Clarity

Edition 1.0

The cyber behaviour gap.

A Clarity insight report. Summer 2026.



© Clarity 2026. All rights reserved.

Cyber security has a behaviour problem.

Cyber security teams have never had more tools at their disposal – investment in technology continues to rise, systems become more sophisticated, and threat intelligence grows more advanced by the day.

And yet, attacks proliferate, vulnerabilities are exposed, data is lost, and with it customer and brand trust.

To better understand why, we surveyed 250 cyber security leaders to understand their perspective. What we learnt won't surprise all CISOs – but it does explain why we're not winning the battle.

It's about people, not patches.

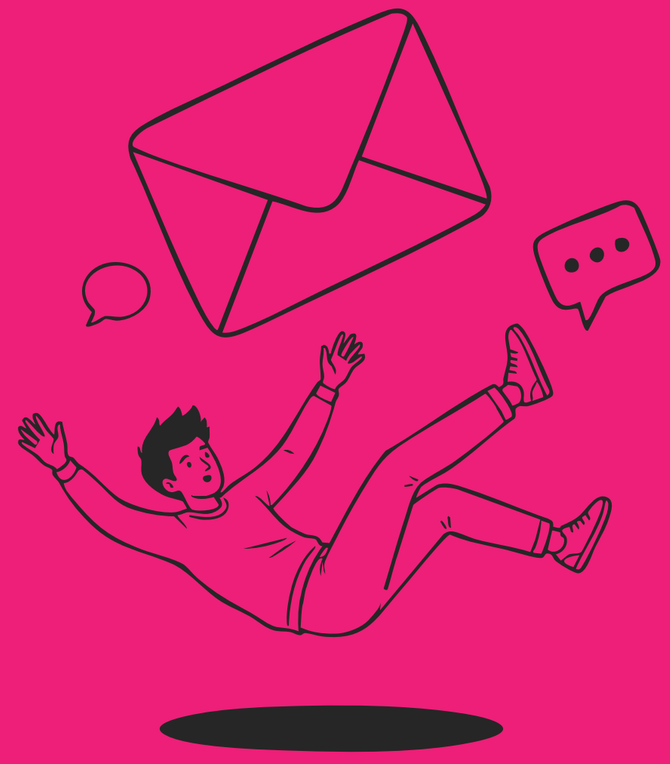
93%

Surveyed said human behaviour is either the primary cause or a major contributing factor in cyber security incidents*

Not a minority. Not an edge case.
Almost everyone agrees.

It confirms what many already know instinctively: technology alone cannot keep organisations secure. The everyday decisions people make – clicking, sharing, reusing passwords, bypassing processes – remain the biggest source of risk.

What's interesting isn't that this is true, but that despite widespread agreement, many organisations still struggle to change it.



*Clarity Cyber Engagement Survey 2026

Engagement remains the weakest link.

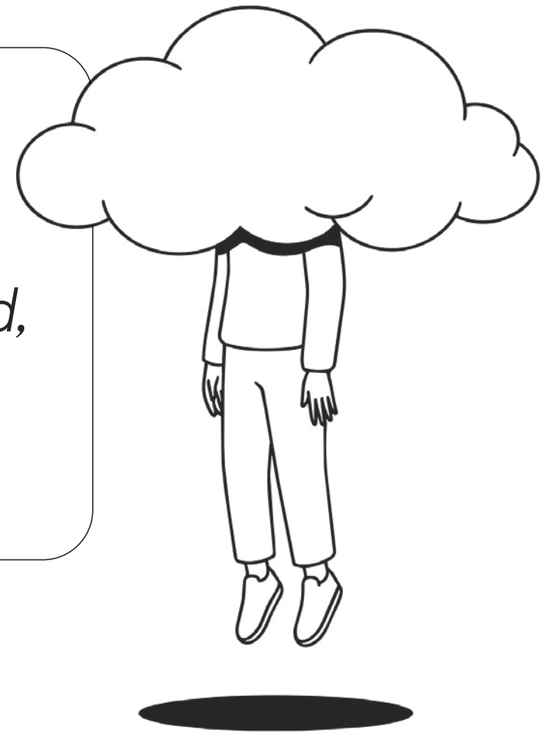
When asked, only a minority described their current communications as genuinely engaging, while a significant proportion felt they were neutral or disengaging. This matters, because engagement is the gateway to behaviour change, and we know, if people don’t pay attention, nothing else will follow.

Respondents were clear...

- Content feels too technical
- Messages are repetitive or easy to tune out
- Communications lack creativity
- Teams don’t always understand how different audiences actually work day to day

The issue?

'It's not what is being communicated, but how.'



*Clarity Cyber Engagement Survey 2026

Brand matters more than ever.

While just under half of respondents said their cyber communications had a consistent identity, most described them as inconsistent, or having no defined identity at all.

That's important.

When communications don't feel familiar or culturally aligned, they're easier to ignore. In contrast, when people instantly recognise something as "from the cyber team", it reduces friction and increases trust.

This is an area where organisations are starting to borrow thinking from external brand and marketing disciplines, with noticeable impact.

The truth

'Messaging shouldn't fight for attention, it needs to earn it.'



Some measurement exists. Confidence, much less so.

40%

Surveyed were not fully confident that their cyber awareness activity leads to lasting behaviour change*



Most teams measure something. Mandatory trainings, phishing simulations and team surveys are often referenced.

But the gap between measurement and confidence is telling.

Tracking activity is not the same as proving impact. Without a clear vision of what success looks like – it becomes difficult to demonstrate any shift, leaving cyber teams under pressure to justify investment.

*Clarity Cyber Engagement Survey 2026

Where relevance beats repetition.

One encouraging signal from the data is where teams believe the biggest opportunity lies.

Repeatedly, we see the most effective cyber programmes don't try to say more – they work harder to say the right things, to the right people, at the right moment.

In some organisations, that has meant focusing on frontline teams with time-poor, line manager led structures. In others, it has meant using personal-life scenarios to make risk feel real. In others still, it's about creating immersive experiences that stick with people.

Different contexts, same principle: relevance first.

Respondents consistently pointed to...

- More engaging and creative campaigns
- Clearer accountability for behaviour
- Better alignment to real risks people face



What does this mean for cyber leaders?

The data suggests cyber teams aren't failing – they're operating in a system that still undervalues communication as a discipline.

Most respondents already understand the role of human behaviour. Many are experimenting with new formats. Fewer feel able to prove, confidently, that they've changed outcomes.

The opportunity now is not to create more noise, tools or training modules, it's to be clearer in our approach to fostering change.



Ask yourselves...

- Whose behaviour needs to change
- What does that change look like
- How our comms earn their attention, not demand it

In 2026, the strongest cyber cultures won't be built through fear or compliance. They'll be built on clarity, consistency and communication that understands our people and their roles.

Ori Fragman. Global Security Lead. Arrive.

Let's talk.

Clarity help organisations including **H&M, Ahold Delhaize, Primark, Hapag-Lloyd, Zalando** and **PayPoint** to build cyber aware cultures, shaping the behaviour of over 1 million associates daily.

If you're wrestling with similar challenges, or want to explore how clearer, more engaging communication could help shift behaviour in your organisation, we'd love to talk.



Clarity

Norfolk House, Saxon Gate, MK, UK
hello@wecreateclarity.co.uk

Best Workplaces™ In Advertising, Media & Marketing

Proudly employee owned.

Institute *of* Internal Communication

© Clarity 2026. All rights reserved.