# Security Culture is a People Game

Your people are the first line of defence against a cyber attack. According to **Lawrence Hay**, Principal for People and Talent at PA Consulting Group, leaders need to engage them in order to mitigate risks

For many people, cyber security means either stopping radicals from bringing down the Government or watching an overpriced anti-virus system scan a document. We can't relate to the first scenario and the other is a hassle. As a result, many people don't give security enough thought in their daily lives.

Witness the rising number of people who bring their own devices to work – or, who work from home or from coffee shops, connecting to remote servers and sharing documents on the cloud. Our digital thumbprint has grown and we now have more to lose.

A poor security culture can present huge risks for a company. Not only does it come with hefty fines from the Information Commissioner's Office, but the loss of trust and brand reputation can be fatal. And it can come at any time – take the hacking of Ukraine's power plant or the cyberattacks on Sony PlayStation and TalkTalk as evidence.

Much of the advice on building a good security culture is esoteric: get buy-in from the top, build it into your values and so on. While relevant, they don't get to the heart of culture.

Behavioural change isn't defined by one-off activities and long-winded process documents, it's about people >

regularly connecting with it. By making it interesting and a part of their lives, people will engage.

Here are five things you can do right now:

## 1. Bring in the Big Guns

Security often rightly falls to the information or ops lead. But to establish a new culture you also need to involve the 'people' people – change managers, behavioural experts or natural influencers who quickly create cultures in your organisation.

Just having security folks involved will segregate any initiatives immediately into 'them' not 'us'. Pull together a crack team of leaders, technical experts and people specialists. Get others involved and make the team as diverse as you can.

## 2. Engage Emotional Brains

Promoting security via a few office posters won't get you far. In fact, nothing will if it isn't relevant to people. Run a culture survey to understand your people's values and build a communications campaign that speaks to them emotionally.

Case studies, discussions and storytelling are good conversation starters, while impactful videos enable people to empathise with the implications. For example, you could send a fake phishing email to the company and then report back the findings – 'Only 14 per cent of people passed this onto IT security – why didn't you?'

## 3. Build Habits

People don't change overnight and beating them over the head with a large security manual isn't going to help. Change comes down to habits; the culmination of small everyday individual actions can greatly impact organisations.

Building new habits is about practising regular activities so that they become subconscious. To do this you need to build it into a routine and keep on top of it. For example, the Pentagon's hacking was caused by employees failing to change their passwords from the default 'password' setting.

## 4. Make Everyone an Expert

It's easy to think that security belongs just to those tech gurus hidden in a darkened room somewhere.

People are more likely to work towards a goal if they feel they have knowledge of the risks, so empower your people to own their security. Use champions to run workshops during which teams think about impact scenarios, from the mundane to the extreme.

For example, what if a competitor stole your secrets or what if vital customer information were leaked? Make it an interesting experience that is done regularly and part of business as usual.

Consider running hackathons so your tech stars can attempt to crack systems and plan mitigations.

## 5. Prepare for the Difficult

While it's important there's an element of fun, the organisation's preparation for security breaches is paramount. Scenarios, escalation processes and responsibilities – from the CEO right through to the graduates – need to be clearly mapped out and publicised. Make it clear what a breach is, what the consequences are and what to do if one happens.

Train your line managers to have courageous conversations and keep on top of it. In particular, international organisations should consider how they tailor their approaches in different organisational and national cultures, from the highly autonomous to the stringently authoritarian.

Many organisations believe they have a security culture in place. But it's one thing to have a plan on paper and quite another to ensure that everyone regularly thinks and acts on it. ■

This article was originally published on PA Consulting Group's website. Find out more here

**Lawrence Hay**
Principal, People & Talent
PA Consulting Group

Lawrence works in PA Consulting's People & Talent group. He is passionate about creating people-based approaches to help companies build their future. He has a background in occupational psychology and strategic consulting where he has worked with executives and teams to manage their talent, grow their leaders, and build innovative learning approaches.

Contact Lawrence through:
www.criticaleye.com