

Top tips for improving information security training

According to the Information Commissioner's Office, as at November 2009, 58% of all reported data breaches arose from lost or stolen data or hardware. A further 23% of data breaches arose from the erroneous disclosure of personal information.

However, we should be mindful of the old adage, that 'there are lies, damned lies and statistics'. However much we look at how the majority of data breaches arise, it hardly needs to be said that there needs to be only ONE breach for customers' personal information to be compromised and for business reputations to be tarnished.

Fortunately, firms take their responsibility for training their staff in information security very seriously. But if existing training was fundamentally changing attitudes and behaviours, we would surely be witnessing a decline in the number of breaches experienced and reported, rather than an increase.

The Fifth Business Experience specialises in bringing regulatory training to life, so that it fundamentally changes employee attitudes and behaviours and so that it changes the way they protect personal information in their work and in their private lives.

As we enter a new decade, what top tips can we provide that will help firms to enhance their regulatory training:

- **Make training meaningful and relevant to employees:** most firms tend to focus on work related information security, but if attitudes and behaviours are to be changed, we need to focus on peoples' experience of protecting their own personal information and the value they place on it.
- **Make training personal:** information security, like so much regulatory training, is typically seen as a chore, something that has to be repeated each year and then be forgotten until the following year! Since information security is about the protection of people by people, reducing it to bullet points and slideshows, whether delivered face to face or through computer-based training will do little to raise it up the individual or collective agenda.
- **Link actions to consequences:** often, firms will convey to employees the consequences that are likely to follow a data breach. The firm will be investigated; it may be subject to a fine; there is likely to be reputational damage; if it is found that an employee was negligent following training, s/he may face disciplinary action. Yet rarely do firms focus on the consequences of data breaches for customers; distress; cost of putting things right; damage to personal reputations if credit ratings are temporarily compromised, etc. Since all employees are customers of one firm or another, getting them to put themselves into customers' shoes is a simple, yet powerful way of making them about the consequences of their actions.
- **Use stories and scenarios:** stories provide a framework through which training can be delivered in a 'true-to-life' context and allow us to communicate what people should and should not do in their work and personal lives to protect personal information without preaching or lecturing.

- **Emphasise that breaches arise due to the actions of ‘ordinary’ rather than ‘stupid’ people:** most data breaches occur not because people are stupid, but because of an individual’s momentary lapse, whether they are under pressure, or trying to meet a deadline, or simply acting without thinking of the consequences. Few will identify themselves with ‘stupid’ people, but most will be willing to recognise their own behaviours in others, if the examples presented to them are of the actions of ordinary people – people just like themselves.
- **Make training interactive and participative:** the more people must do in their training, and the more they must think about how they would act in real life situations, the greater the likelihood they will transfer their learning into their ordinary, day to day, work environment.

For information about how The Fifth Business Experience can help design and deliver innovative, compelling, yet cost-efficient training that will have lasting benefits and will minimise risk, whether delivered face to face, or through e-learning platforms, email enquiries@fifth-business.co.uk or telephone 020 8907 2333.
