

Stories: a powerful training tool to raise information security awareness

(This article was originally published in The Compliance Institute Gazette, Issue 173, January 2010)

Do you know the story of John and his laptop? Not sure? Well, let me tell you about it now!

Whenever he thought about it, which, now that he had time on his hands, he did pretty much every minute of every day, John couldn't help but wish he could turn the clock back. Once, not very long ago, he had been a successful senior executive. Exceeding all his targets, he had always been well regarded by everyone in his firm. Yet this had suddenly come to an end leaving him financially and emotionally devastated.

The day it happened had been much like any other. Well, maybe not! After all, it wasn't every day that you closed such an important deal. Reflecting on his success as he sat back in his seat on the inter-city train, laptop open on the table in front of him, fingers dancing over the keyboard and USB memory stick plugged into the side, John realised he had not tasted a hot cup of coffee for hours. Suddenly, he felt very thirsty. The buffet car was just a couple of coaches down; he'd quickly grab a coffee and a snack and be back in his seat in just a few moments. As John rose from his seat, he leaned over to the passenger nearest to him; an elderly, respectable looking man, dressed in a heavy overcoat.

"Would you mind just keeping an eye on my laptop?" John asked.

"No problem at all!"

"Thanks! I'm only going to the buffet. 'Be back in the next couple of minutes!"

With that, John hurried away, leaving his laptop lying open on the otherwise empty table, save for the USB stick still inserted into the port.

When he arrived at the buffet, there was a queue. One of the passengers in front of him seemed unable to find the right change. As John waited, the train slowed, pulled into the next station and came to a halt at the platform. The minutes ticked by, the train moved out of the station and it was some ten minutes before John returned to his seat.

He thought maybe he was in the wrong coach, but no it was, indeed Coach C. Maybe he was at the wrong table? None of the passengers around him seemed familiar. But there was his coat on the seat opposite. So where was the elderly gentleman who had promised to look after his laptop? More important, where was his laptop? And where was his USB stick containing the personal information of thousands of customers?

John's story has been invented for the purposes of this article, though most of us probably know someone like John; someone who, in spite of their intelligence, common-sense and reliability, unwittingly leaves themselves, their customers, their fellow employees and their employer exposed to risk through their actions, because they just do not think about protecting personal information.

No matter how unflinchingly we put the fictional John, and the real people like him, through annual training, (which invariably they pass), we know fundamentally that their attitudes

towards information security have not changed and that they leave individuals and organisations at risk as a result of their actions.

The traditional approach to training relies on telling employees about the legal frameworks, the rules, regulations, controls and systems they must follow, what they should and should not do, and occasionally, the ramifications for employees if they fail to comply. There are two problems with this approach; first, whilst it is a very rational approach, it ignores the fact that protecting personal information is about the protection of people by people; and second it depends on 'pushing' information out to employees – information they have probably had many times before, (and ignored) – rather than drawing them in and getting them to reflect on their own behaviour and what needs to be modified.

Integrating stories into training programmes overcomes both these problems.

1. Stories provide a framework through which training can be delivered in a 'true-to-life' context. Life itself is not simply a series of unrelated actions that occur one after another with little, if any connection between them and so the protection of personal information should not be reduced to a series of bullet points on slides or on e-learning platforms. Stories 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 and they encourage employees to think for themselves. According to Live and Rietz,¹ 'story is a way of knowing and remembering information – a shape or patten into which information can be arranged. It serves a very basic purpose; it restructures experiences for the purpose of "saving" them.'
2. If employees are to change their attitudes and behaviours towards information security, they need to be able to be able to reflect on the actions of ordinary, believable individuals; people like those they know. When stories reflect the actions of ordinary people, employees recognise themselves in those stories and are able, without loss of face to recognise their own behaviours, challenge them and modify them. Conversely, stories that are about foolish people are generally ineffective; employees, not unreasonably, will not identify themselves with foolish people and their own behaviour is likely to become even more ingrained.
3. But it is not simply a question of providing a framework, or telling stories of ordinary people. The situations described in stories also need to be ordinary. As we enter a new decade and the pace of life grows ever faster, which of us has not observed people working on their laptops during long train journeys, screens open to any other passenger to view, sometimes left, with other valuables, unattended? Stories that convey everyday activities, such as working on a laptop on a train, the ordinariness of which we typically fail to consider, help employees identify with and recognise situations and begin to reflect on how they would and should behave in those situations themselves.
4. We can (and should) 'lock down' IT, systems and controls; yet most breaches occur as a result of some kind of momentary lapse. Virtually every high profile data breach reported over the last two years has been the result of a lapse on the part of an individual; there are those who placed laptops on the floor as they checked out of their hotels, only to discover their laptops had been stolen from in front of them; there are those who left USB sticks storing sensitive information on 'planes; and those who have left sensitive hard-copy reports on commuter trains. When we discover in a

story that a high-performing individual, valued by his employer, his colleagues and his team is susceptible to that momentary lapse, it helps us to realise that that uncharacteristic lapse could just as easily have been ours and prompts us to reflect on how we can ourselves avoid such lapses.

5. Regardless of whether training is conducted face to face in 'classrooms', or using other e-learning platforms, because stories pre-date even language itself and are 'the oldest form of propagating information',² we can use them to our advantage to make training stick. Good stories are naturally absorbing and they have the power to make human what has traditionally been given very abstract treatment.
6. Quite simply, there is no area of company policy, statutory duty, procedure or control that cannot be conveyed in a meaningful story that resonates for employees.
7. All our actions have consequences; stories convey far more effectively the consequences of our actions, than do warnings that employees may be held personally liable for data loss.

Perhaps consequences then, presents a good place to conclude. Because, of course, John's is not the only story to be told. Since actions can have far-reaching consequences that we may not immediately see, let us now turn to Cathy's story:

It was a bright, though crisp December morning, just in the run up to Christmas, when Cathy hurried along the high street to the cashpoint. She really couldn't afford to take the morning off work; it was difficult enough as it was to make ends meet, but as it would be the first Christmas they would spend together, this was a sacrifice worth making. Cathy would draw cash from her account and together with careful use of her credit cards, she would buy presents for all her family.

She tapped in her PIN number and waited a moment or two. Unexpectedly, a message popped up on the screen in front of her. No money in her account. As the morning went on, her credit and storecards were refused, and after 'phonecalls to her bank and card provider, it became clear she had been the victim of credit card fraud. Of course, Cathy would never know that her personal information was stored on the USB stick which had been stolen from a train, along with a laptop, after a high-achieving executive had left it unattended in a momentary and uncharacteristic lapse. She wasn't held responsible for the financial losses; she had, herself, not been negligent; but by the time she had sorted out the mess and had funds available again, a very memorable Christmas had been and gone – though it was memorable for the disappointment and distress caused than for the joy of giving and receiving presents by the tree.

(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 Live, N.J., and Rietz, S.A., 1986, 'Storytelling: Process and Practice', Littleton, CO: Libraries Unlimited, Inc.

² Samuel, Alan, 'Storytelling is magical – so make it part of training', Training and Coaching Today, Feb 2007, p20