THE SECURTY BREACH

MAKING SURE EMPLOYEES ARE NOT YOUR WEAKEST LINK

level seven Technologies

> Despite the significant effort that governance, compliance and security functions put into managing information security, employees often remain the weakest link in your business'sdefence.

EMPLOYEES ARE YOUR STRONGEST DEFENCE

Even with a basic level of risk awareness and understanding, they can prevent simple lapses in control that are often the root cause of breaches. 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'. Businesses 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.

Level Seven Technologies helps businesses develop employee awareness, communication and engagement programs that focus on three requirements essential to every employee:

- **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.

10 STEPS TO TURN EMPLOYEES INTO YOUR STAUNCH LINE OF DEFENCE

1. 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 program. It also means checking that what you ask employees to do is actually reasonable, and you aren't sending out mixed messages. For example, if your sustainability team encourages employees to recycle paper while the information security team advises them to shred it, employees will be caught in the crossfire of two competing messages. Decide on a plan that makes sense right from the start.

2. KNOW YOUR AUDIENCE

Different employees will face different information security challenges.
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.

3. 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.

4. KEEP IT SIMPLE

It's a complex subject and busy employees won't engage with overly complex messages. Simplify and clarify your message.
Often the secret is to take a much higher-level view, steering away from the dense undergrowth of policy and procedure. Let your employees see the forest for the trees.

5. TELL THEM WHY

Employees need to understand their role in managing information security. But unless you provide them with the right motivation, 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 organization. Get their buy-in.

6. 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.

7. BE ENGAGING

Information security messages and content can be dry and uninteresting, which can influence if and how they are received. Communication needs to work hard to make those messages interesting, compelling and thought provoking. 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).

8. BE DISTINCTIVE

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

9. KEEP IT GOING

Successful campaigns recognize 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.

10. 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.

"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.

An important measure therefore is the confidence of your organization 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.

SECURITY BREACHES HAPPEN

Effective employee communication in today's business environment is more imperative than ever.

At Level Seven Technologies w
can help you plan for and
prevent information securit
breaches. Ask us how.

www.levelseventechnolgies.c

Or find us on Facebook at *Lev*
Seven Technologies Inc.