CyBehave

WHITEPAPER

Beyond the Checkbox: Evolving from Awareness to a Resilient Security Culture

How to make the move from awareness training to a behaviour and culture programme.

Publication Date: April 25th, 2025

Abstract

This whitepaper explores the critical journey organisations must undertake to evolve from basic cybersecurity awareness programmes toward embedding secure behaviours and cultivating a mature security culture. While traditional awareness training serves as a necessary foundation, it is often insufficient to effect lasting change. Drawing on behavioural science, particularly the COM-B model, the paper outlines how organisations can bridge the gap between awareness and action through context-specific, motivational interventions. The development of a strong security culture, where secure behaviours become habitual and collectively reinforced, is positioned as the ultimate goal. The role of Security Champions, leadership modelling, and psychological safety are examined as key enablers of cultural transformation. The paper concludes with a call to action for business leaders to invest in the maturity of their security programmes - not only to protect assets and build resilience but also to drive a broader societal shift toward responsible and secure digital behaviour. This evolution, from awareness to behaviour and ultimately to culture, represents a strategic and moral imperative in an increasingly digital world.

> *"Awareness informs the mind.*
> *Behaviour reveals the intent.*
> *But culture, culture shapes the future."*

The Pathway to Culture

For too long, corporate strategies have rested heavily on one-off awareness training sessions that aim to 'educate' users. While raising awareness is an important step, it is insufficient on its own to produce measurable changes in security behaviour or embed a resilient culture. This whitepaper argues that the true maturity of an organisation's cyber posture emerges only when awareness evolves into behaviour, and behaviour solidifies into culture. This paper sets out the case for this evolution, the pathway to achieve it, and the wider societal benefits that stem from such a transformation.

The Limitations of Awareness Alone

Organisations have become stuck in a cycle of checkbox awareness training largely due to regulatory pressures, budget constraints, and a historical over-reliance on traditional learning approaches. Compliance-based frameworks such as ISO/IEC 27001 encourage the implementation of awareness programmes, but rarely specify qualitative measures of behavioural change. As a result, many businesses have opted for generic, annual training modules that meet the minimum legal standard without driving meaningful outcomes.

This results in what is often referred to as 'awareness fatigue'. Employees disengage from repetitive, irrelevant messaging and fail to internalise secure practices. Research shows that awareness without behavioural reinforcement can lead to complacency and even risk compensation, where individuals assume protection merely because training has been completed (Parsons et al., 2017; Bada et al., 2019).

If we continue down this path, we risk embedding a false sense of security at every level of the organisation. Leaders may overestimate their workforce's readiness, while employees remain unprepared for the nuanced, socially engineered attacks that characterise modern cyber threats. Inaction also fosters a toxic blame culture where breaches are attributed to 'user error', ignoring the systemic failures in training, environment, and leadership (ENISA, 2019).

The cost of not evolving beyond awareness is substantial: increased vulnerability, reputational damage, regulatory penalties, and human harm. Cybercriminals exploit behavioural weaknesses, not just technical ones, and unless we address this gap, we will remain in a reactive and fragile state.

From Awareness to Behaviour

Behavioural science offers valuable insights into how awareness can be transformed into sustained behavioural change. The COM-B model (Capability, Opportunity, Motivation - Behaviour) developed by Michie et al. (2011) provides a framework that organisations can use to diagnose behavioural barriers and design effective interventions. This model aligns with other leading theories, such as Fogg's Behaviour Model, which emphasises that behaviour occurs when motivation, ability, and a trigger converge (Fogg, 2009).

Awareness alone may create Capability (knowledge), but without Opportunity and Motivation, behaviour does not follow. Employees need the time, tools, supportive environments, and incentives to act on what they know. Crucially, the messaging must be timely, relevant, and delivered in a way that aligns with their values and roles (Thaler & Sunstein, 2008).

Targeted, context-sensitive interventions should:

- Build capability through hands-on, scenario-based training that makes secure behaviour practical and personalised;
- Create opportunities by integrating security into daily workflows, making it effortless to make the secure choice;
- Enhance motivation through meaningful rewards, real-life examples, leadership endorsement, and demonstrating how security supports, not hinders, their work.

Behavioural interventions such as nudging, habit formation, and peer modelling have shown success across sectors. In cybersecurity, this could mean moving from static eLearning to dynamic, team-level challenges, interactive simulations, and real-time behavioural feedback (LaRose et al., 2008; Hadlington, 2017).

Sustained behaviour is about building habits. Repetition, reinforcement, and visibility are key. Without positive reinforcement, behaviours tend to lapse. Recognition, feedback, and leadership visibility all help embed secure practices as daily norms.

From Behaviour to Culture

Culture is the aggregation of behaviours, values, and norms that define how people act when no one is watching. A security-aware culture is one where secure behaviours are the norm, not the exception. Culture acts as the collective immune system of an organisation: strong, pervasive, and often invisible until tested by crisis (Schein, 2010).

Organisations often falter at this stage because cultural change is less tangible than awareness metrics or behavioural outputs. It requires long-term thinking, trust-building, and leadership commitment. However, the pay-off is a deeply embedded mindset that empowers employees to take proactive ownership of cybersecurity.

Cultural maturity is achieved when:

- Security is embedded in the language and priorities of every team, not relegated to the IT department;
- Senior leaders regularly communicate the importance of secure behaviours, backing words with consistent actions;
- Peer-to-peer learning and informal norms validate secure practices as socially expected behaviours;
- Employees feel psychologically safe to report incidents, question decisions, and suggest improvements without fear of punishment.

Without this evolution to culture, secure behaviours remain vulnerable to stress, pressure, or competing demands. In contrast, when secure choices become part of the organisational identity, they persist even in challenging conditions (Furnell & Clarke, 2012).

The Role of Security Champions and Change Agents

Security Champions and informal influencers represent one of the most effective ways to spread behaviour and culture organically. Rather than relying solely on top-down communication, champions provide a human connection to security, contextualising guidance for their teams and surfacing local challenges.

These champions need ongoing investment. When adequately supported, they drive grassroots change, build local ownership, and act as the 'emotional intelligence' of the security function. Champions can turn abstract policies into relatable, actionable habits by bringing lived experiences into the conversation (Werlinger et al., 2009; Sasse & Flechais, 2005).

Organisations must identify, train, and reward these agents of change. Without formal recognition or a structured framework, champions may burn out or disengage. A mature champion network is adaptive, inclusive, and integrated into business objectives.

Organisational Benefits of a Behaviour and Culture Approach

The business case for evolving from awareness to behaviour and culture is not just ethical, it is strategic. Embedding secure behaviour and cultivating a strong culture provides organisations with a competitive edge. It strengthens the entire security posture by making human defences as robust as technical controls (PwC, 2021).

Benefits include:

- Measurable reduction in security incidents related to human error;
- Quicker and more effective responses to emerging threats due to improved vigilance and communication;
- Increased employee engagement and trust through empowerment and transparency;
- Enhanced brand reputation and customer trust from visibly prioritising responsible digital practices.

The shift also creates alignment between cybersecurity and other organisational values, such as wellbeing, inclusion, and sustainability. It positions security as an enabler of business, not a blocker.

Looking Beyond: A Societal Opportunity

The influence of workplace behaviour on home life is profound. Employees who understand the value of strong passwords, privacy controls, and phishing identification share these skills with partners, children, and friends. Over time, this builds a more cyber-literate society (UK Cabinet Office, 2022).

Public-private partnerships, education initiatives, and grassroots campaigns can all benefit from the behavioural science underpinning this cultural approach. From schools teaching digital resilience to community centres offering cyber clinics, the ripple effects are immense (NCSC, 2023).

This societal opportunity must not be missed. If we continue to treat awareness as an end goal, we risk a future where digital threats outpace our collective ability to respond. But if we embrace culture as the foundation of cybersecurity maturity, we pave the way for lasting, inclusive, and community-wide resilience.

Summary

Cybersecurity awareness is the necessary first step, but not the destination. Organisations must invest in evolving their programmes to focus on behaviour and culture. This evolution is both a strategic imperative and a moral responsibility, ensuring not just the protection of assets but the empowerment of people.

The pathway from awareness to behaviour to culture is one of increasing maturity, resilience, and impact. It requires a mindset shift, from educating employees to enabling and empowering them, from compliance checkboxes to everyday ownership, and from reactive measures to proactive cultural resilience.

Building this security culture requires sustained leadership commitment, intelligent behavioural interventions, and an environment that supports and rewards secure behaviours. It demands integrating cybersecurity into the daily fabric of the organisation, aligning secure practices with broader business goals such as wellbeing, innovation, and sustainability.

The benefits are tangible: fewer security incidents, faster responses to threats, stronger trust internally and externally, and a competitive advantage in an increasingly digital and risk-laden world.

However, the impact goes even further. By embedding a security culture in organisations, we create ripple effects across society. Employees carry secure behaviours home, influencing families, communities, and future generations. Businesses become role models for responsible digital citizenship. Collectively, we move towards a more cyber-resilient society.

By doing so, we don't just secure companies. We build trust. We protect the vulnerable. We enhance societal resilience. And we contribute to a future where digital interactions are underpinned by informed, intentional, and responsible action - securing not just our data, but our collective future.

References

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

ENISA. (2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Fogg, B. J. (2009). A behavior model for persuasive design. *Proceedings of the 4th International Conference on Persuasive Technology*, 1–7.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983–988.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346.

Kahneman, D. (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM, 51*(3), 71–76.

Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science, 6*(42). https://doi.org/10.1186/1748-5908-6-42

NCSC. (2023). *Cyber Aware Campaign Resources*. UK National Cyber Security Centre. https://www.ncsc.gov.uk

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

PwC. (2021). *Global Digital Trust Insights Survey*. PricewaterhouseCoopers. https://www.pwc.com

Sasse, A. M., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In *Security and Usability* (pp. 13–24). O'Reilly Media.

Schein, E. H. (2010). *Organizational Culture and Leadership* (4th ed.). Jossey-Bass.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin Books.

UK Cabinet Office. (2022). *National Cyber Strategy 2022*. https://www.gov.uk/government/publications/national-cyber-strategy-2022

von Solms, B., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*.

For further tools, insights, and resources on human risk management and cybersecurity culture, visit **www.cybehave.com**.

CyBehave offers a wide range of practitioner guides, learning journeys, behavioural toolkits, and leadership resources to support organisations at every stage of their human cyber risk maturity. Join our growing community of security and change leaders who are working to empower a more secure, cyberwise society.