

Information Security – Beyond Regulation

Some thought leadership on implementing data security at work

First published under ‘City Comment’, in The Company Lawyer, August 2009

The initial part of this comment contextualises the legal and regulatory requirements in UK data security obligations. This is followed by a comprehensive insight into the practicalities and common pitfalls that organisations face when embedding their policies, systems and controls on data protection and data security, alongside recommendations to maximise the effectiveness of training and awareness programmes

Background and context

Increasingly, there have been reports in the press regarding data loss and the impact of this on clients and firms. If data protection procedures are not adhered to this may result in commercial, reputational, regulatory and legal action. It is therefore necessary that firms have in place systems and controls to minimise the risk.

All firms should be registered with the Information Commissioner’s Office (ICO), which maintains a public register of the information the firm obtains and the reasons why. This relates to the personal data of individuals as well as staff members of the firm, including curriculum vitae held. Within the past two years, the Financial Crime and Intelligence Division did a thematic review of data-security controls, visiting 39 firms, including 20 small firms. The FSA found that poor data security was a serious, widespread problem across the entire industry. Subsequently the FSA issued a report (April 2008) on the importance of data security, reminding firms that they need to take the protection of customer data with the utmost seriousness, and that firms have a responsibility to assess the risks of data loss and to take reasonable steps to prevent that risk occurring. The FSA requirements can be found in the Senior Management Systems and Controls (SYSC) 3.2.6A states that firms’ relevant systems and controls must be “comprehensive and proportionate to the nature, scale and complexity of their operations”. The secure handling of customer data is also part of the “Treating Customers Fairly” standard that all firms must adhere to.

It is good practice for firms to have procedures in place to investigate fraud and help the customer where appropriate. For example, firms can place blocks or anti-fraud flags on an account, change details and passwords and provide advice to the consumer on how they can protect themselves from further fraud. The Data Protection Act 1998 (DPA) gives legal rights to individuals in respect of personal data processed about them by others. There are eight principles in the DPA that apply to all data controllers who must comply with them, unless an exemption applies. There is also a requirement for a data controller to notify the ICO of their processing of personal data, so the ICO can maintain a public register. The ICO has certain powers and duties under the DPA to ensure that data controllers comply with this legislation. So it is important that firms are aware of their obligations under the DPA.

Therefore, written policies, procedures and guidance are fundamental in ensuring that staff are aware of data security risks and the procedures to tackle those risks. Firms with no written policies, procedures or guidance are unlikely to be training their staff properly and ensuring proper awareness of data security risk throughout their business. However, even the best policies and procedures have little value if front-line staff are not aware of them or do not understand what they mean in terms of their day-to-day responsibilities. Even when firms have detailed written policies, they often fail to train staff effectively and to provide staff with specific courses or coaching on the importance of data security, even on a risk-based approach. The FSA states that many instances of data loss occur because staff do not know or understand relevant policies and procedures. So it is good practice for senior management to put in place appropriate training and awareness mechanisms to ensure that their staff understand the relevance of policies and procedures to their roles. It is important that firms have in place systems and controls to minimise the risk that their operations and information assets be exploited by thieves and fraudsters. Consumers are entitled to rely on firms to ensure their personal information is secure, notwithstanding the fact that consumers themselves are often oblivious to imparting their own sensitive data.

Personal Attitudes and Behaviours

That 60% of people when asked on the street to divulge personal information such as computer passwords or their dates of birth will do so in exchange for a bar of chocolate should make anyone professionally involved in efforts to protect personal information and reduce spiralling financial crime, stop in their tracks. Findings last year from Info security Europe¹ showed that whilst people are becoming more aware of the need to protect their personal information, they continue to give it away to market researchers on the street, sufficient that if it fell into the wrong hands, would significantly increase their chances of falling victim to financial crime. Symantec, the security software firm, drew similar, if not more worrying conclusions from its own research. Symantec found that similar proportions² would not only reveal personal information, but would divulge their computer passwords in exchange for a £5 department store voucher! Moreover, they found that 45% of people interviewed select their birthday, their mother's maiden name or the name of their family pet as passwords, all of which could be relatively easily guessed by those with criminal intent.

How can it be that when the media draws our attention, ever more frequently, to the accidental loss of personal information by banks, building societies, insurance providers, NHS trusts, government departments, and others, we throw up our collective hands in horror, yet as individuals, we continue to treat our own personal information with such disdain?

Perhaps we should not be surprised at this apparent contradiction. If 60% of us place so low a premium on our own personal information that we will willingly give it away, then it is unlikely we will place any greater value on the personal information of our customers or our colleagues when we are at work. Neither should we be surprised, then, that the vast majority of corporate data losses, being accidental, are generally caused by 'ordinary', rather than 'stupid' people; ordinary people for whom the connection between information security and financial crime has not been made. If we are to stem the tide of corporate data losses, training and awareness programmes need to promote changes in our personal attitudes,

beliefs and behaviours so that 'ordinary' behaviour demonstrates far greater respect for personal information.

Typical approaches to training change neither attitudes nor behaviours at work

Yet significantly, training and awareness programmes typically fail to attempt to change personal attitudes and behaviours, preferring instead, to concentrate on instructing people in processes and procedures. Indeed, the FSA recently found that training in financial services firms typically, 'focuses more on legislation and regulation than the risk of financial crime. This means staff are often unaware of how to comply with policies and do not know that data security procedures are an important tool for reducing financial crime.'³ Whilst the FSA's findings were drawn specifically from their review of the financial services sector, they will no doubt resonate for organisations across every sector. When training is focused on the data principles, rules, regulations, statutory obligations, policies and guidelines, it satisfies subject matter experts such as those who work in departments that include Legal, Risk and Compliance, Company Secretarial, Data Protection, Information Security; but these are the very people who are least likely to need training because of their existing subject matter expertise!

Those who most need training are those who operate at the front line of customer and employee service and many of those working in support functions; those who have access to and the means of disclosing, copying and / or transferring personal Information those, for example, working in marketing, sales, call centre operations, payroll, IT; those, who because of the very nature of their work, pose enormous risk to individuals and their organisations, if for any reason they fail to be vigilant in protecting personal information.

These are the people whose job it is to design new products and services, bring in new and profitable business, deliver high quality customer service, whether face to face or through development and deployment of ever more complex technology and systems. These are the people who have stretching targets to achieve and deadlines to meet, who through one uncharacteristic lapse can put us at risk of financial crime and loss of privacy. Yet for these very people, data protection and information security seems dry, dull and legalistic; at best it seems irrelevant to their jobs and at worst, a myriad of rules devised by zealots to thwart them in their achievement of corporate strategies and goals!

If personal attitudes, behaviours and the habits of several lifetimes are to change, a more imaginative and compelling approach to training and raising awareness is required; one that goes way beyond setting up a 'dodgy desk' for staff to look at to identify 'all kinds of poor practice relevant to data security', (as described by the FSA).

A more compelling approach

So, how can we make training and awareness programmes more imaginative and compelling? First, to make them truly effective, we need to re-frame our language. For too long, we have allowed and indeed encouraged a shift away from the personal to the abstract. We talk of data, data sets, databases, data sticks, bits, bytes, DVDs, CDs, secure emails, hard copy reports, schedules, and spreadsheets. This is the language of the impersonal and the abstract; the language is dull, dry and mechanistic. We have

inadvertently de-personalised what is fundamentally about people and their personal security and privacy.

We need to reverse this trend and emphasise the personal. One way of doing this is to focus on consequences; consequences to victims of identity theft and financial crime committed against them, (whether those victims are customers or employees); consequences of disclosing personal information without having diligently and intelligently (rather than routinely) followed identification and verification checks; consequences of failing to fully conduct due diligence of a third party hired to process

our organisations' payroll or pension schemes; consequences of copying personal information for use by developers in systems testing. A focus on consequences helps us to better connect impacts with our own actions and so helps us to recognise our own personal responsibility to ourselves and to others. It also helps us to appreciate that data protection and information security is fundamentally about real people, not just data.

Second, traditional training and awareness programmes are designed to trigger only our intellectual responses. Yet our intellectual selves tell us information security and data protection is a matter of common sense and that we all know what we need to do to protect our customers and colleagues. Unconsciously, we rationalise that because it is common sense and we would never, ourselves, act foolishly, protecting personal information can afford to slip from our personal agendas.

To move beyond this rationalisation, raise the profile of information security and to promote changes in personal attitudes and behaviours, we need to recognise that when a person falls victim to identity theft or fraud, or when privacy is invaded, the initial response is typically emotional rather than intellectual.

Focus therefore needs to be on stimulating emotional as well as intellectual responses. High quality training, communications and awareness programmes consequently replicate, through creative design and imaginative delivery, the range of emotions that victims tend to experience. They focus on the devastation that financial crime or loss of privacy can cause and they raise in people's consciousness how vulnerable they are in their own personal lives to 'attack'. They help people pinpoint what they must do in their private lives. As people begin to place a higher premium on their own personal information, and learn what they can do to protect it, they come to respect the value of their customers' and colleagues personal information and how they can protect that too.

An approach that integrates the personal with the corporate and the emotional with the intellectual has huge impact because it stimulates real change. As an approach, it informs what content should form the subject of training, how it should be treated and to whom it should be targeted. It also reinforces the notion that financial crime is not victimless and, as important, that we all have a vital part to play in reducing it and protecting privacy.

Ultimately, we need to be comfortable telling our people that they should treat others' personal information as they would treat their own, certain in the knowledge that they are rigorous in the protection of their own information and that they do not give it away in exchange for a bar of chocolate or a £5 department store voucher! But as long as 60% of the population continue to hand over their personal information to strangers on the street, our

work is cut out for us and we all of us remain vulnerable to financial crime and invasion of our privacy.

This article was co-written by Ken Cohen and Jason Haines, a leading expert on fighting financial crime

1 'Women 4 times more likely than men to give passwords for chocolate', Infosecurity Europe, reported in The Guardian, 16th April, 2008, <http://www.guardian.co.uk/technology/blog/2008/apr/16/woman4timesmorelikelythan>,

2 'Passwords are an easy giveaway', Research undertaken by Symantec and reported in Which? 26th September 2008, <http://www.which.co.uk/news/2008/09/passwords-are-an-easy-giveaway-157522.jsp>,

3 'Data Security in Financial Services', Financial Services Authority, April 2008