LAYER 8

Main House, Colworth Park
Sharnbrook Bedfordshire MK44 1LQ
0800 772 0372
layer8ltd.co.uk

Changing Security Behaviours – From Knowing to Doing (Presented at the Bedford BCS Meeting, Park Inn 22.05.18)

Mike Carter & Amanda Price (Creative Directors, Layer 8 Ltd)

A change in behaviours can't happen individually; it requires a proactive culture to help facilitate a shift from knowing (awareness) to doing (proactive behaviour).

What does a proactive culture look and feel like?

You may have experienced this as part of a sports team, a family group, or a work group.

Successful cultures share the following characteristics:

- Everyone feels seen and valued.
- It feels like a substantial thing entity in your life. You feel happy and privileged to be part of it.
- The culture encourages you solve problems – if a crisis hits or action needs to be taken, there are people around who are able to get together and work out a solution.
- You feel able to bring your best self to the group, because you all knew that this group was more than the sum of its parts – it brings out the potential in each one of its members.

An effective culture is a way of being with each other that brings advantages for every single participant. It also works very effectively in achieving its goals.

And the good news is that they don't happen by accident, great cultures are made.

What is a proactive security culture?

At Layer 8 we're in the business of making security cultures. Our aim is to take businesses on a journey from being compliant, to becoming a security culture which is resilient, adaptive and proactive in its response to the security threats they encounter.

The most successful security cultures are ones in which:

- Everybody understands and accepts that they all need to take responsibility for security.
- Where policies aren't kept in desk drawers but they're living, breathing things, embodied by everybody.

Main House, Colworth Park
Sharnbrook Bedfordshire MK44 1LQ
0800 772 0372
layer8ltd.co.uk

- The contribution that you make is seen and valued.

What does a proactive security culture look and feel like?

Imagine, for a moment that you've been away from your business for a year or so. In your absence, you hear that a proactive security culture has been developed across the business which is operating successfully, so on your first day back you're quite excited to see the difference:

- **Visitor-friendly security -** You walk in behind a visitor and things are different about the way they're treated. There's an extra level of care that's taken over how they're let in, how they're met and how they're monitored throughout their visit, but that doesn't mean there is any lack of warmth and welcome in their experience. In fact, they seem to be really 'seen' and looked after.
- **Office spaces are clear -** You enter the office space and it takes you a moment to realise what's so shockingly different: it looks a lot tidier, and every desk is clear of documents and every unattended computer screen is locked.
- **Employees talk about security -** In the kitchen, where you make a coffee, someone mentions a data breach that's been in the news and a conversation starts up about the implications for your business.
- **Security is on every agenda -** You open your emails and you find an invitation to a meeting. You're flabbergasted. Why? Because security is on every meeting agenda, and the 10-min slot is one that's filled with discussion, collaboration – and actions.
- **Security incident reporting is normal -** And on your way to the loo you see a poster about the importance of reporting. And a colleague who sees you looking at it tells you how reporting is encouraged because that's how the organisation learns to be more secure – and even if you've made a mistake they want to hear about it and nobody gets blamed.
- **Security culture includes the senior team -** You go back to your desk and there's short film from your CEO on the intranet, in which she speaks in glowing terms about the efforts of everyone to make the business more resilient, that the CISO was able to demonstrate measurable changes and there will be funds allocated to answer the requests for further security training that staff have asked for.

What you're seeing as you walk through your place of work is a proactive culture in which everybody is seen, everybody makes a difference, and everybody's contribution is valued.

How can we move from a compliant security culture to a proactive one?

Layer 8 came into being because we saw a common problem emerging across businesses in all sectors; tech is installed in response to a range of security vulnerabilities, but detailed training for employees in their responsibilities and behaviours around security is minimal.

Main House, Colworth Park
Sharnbrook Bedfordshire MK44 1LQ
0800 772 0372
layer8ltd.co.uk

The absence of effective training creates a new vulnerability. Often, when we talk to employees they express confidence in their ability to work securely in their daily routines. When asked to talk about what that means, they will often say that the tech installed by the IT department provides security across all systems. There may be no awareness of themselves as key players in the development of a secure environment and surprise may be expressed at the idea that security is part of their daily role.

Now this is changing slowly, but what organisations still struggle with is first, the need to create a security culture and, second, where to start.

Where to start when creating a proactive security culture

At Layer 8, we always start with a question: How can we create an effective security culture that spreads from person to person through an organisation until it involves every employee from the top to the bottom?

We've worked with very large organisations with tens of thousands of employees, through to those with just 150 staff. We treat each culture change programme as research and, over the years, we have discovered some common themes that recur again and again.

These include:

- The majority of organisations we have worked with find they already have a number of passionate security advocates waiting to take on a more active and visible role in their organisation, they just haven't been asked to do so.
- Nine times out of ten, there is already good work being done that nobody knows about because the focus has been on problems rather than solutions.
- Information that is passed on peer to peer, sticks and has impact beyond anything passed down from above, or from people the employee doesn't know.
- Once people find ways to start talking about security, the growth is exponential, and the movement is rapid – much faster than you might expect.

How does cultural transformation happen in an organisation?

We're going to share a short story about how we saw this happen in an organisation we worked with – a large organisation. At the time Openreach had 33,000 staff. Our brief was to start a process of security culture change that would reach out to meet everyone across a workforce dispersed across the whole of the UK.

LAYER 8

Main House, Colworth Park
Sharnbrook Bedfordshire MK44 1LQ
0800 772 0372
layer8ltd.co.uk

We walked into a room with a team of 40 engineers who had a security remit and they shared one belief amongst them: That people were rubbish when it came to security and they'd never change that, because they'd tried.

So big job then. How are we possibly going to turn this around? This might take months to crack!

We'll actually it took half an hour and one question, which was this:

Tell me about a time when you defended/protected something /someone that mattered to you.

We asked people to pair up and have a conversation focused around their own experience of defending something that mattered to them. We gave everyone a list of questions to get them started and told them they had 30 minutes each to tell their story.

Silence.

They looked at us as if to say: Really? You want me to talk about *this*? You've got to be kidding…

This was quite possibly going to be the first time this group of engineers had ever been asked to talk about some of the best things they'd done, about security that they felt proud of.

We had to hold our nerve. After sizing us up, one of the natural leaders in the room gave the go ahead and – rather sheepishly – everyone turned, in pairs, to face one another.

And you know what? Once they began to talk, the room became alive with their energy, and a whole new world opened up for them – a world of possibility. And when they fed back it was to say:

"This guy's a hero! Do you know what he did?"

"Why do we never get a chance to talk about this stuff?"

"I want to know what everybody else has been talking about."

"What a relief to talk about something inspiring. "

"How can we have this conversation with everybody?"

Main House, Colworth Park
Sharnbrook Bedfordshire MK44 1LQ
0800 772 0372
layer8ltd.co.uk

Our next task was to work out, collaboratively, how they could take this conversation into the workplace, and start generating positive energy around security wherever they went.

One solution was to use the regular compliance checks they all carried out as an opportunity to ask people in the workplace what their impression of security at Openreach was, and how they thought it could be improved – before the checklist came out.

Another of the advocates suggested that they offer one-to-one conversations with members of the security team at the Openreach roadshow that toured the sites over the summer months.

As the day came to a close they were set a target – the number of conversations they were to clock up over 3 months. There was apprehension when the target was announced, but everyone left determined to do their best and the desire to make a difference was high.

Three months later we were invited on a conference call with the team.

- They smashed their target re number of conversations they'd have.
- They had discovered tons of good practice that had been unsung – and they were excited to share it.
- They were able to report changes and actions to tighten security. They were also putting place measurement to track the speed and effectiveness of the developing security culture as it occurred.
- Many of the people they had talked to wanted to volunteer to spread the security conversation themselves and help to develop security culture.

Most importantly, they had established a new relationship with the people they worked with; one that was not about problems and telling them what to do, but about dialogue and collaboration towards a goal based on shared values.

Once the conversation changed, the culture began to change.

Why did this approach to culture change work?

- The change began with each individual talking about their values.
- Security was reframed as a positive and motivating force.
- The security team 'felt' the power of conversation as a tool for change, and they wanted to perpetuate it across the business.
- Collaboration was recognised to be more effective as a force for change, than checking for compliance, or telling people what to do.

Main House, Colworth Park
Sharnbrook Bedfordshire MK44 1LQ
0800 772 0372
layer8ltd.co.uk

- The feedback loop told them they were on to something powerful; the people they spoke to immediately wanted to be part of the culture they were creating.

To develop the security culture you want to see, there is no substitute for face-to-face conversation. Person to person communication is a powerful weapon and it's the lifeblood of culture. Being in a room together - seeing and valuing one another – gives everyone an added motivation to play their part in protecting their business.

Daniel Coyle, author of *The Culture Code* writes that: "Culture is the 15 feet around you every day." Culture change happens one conversation at a time.

For a more detailed discussion of the journey from compliant to proactive security culture, see "Activating the Human Firewall: The Leap from Knowing to Doing" by Carter, M. & Price, A. in Reuvid, J. (ed.) (2018) **Managing Cybersecurity Risk: Case Studies & Solutions.** London: Legend Business