IT'S A CULTURAL THING

Awareness of cyber threats is one thing, but increased security from change will only come from a cultural shift, say **Simon Borwick** and **Lushin Premji**

A recent report by Juniper Research found that 74% of the UK's small and medium-sized enterprises (SMEs) believe they are safe from cyber attacks. This contrasts with half of these SMEs that have admitted to having sustained such a breach, two thirds of which occurred in the past 12 months.

Many small businesses say that their people are their greatest asset, yet often people also represent their greatest source of cyber risk. PwC's *Global State of Information Security Survey* showed 51% of the worst security breaches reported stemmed from an initial human error, 28% caused by current employees. There have been a number of recent examples that have started with an employee inadvertently making a mistake resulting in widespread and high-impact consequences.

The so-called 'human firewall' is therefore a vital defence in every organisation's cyber armour. This is especially significant for smaller enterprises, where significant investment in technology to reduce the impact of human error may not be feasible. With stretched margins and considerable uncertainty affecting investment decisions, how can SMEs upgrade their human firewall to make their people the first line of defence against a cyber attack?

AWARENESS VS CULTURE

Building a cyber-resilient workforce requires two things: awareness in each individual employee and a culture that drives them towards the right behaviour. Culture and awareness are not the same thing, but both are necessary. Awareness can be defined as having knowledge about a series of facts or assertions. For example, you and your family may be aware that they each should be eating five pieces of fruit or veg each day. However, if the culture in your family doesn't reinforce and encourage acting on that message, then despite that awareness your children may wilfully eat fewer (maybe they don't like vegetables and don't understand its importance) or simply fail to do so (perhaps they are not reminded or rewarded for doing so).

Traditional approaches to improving the human firewall have focused on awareness, often through mandatory training, poster campaigns and so on. But that misses the point: we may know that we should eat our five-a-day, we simply don't care enough to do it! An awareness programme can be implemented quickly through a variety of techniques, many of

which can be low-cost. The challenge is then to follow them up with meaningful cultural change.

MODERNISING YOUR SECURITY AWARENESS METHODS

There is often little space for expression, emotion and engagement in cyber security, yet they can be powerful, low-cost approaches. Guerrilla marketing and storytelling should be embraced by those responsible for educating their employees about cyber security. Guerrilla marketing is all about surprising employees and disturbing the norm of routine. These concepts can be combined with any security message you want to raise awareness of.

For example, we recently visited an organisation where the mirrors in the lifts bore the message: "You look great; but you'd look better if you were wearing your security pass!" The phone number of the IT helpdesk where phishing is reported could appear where employees least expect it, such as on the apron of kitchen staff, or on the cups at the water cooler. The key here is thinking differently, thinking outside the box to go against traditional organisational norms.

Storytelling is another powerful concept that can raise awareness by helping employees understand the consequences of taking certain actions. Many organisations have a list of cyber security dos and don'ts, but providing context behind these instructions through stories makes them even more powerful. Instead of instructing employees not to click on a phishing link, explain to them what could happen when they do so, perhaps also using a personal example of how phishing can relate to their own private lives.

Positive reinforcement goes a long way in strengthening a security culture. Employees should be recognised when demonstrating good security behaviours

BUILD A CULTURE THAT BREATHES SECURITY

SMEs tend to be entrepreneurial and innovate very quickly in order to grow. But a strong security culture requires frameworks and planning, which may be seen as running contrary to that agile spirit. The keys to building a secure culture lay beyond simple awareness. Employees must understand why cyber security is important, believe they can have an impact and want to behave securely. Highlight key behaviours you want within your culture, such as expecting all employees to take care of your customers' data. Applying positive behaviour surrounding personal data to business culture can be done by showing how this behaviour allows everyone in the organisation to achieve both corporate and personal aims and objectives.

In a recent *Audit insights* report ICAEW noted the need for boards to set the tone from the top. This requires support from both informal and formal leaders explicitly – not just in what they say, but in what they do. Employees must begin to see the behaviour as an intrinsic part of "the way things are done around here". The counter to this is that "good behaviour" must be made as easy as possible. Look at your key business processes and ask how you can remove barriers and obstacles to doing the right thing.

Positive reinforcement also goes a long way in strengthening a security culture. Employees should be recognised when demonstrating good cyber security behaviours. This reinforcement could be a simple thank-you postcard signed by their team leader's manager when an employee reports a phishing email, for example.

Finally, look to remove perverse incentives. For example, if a key performance objective within your organisation is on throughput of a particular process, then look for any shortcuts which might be insecure, and provide tools or techniques that make acting securely easier than not so that employees are not unintentionally penalised for behaving securely.

MEASURE AND SUCCEED

Measurement is key to ensuring the effort you pump into your security awareness or culture programme delivers benefits. Most companies start by monitoring pass marks within elearning modules, but most fail to use their elearning platform to its full ability. For example, rather than monitoring a simple pass mark, it might be more informative to monitor which questions employees are getting wrong and which answer is the most wrongly selected. This will allow you to target your training and make your programme one that targets cultural or awareness blind spots.

Context is also crucial, and a security culture dashboard can be helpful. For example tracking lost devices, reported incidents and results of phishing tests are a good start. The power of a dashboard multiplies when metrics are combined, for example comparing those who lost devices against the score that those participants gained within the elearning, mapped to which departments these individuals reside in. Some friendly rivalry between teams can be constructive provided it is managed in the right way.

Security awareness is something that can be implemented fairly quickly as long as you have plenty of imagination, understand your workforce and are able to take all departments with you. Changing security culture, on the other hand, requires a long-term effort from your entire organisation – from boardroom to basement. Integrating security into your DNA is an imperative for SMEs who want to avoid the risk of being one of the 50% likely to have a breach in the next year.

51%
of the worst security breaches reported stemmed from initial human error

28%
of which were caused by current employees

74%
of the UK's SMEs believe they are safe from cyber attacks

Simon Borwick, director, cyber security practice, PwC London
Lushin Premji, cyber security culture and awareness team, PwC London

GETTY