

OF ALL THE ISSUES THAT IC PROFESSIONALS HAVE TO COMMUNICATE, FEW CAN BE AS DRY AND TEDIOUS AS SECURITY. HELEN WILSON EXPLAINS WHY – PARTICULARLY NOW – THE MESSAGES ARE SO CRUCIAL AND LOOKS AT WAYS TO SPICE UP YOUR COVERAGE

HOW TO SECURE READER BUY-IN

I can almost hear the collective groan at the mere mention of the words 'security issues' but please stick with me.

Security has never been more critical than during this economic downturn but people have had far more pressing issues on their minds – like keeping their jobs.

It means the focus on security procedures has reduced and, as a result, breaches have increased.

"I have yet to meet a computer that has committed a crime," are the immortal words of Martin Smith, chairman of The Security Company.

Most security incidents can be attributed to human error. Companies spend thousands of pounds on state-of-the-art technology to secure their assets, yet if their employees are not security conscious it is futile. Invariably it is human behaviour that causes security failures time and again – desks that aren't cleared of documents and equipment at the end of the day, computer screens that aren't locked when left unattended and files that aren't encrypted.

Don't get me wrong, this usually isn't intentional. We all want to do the right thing. It's just that it simply doesn't cross our minds.

Criminals rely on this type of behaviour and target businesses, especially during a recession when their defences are down. Sadly, at times such as these, it is also not uncommon for redundant employees to sabotage companies in acts of revenge.

So how do we, in internal communication, ensure that we not only convey the security messages needed to protect our companies but that we do it in a way in which employees will actually pay attention?

It's the million-dollar question.

As always, the first port of call is to put ourselves in the shoes of our audience and ask 'what's in it for me?'

Employees don't care about making sure that their computer screen is locked every time they leave their desk but they do care about what their children are looking at online. It is imperative that we address the issues that not only affect us as a business but affect people on

a personal level as well. If people can relate to the security issues that we communicate, they will be far more receptive to them.

The next step is to create this personal element or 'hook' as a way of engaging the audience. Using a compelling strapline helps as it grabs the attention of the reader and puts what you are asking employees to do in to context. For example: 'you wouldn't leave your home unlocked, so why would you leave your computer unlocked?'

It is also effective to use shock tactics such as emotive headlines that make people stop and think: 'Business travellers lose more than 12,000 laptops per week in US airports – www.dell.com. That's a pretty sobering statistic and exactly the sort of thing that will encourage most people to read on.

Now the real challenge – how to make security humorous? As ridiculous as that sounds, it isn't beyond the realms of possibility and it really works! If employees can actually get enjoyment from your security campaigns, the more successful they will become.

ANIMATION: One technique that has proven very popular is the use of a cartoon animation. It consists of a 'hero' and a 'bad guy' both drawn in a way that doesn't resemble real people but as cartoon figures acceptable across all cultures. The premise is that the hero gets into entertaining scrapes caused by his own bad security practices or by the bad guy's security breaches.

For example, the hero lets the baddie tailgate through an access control point using his pass; he then gets trampled by a stampede of people who are also trying to tailgate. The aim is for it to be humorous and light-hearted but with a key security message and, most importantly, nothing like what people expect to come out of the security department.

The key to success is ongoing security communication campaigns that are engaging and informative. They need to be regular enough not to lose momentum, but not so frequent that they become routine and ignored. Strive to be different and ground-breaking in the way that you communicate security.

You might even find that you enjoy it.

No really, I'm serious; security can be a fascinating subject. Just look at how often it makes the headlines nearly every day. The general public have a vested interest in a lot of the breaches that take place, especially when they involve banks or government departments losing their personal data. Discussions and debates over these stories fill column inches for weeks afterwards. If you think communicating security is difficult now, wait until you've had a breach.

The worst possible thing you can do is to wait until a breach occurs: the only recourse then is damage limitation. Recognise the consequences that a breach could have and how it could have been prevented if your employees had been given regular information.

I appreciate that internal communications teams are under pressure from departments, all with their own arguments as to why they require your services the most, so why should security jump the queue? Some of the following headlines might explain:

- » **Nationwide fined £1m over laptop theft security breach**
- » **HMRC data breach affects 25 million**
- » **TJX counts continued cost of data breach – Firm pays out over \$500,000 to affected banks**

The consequences of a security breach, as some of you may have experienced, are loss of reputation and customers; having an impact on profits and possibly resulting in redundancies and low morale.

Communicating under these conditions is no mean feat and I urge you to discuss these issues with your security department and consider how you can work collaboratively to ensure that you don't fall victim.

The security department often has a poor public image, as employees sometimes perceive it to be overbearing and obstructive to normal working life. However, the job it does is essential to the continuity of business and it needs your assistance to ensure the security message is received and understood. Security has potential to be the most talked about area of business for all the right reasons. Are you up to the challenge? ➔



ILLUSTRATION: STEVE MAY