for_data_protection_uk_white_paper_final5_doc.pdf

² 'Table of data security breaches notified to the ICO since November 2007' ICO', 26 January 2010, http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet_jan09.pdf

³ 'Annual Study: Cost of a Data Breach, Ponemon Institute, February 2009, http://download.pgp.com/pdfs/whitepapers/Ponemon_COB_2008_UK_090203_2-final.pdf

⁴ 'The Privacy Dividend: the business case for investing in proactive privacy protection', Information Commissioner's Office, March 2010,
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_dividend.pdf