

## **Reducing risk and fighting financial crime: How high quality data security training can change personal attitudes and behaviours**

*(This article first appeared in the Compliance Institute Gazette, Issue 168 in August 2009).*

### **Introduction**

How many people in your organisation make purchases from their mobile 'phones, quoting their credit card details, whilst travelling on a crowded train? How many make what they consider to be secure transactions on computers sited in internet cafes, not knowing whether their every keystroke is being captured? How many have broadband access from their home computers with little if any internet security, firewall, anti-virus, anti-phishing, or spyware protection?

Maybe the answers to these questions do not concern you. After all, what people do in their personal lives is a matter for them. Perhaps your philosophy is to influence those things over which you can have influence, (what people do and the way they do it in the workplace), rather than try to influence those things you cannot, (what people do in their own private lives). This may seem to be a reasonable philosophy; it is certainly one that informs much of the data security training that is widely delivered today.

Yet how people think, what attitudes they have, and what assumptions they make in their private lives, all have significant impact on how they behave in the workplace. People, for example, who announce their credit card details in public places, or who are lax about their own computer and internet usage, may well be doing business, (possibly your business), on trains, on station platforms, in coffee bars, in waiting rooms or even in pubs, divulging personal and maybe sensitive information within easy earshot of others. And according to two studies conducted during 2008<sup>1,2</sup> 60% of people sampled were willing to divulge their personal information and passwords to strangers on the street in exchange for bars of chocolate or £5 department store vouchers. When people place so low a premium on their

own personal information they are unlikely to place any greater premium on the personal information of others, whether they are your customers or your colleagues.

With data breaches on the increase, with many companies reporting multiple breaches each year,<sup>3</sup> and with identity theft and financial crime growing at an alarming rate, now is the time to critically reflect upon the effectiveness of traditional approaches to data security training and to ask whether we have not now reached a point at which we need to engage in a more powerful and compelling training and awareness effort to reduce risk and escalate the fight against financial crime.

### **Limitations of traditional approaches to data security training**

All too often, traditional approaches to data security training rely entirely on triggering intellectual responses from staff within a wholly corporate context. Focus is primarily on statutory obligations, the data principles, rules, procedures, policies and regulations, a focus which the Financial Services Authority noted in April 2008<sup>4</sup> 'does not teach staff about why data security is an essential tool in reducing the risk of financial crime'. Even the language of data, data-sticks, data-bases, bits, bytes schedules, clear-desk policies, locking of computers and encryption is abstract and de-humanising leaving training unnecessarily technical, theoretical, legalistic, dry and dull. People on the 'front-line' dutifully attend routine, generic training, regardless of whether or not the subject matter is relevant to their roles or the level of risk that might be attached to their work. Training is delivered using a combination of PowerPoint slides, handouts and worksheets, and is usually followed by tests which merely test memory of the rules, regulations and theory covered rather than an understanding of their practical application in everyday situations.

Little wonder that whilst such training may satisfy subject matter experts working, for example, in departments such as Legal, Risk, Compliance and Company Secretarial, (those who least need training), it is perceived by many on the 'front-line', (those who need it most),

to be something of a chore, largely irrelevant to them and a distraction that diverts them from their day job when it should be core to the way they work and behave every day.

Such approaches represent the easy option. Little thought is required in their design and they can be delivered at low cost. Yet their effectiveness is now surely at question given that over the last year, the number of UK organisations experiencing a data breach has increased by nearly 17%<sup>5</sup>, that in the financial services sector alone, firms on average report more than three breaches in a year, and public sector bodies each in excess of four.

Something more compelling is required; something that captures peoples' attention and imagination; something that challenges individuals' core attitudes and beliefs so they do not simply throw up their collective hands in horror when another high profile breach is reported by the media, yet at the same time willingly give away their own personal information on the street; something that changes individual and collective behaviours both in the workplace and in peoples' private lives; something that enables us to mount a more effective campaign to reduce risk and fight financial crime.

### **The power of the personal and the emotional**

Put quite starkly, what traditional approaches to data security training miss is that data protection is fundamentally about people. Whilst the theory and the rules and the data devices are important, protecting people, whether they are customers or colleagues needs to be placed at the core of any data security training. When a person falls victim to financial crime, or when their privacy is invaded, their initial responses are neither intellectual, nor corporate. Their responses are emotional and highly personal.

Effective, high quality data security training consequently stimulates not only intellectual but also emotional responses. It emphasises the potential consequences for individuals of accidental disclosure of personal information or of it being lost or stolen; consequences that may include loss of privacy, identity theft, financial crime, and indeed, loss of personal

reputation; consequences that re-create, as far as training allows, the feelings of distress, resentment, anger, devastation and loss of control people experience when they fall victim to financial crime. When consequences are emphasised, a direct link is made back to the actions that may have contributed to them, and brings to the forefront, the importance of personal accountability, (and indeed liability). It becomes possible to demonstrate cause and effect; this behaviour causes that distress and damage.

Injecting the personal and the emotional presents opportunities to be more inventive with training content. It liberates training from the generation of lists of 'do's and don'ts' and from focusing on the technical and the theoretical, and makes it all the more possible to design content around real life situations that have relevance and meaning to people in their everyday work and personal experiences; situations that illustrate what constitutes safe and secure behaviour and what does not; scenarios with which people can readily and easily identify and from which they can learn how better to protect themselves, their customers and their colleagues. And importantly, when imaginative content is designed around real-life situations and scenarios training is a more absorbing and engaging experience which results in longer-term retention and ongoing application of learning.

An emphasis on stimulating personal and emotional responses also opens the doors to deploying a wider range of delivery methods. Whether 'classroom' based or delivered through Computer Based Training, (CBT), content can be conveyed through:

- real-life stories, for example of people falling victim to financial crime and identity theft;
- visual images, (still or moving), illustrating, for example, bad practice when working away from the office, perhaps in a hotel, or in a home office;
- audio / pod-casts, for example of 'blaggers' building identities through a series of calls to unsuspecting call centre agents; and

- personal experiences of participants, drawing on, for example, the steps they take to protect their own information and where they think improvements can be made to protect customers' and colleagues' personal information.

These more innovative approaches to data security training have the effect of reducing the numbers of people who make purchases from their mobile 'phones, quoting their credit card details, whilst travelling on a crowded train and reducing the numbers who make what they consider to be secure transactions on computers sited in internet cafes. When people place a higher premium on their own personal information, when they treat it with greater respect and protect it more effectively, you can be confident that they share your commitment, in both concept and practice, to protecting the information of your customers and your colleagues, and hence the reputation of your business.

(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](mailto:ken.cohen@fifth-business.co.uk))

---

<sup>1</sup> 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>

<sup>2</sup> '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>

<sup>3</sup> 'UK Data Breach Incidents on the Rise'; research conducted by the Ponemon Institute for PGP and reported in 'The A Register', 9<sup>th</sup> July 2009, [http://www.theregister.co.uk/2009/07/09/data\\_breach\\_survey/](http://www.theregister.co.uk/2009/07/09/data_breach_survey/)

<sup>4</sup> 'Data Security in Financial Services', Financial Services Authority, April 2008, [http://www.fsa.gov.uk/pubs/other/data\\_security.pdf](http://www.fsa.gov.uk/pubs/other/data_security.pdf)

<sup>5</sup> 'UK Data Breach Incidents on the Rise'; research conducted by the Ponemon Institute for PGP and reported in 'The A Register', 9<sup>th</sup> July 2009, [http://www.theregister.co.uk/2009/07/09/data\\_breach\\_survey/](http://www.theregister.co.uk/2009/07/09/data_breach_survey/)