blue goose

YOU'LL GET THE SECURITY BREACH YOU DESERVE IF YOU DON'T INVEST IN YOUR EMPLOYEES

Despite the significant effort that governance, compliance and security functions put into managing information security, employees often remain the weakest link in an organisation's defence.

Yet employees are also capable of being the strongest line of defence: indeed, even a basic level of risk awareness and understanding can prevent simple lapses in control that are often the root cause of breaches. And well-informed and motivated employees are capable of creating a security environment that is based on commitment and not just 'compliance'.

Employee awareness, communication and engagement have a critical role to play in achieving this. However, this is not simply a matter of better 'internal marketing'. Neither is it an annual skip through the compliance training module: organisations need to make both a rational and an emotional connection with their employees and move them along the "message received > understood > acted upon" continuum. Put simply, they need to take a strategic approach to engaging their employees.

blue goose help organisations develop employee awareness, communication and engagement programmes that focus on three requirements to ensure their guard is up:

- **INFORMATION:** they know what to do – they have the essential understanding about what they should do to deliver their contribution;
- **EDUCATION:** they know how to do it – they have both the competence and confidence to perform the necessary skills and behaviours that will deliver the required outcomes;
- **ENGAGEMENT:** they know why they should – they have the motivation to perform the information security tasks and activities required of them.

Here are ten internal communication tips to help turn employees into a staunch line of defence.

ONE/TAKE A STRATEGIC APPROACH

Being strategic means aligning information security with your broader business-wide objectives (including your mission, vision and values) and integrating employee education efforts (such as e-learning) with your communication programme. It also means checking that what you ask employees to do is actually do-able, and that infosec messages complement – rather than contradict – other messages. For example, if your sustainability team encourages employees to recycle paper whilst the information security team advises them to shred it, employees will be caught in the crossfire of two competing messages. Join it all up at the start, and everyone will appreciate it.

FIVE/TELL THEM WHY

Employees need to understand the risk, their role and the actions they should take. But unless you provide them with the right motivation – why infosec matters – your communication could fall on deaf ears. So before you provide specific guidance around the risks and what to do, make sure you tell employees why it's so important to both them and your organisation.

TWO/KNOW YOUR AUDIENCE

Different employees will face different information security challenges – PCI for customer-facing teams, data protection for HR, and so on. Before you start communicating to anyone, find out who needs to know what. Then explore the security culture in your business - are there are any particular blind spots or recurring patterns of behaviour? Understand this, and your communications planning can begin.

SIX/MAKE IT ACTION-ORIENTED

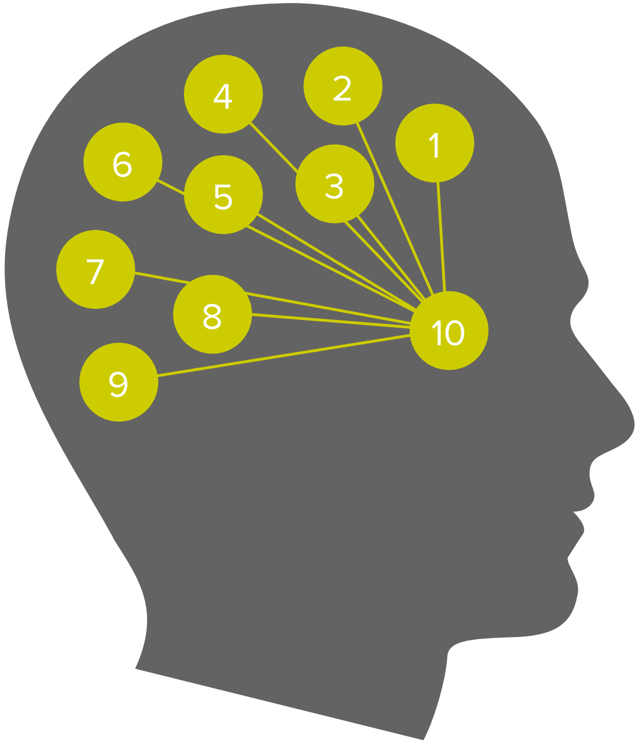
Once you've explained 'why' your topic matters, you need to be clear about employee objectives, at both a macro and micro level, and have a simple and direct call to action. This is not about plastering a set of imperatives or instructions, just the clear articulation of how employees can do the right thing.

THREE/TAILOR YOUR COMMUNICATION

Employees need to be receptive to your message so it's really important to engage on their terms, not just yours. Work out what will resonate for each segment of your audience. By now you will know a fair bit about them, but what more could you consider? People don't like wasting time, so make sure your communication is as relevant to their day-to-day lives, inside and outside the business, as possible.

FOUR/KEEP IT SIMPLE

It's a complex subject and busy employees won't engage with overly complex messages. Simplifying and clarifying takes effort, determination and often ingenuity to deliver. Often the secret is to take a much higher-level view, steering away from the dense undergrowth of policy and procedure.



SEVEN/BE ENGAGING

Information security messages and content could be perceived as dry and uninteresting, which could influence if and how they are received. Communication needs to work hard to make them interesting, compelling and thought provoking (even finding room for a little wit when appropriate). Communications need to be smart and seek to actively engage. Think about trying to 'invade the spaces' that exist both literally (in the business environment) and conceptually (in how employees think and behave regarding information security).

EIGHT/BE DISTINCTIVE

Information security is just one of many topics competing for employees' attention and the noise level can be deafening. Not only does your communication need to stand out, it needs to stick. And stay stuck. You will need an effective 'creative platform' – the creative and intellectual glue to connect all related communications to ensure they remain distinctive, coherent, compelling and effective.

NINE/KEEP IT GOING

Successful campaigns recognise that influencing behaviours around a difficult subject is an ongoing challenge. Threats, systems and people change. Information security needs to be business as usual, and all employees need to be reminded and updated about things – most especially on their role in doing the right thing.

TEN/MAKE IT MEASURABLE

Increasingly, someone somewhere wants to convert it all into a number, to know the ROI, the benchmark levels and the changes. The right measurement could help you understand how effective you are and how the culture is shifting. It's not a simple or singular activity, but really it comes down to the old adage of 'things you can count versus things that count'.

"Did you see the poster?" is an awareness-based question; you can put it to as many people as you like and get some hard numbers. But finding out if they actually carried out the action can be a completely different thing. And of course it's the critical thing.

Having clear objectives at the outset will usually enable a set of appropriate measures to be formulated, or at least provide a glimpse as to what is going on, if not hard and fast proof.

It's worth remembering that in most cases the big goal here is for long-term sustained behavioural change, not a reactive blip. In other words the desired behaviours become part of business as usual – the very DNA of the organisation.

An important measure therefore is the confidence of your organisation and leaders. They need to be able to demonstrate that any incident was indeed an isolated case of individual behavioural dissonance, and not a systemic failure of culture.

So perhaps the ultimate measure is how well you or your CEO sleep at night.

Recent years have witnessed an unprecedented number of information security breaches across the world in all areas of business and society. And whilst effective employee communication has always been a good idea, catalysts in today's business environment make it more of an imperative than an option:

- increased focus from regulators and legislators around the world to prove that organisations are taking a strategic approach to employee awareness, communication and engagement;
- external pressures from customers and investors to ensure the safety and security of their confidential information;
- the financial and reputational damage that can arise from information security breaches.

To see our folio of case studies and discuss how we can help you make employees a staunch line of defence, please call Chris Barrington on 0207 299 1670 or email ***chrisb@bluegoose.co.uk.***