INTERNATIONAL CYBER EXPO

24 – 25 SEPT 2024
OLYMPIA LONDON

SENIOR LEVEL ROUNDTABLE REPORT

AWARENESS, CHAMPIONS, AND NUDGES: THE BUILDING BLOCKS OF A STRONG SECURITY CULTURE

In association with

KnowBe4

INTRODUCTION

ABOUT KNOWBE4

KnowBe4 empowers your workforce to make smarter Security decisions every day. Over 65,000 organisations worldwide trust the KNOWBE4 platform to strengthen their Security Culture and reduce human risk. KNOWBE4 builds a human layer of defence so organisations can fortify user behaviour with new-school Security Awareness and Compliance Training.

Deploying KNOWBE4 results in Users who are alert and care about the damage that Phishing, Ransomware and other Social Engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering and crowdsourced anti-phishing defence.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

Find out more: www.knowbe4.com

ABOUT THE MODERATOR

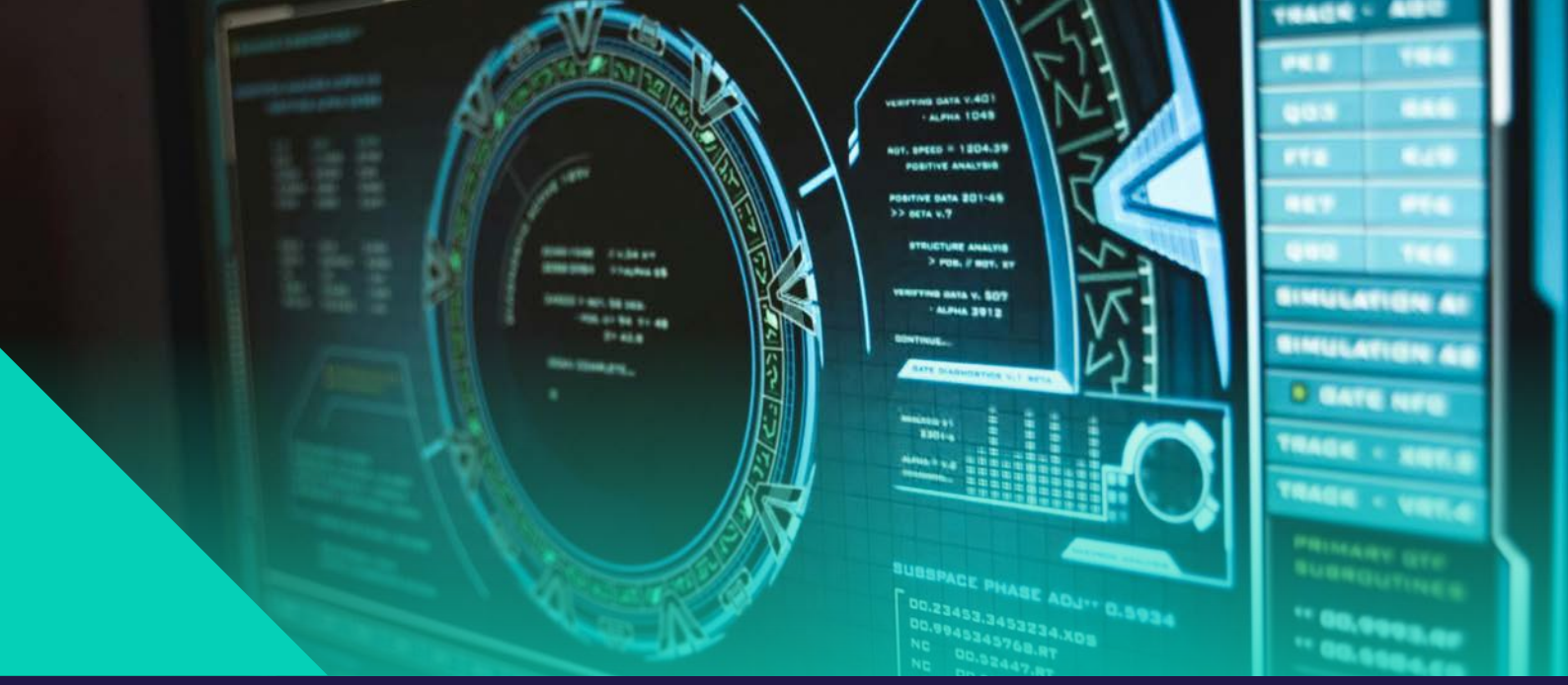
Martin Smith MBE BSc FSyI
Chairman and Founder
The Security Awareness Special Interest Group

With more than 40 years' experience in the security and crime prevention industries, Martin Smith MBE is a well-known, colourful and highly respected personality in the information assurance and cybersecurity world. He is an established and successful communicator, visionary, speaker and blogger on his passion for improving online trust.

Martin gained his degree in behavioural psychology before spending 15 years as a commissioned officer in the Royal Air Force Security (Provost) Branch. After being awarded an MBE for this work, he left the Service to establish a second career in the commercial sector.

He founded The Security Awareness Special Interest Group (SASIG) in 2004 as a subscription-free networking forum for security practitioners. Its membership now comprises 9,000 individuals representing some 2,500+ organisations from both the public and private sectors.

Martin is a Fellow of The Security Institute. In 2017, he received a lifetime achievement award at The Outstanding Security Performance Awards (The OSPAs) for his services to the security industry. In 2024, he received a Commendation from the City of London Police Commissioner and the National Police Chiefs' Council for his lifetime's work in combatting cybercrime.



AWARENESS, CHAMPIONS, AND NUDGES: THE BUILDING BLOCKS OF A STRONG SECURITY CULTURE

Martin Smith, chairman and founder of The Security Awareness Special Interest Group (SASIG), and representatives from security awareness training provider, KnowBe4, recently hosted an invitation-only roundtable on the importance for organisations of establishing a strong IT security culture.

They were joined by a select group of senior cybersecurity professionals from a range of organisations across several different sectors, including telecommunications, aerospace, finance, the public sector, and more.

The roundtable—held under Chatham House Rule to encourage openness and the sharing of information by providing anonymity to those involved—focussed on why organisations must address the staff ABC of cybersecurity – awareness, behaviour, and culture.

While most organisations address the first two, these approaches often reach the limits of their effectiveness as they primarily change an individual's behaviour. Hence, it's an ongoing task that has to be repeated with every new starter.

In contrast, establishing a security culture is essential to sustainability and delivering more efficient practices over the long term. The good practices appropriate to your environment need to become embedded so newcomers will adopt them without needing to be trained.

The insights gleaned throughout the course of the roundtable discussion were so valuable that the key themes and takeaways have been outlined here for the benefit of our wider community.

Security as a collective responsibility

Martin kicked off the session by highlighting that, while 95% of most IT security budgets are spent on technology, 95% of security incidents are caused at the human level. Therefore, shouldn't more focus be placed on culture, training, awareness and/or driving behavioural change?

He then opened it up to the room to discover everyone's thoughts and experiences.

The discussion centred on the challenges and strategies of embedding a robust security culture within an organisation. One participant highlighted the importance of recognising that security is a collective responsibility, not just confined to the security department or operations centre. They emphasised the necessity of shifting mindsets so that all employees understand their role in maintaining security, citing an event that reinforced this idea. The individual underscored that a single mistake, such as clicking on a phishing email, can have significant repercussions, thus necessitating a culture of vigilance and responsibility.

However, another participant challenged this notion, suggesting that changing human behaviour is inherently difficult and that focusing solely on individual responsibility might be futile. They argued for a broader approach that includes understanding and mitigating human risk, rather than solely attempting to alter behaviour. The participant questioned whether pushing the idea that "security is everyone's responsibility" is practical, given that many employees might not take on that responsibility willingly or effectively.

A different perspective was offered by another attendee who acknowledged the importance of embedding a security-first mindset but stressed the need for

realism in achieving this goal. They said their organisation focuses on fundamental security practices such as password management and physical security. They recognised the challenge of making employees perceive the risks as imminent and relevant to them, noting that senior leadership often exhibits poor security behaviour. Their strategy involves leading by example and setting realistic objectives, while also addressing the complexities introduced by expanding their focus to include operational technology.

Another participant aligned with the sentiment of addressing human factors, pointing out that organisations often try to force compliance through technology rather than understanding how employees interact with security measures. They shared an anecdote about their team, including themselves, falling for phishing emails despite their awareness and training, illustrating the challenge of expecting perfect compliance from humans.

The discussion then delved into the balance between extrinsic and intrinsic motivation. One participant argued that relying solely on external directives will only achieve limited success, advocating for an approach that helps employees understand and internalise the importance of security. They drew an analogy to everyday security behaviours, such as locking doors, which people do out of a clear understanding of the consequences. The challenge is to bridge the gap between individual actions and their impact on organisational security in a large, complex environment.

A counterpoint was then raised, which suggested that most people inherently want to do the right thing but face obstacles that hinder their ability to comply with security practices. The speaker advocated for simplifying security measures and providing clear, straightforward guidance, combining nudges, mandates, and other strategies to facilitate compliance. They emphasised the concept of organisational resilience, focusing on mitigating significant risks and understanding where to prioritise efforts for the greatest impact.

Throughout the conversation, participants acknowledge the varying levels of engagement and compliance among employees, influenced by factors such as organisational culture, regional differences, and acquisition of new businesses. They discuss the need for ongoing communication, metrics, and tailored strategies to address these challenges. Ultimately, the goal is to foster a security-aware culture that is resilient and capable of adapting to evolving threats and complexities.

Driving beneficial cultural change

The conversation then moved on to the topic of organisational culture, with one participant noting that their organisation, despite having a generally positive culture and strong security practices in some areas, faced inconsistencies across departments. They emphasised the importance of top-down influence, where senior leaders' behaviours and attitudes towards security trickle down through the ranks. They also discussed the use of metrics, such as phishing campaign report rates and compromised rates, to shape and steer the organisation towards the desired security culture. However, they stressed the ongoing nature of this task, warning against complacency as it can lead to a regression in secure behaviours.

Another participant drew parallels between different industries, such as media and banking, pointing out that security priorities often vary depending on the primary business focus. For example, in a media company, the urgency to get content broadcasted can sometimes overshadow security concerns, whereas in a financial institution like a bank, security might naturally be more ingrained due to the sensitive nature of the work. This highlights the tension between operational goals and security requirements, where employees are often not measured on their adherence to security protocols but rather on their core job functions.

The discussion also delved into the emotional impact of security measures on employees. Multi-Factor authentication (MFA) was cited as an example of an effective but potentially frustrating security protocol. The conversation suggested that

understanding and mitigating the emotional toll of such measures could enhance compliance and overall security posture.

A significant point raised was the concept of judgement in security. It was suggested that instead of dictating exact actions, organisations should focus on enabling employees to make informed risk-based decisions. This approach was likened to health and safety practices, where continuous education and awareness have become second nature, and the goal is to replicate this in the cybersecurity realm.

The discussion also touched on the role of real-life examples in training and awareness programmes. Some organisations have faced internal resistance from communications teams wary of causing panic or negative reactions. However, real-life incidents can effectively illustrate the consequences of poor security practices and drive home the importance of vigilance.

There was a consensus on the need for a balanced approach in security communications. Overemphasising threats can lead to desensitisation, while underplaying them can result in complacency. The challenge lies in making security a priority without inducing undue fear or fatigue among employees.

Finally, the discussion highlighted the importance of organisational transparency and openness in handling security incidents. Encouraging a culture where employees feel safe to report mistakes without fear of retribution is crucial. This can prevent small issues from escalating into major breaches and foster a proactive security culture.

Maximising the outcomes of phishing simulations

The topic of simulated phishing tests was then brought up, specifically the implementation, challenges, and effectiveness of them in organisations. The participants shared their experiences and strategies to enhance cybersecurity awareness and training among employees.

Initially, the conversation touched on the evolution of phishing tests, noting that earlier tests were basic and yielded satisfactory results in terms of click and report rates. However, the participants recognised the need to make these tests more sophisticated to reflect the real risks and complexities of phishing attempts. One of the primary challenges discussed was the struggle to convey the importance and rationale behind these tests to employees. There was a consensus that understanding the "why" behind phishing tests is crucial for meaningful engagement and behaviour change.

The discussion then shifted to various approaches to phishing tests. One approach mentioned was to focus on learning rather than just testing. This involves using phishing simulations to educate employees and then assessing whether the training has been effective. The goal is to change the organisational culture towards better cybersecurity practices. This approach is exemplified by targeting specific departments or business lines with customised and relevant training materials, leading to significant improvements in phishing test performance.

A key point raised was the importance of making phishing simulations relevant and not punitive. One participant shared their experience with a punitive approach, where multiple failed phishing tests could lead to HR involvement or account restrictions. However, they advocated for a more supportive and educational approach, which includes targeted learning interventions and less punitive consequences.

The participants also discussed the importance of metrics in understanding the effectiveness of phishing tests and cybersecurity training. Metrics such as click rates, report rates, and the response to more complex phishing attempts are used to identify high-risk individuals and tailor further training accordingly. The conversation highlighted the need to correlate simulation results with real-world behaviour to ensure that training is impactful.

Another significant aspect discussed was the role of senior leadership in promoting cybersecurity. One participant shared a successful example where phishing the new CEO led to a broader advocacy for cybersecurity within the organisation. This involvement of senior leaders is seen as crucial for embedding a security-conscious culture throughout the organisation.

The conversation also touched on the importance of reporting phishing attempts and the need for a no-blame culture to encourage employees to report incidents without fear of punitive action.

The discussion concluded with various ideas to incentivise and gamify phishing training. Suggestions included phishing tournaments, recognition for reporting phishing attempts, and making training more engaging and relevant to employees. These strategies aim to foster a positive attitude towards cybersecurity and encourage proactive behaviour among employees.

The role of security champions

The subject of security champions came up next, individuals who have agreed to be responsible for advocating and encouraging cybersecurity best practices across an organisation or individual departments.

One of the challenges mentioned was the general lack of understanding among employees about the distinction between information security and data privacy. The proposed solution involved utilising current data privacy champions to also advocate for broader information security measures, thereby enhancing the overall security culture without overwhelming the organisation with new programmes. This pragmatic approach could streamline efforts and make efficient use of existing resources, provided it meets the organisation's specific cybersecurity needs.

An example of a well-established champions network consisting of 200 members across 20 countries was illustrated. These champions play a critical role in bridging the gap between central security directives and local implementation. They help to surface local issues, facilitate communication, and ensure that security practices are adapted to the unique cultural and operational contexts of each region. The key to their success appears to be their influence and respect within their local environments, rather than their technical expertise.

Becoming a champion in this network involves a selection process that includes studying and testing. The champions range from junior to very senior employees, all of who volunteer for the role. The organisation's leadership recognises that these champions do not need to dominate their day jobs with this role, instead, their participation is integrated into their regular objectives and assessments. This dual-role strategy ensures that their contributions are valued and aligned with their career goals.

Building and maintaining a robust champions network requires constant engagement and recognition. The organisation employs various incentives, including branded merchandise and formal recognition programmes, to maintain high levels of enthusiasm and participation. This sense of belonging and pride in being part of an identifiable team fosters a positive security culture.

Another significant point of discussion was the relationship between local champions and central leadership. Effective security measures cannot be dictated solely from a central office; they must resonate with local practices and behaviours. The champions help tailor these measures to fit local needs, ensuring better compliance and effectiveness.

Moreover, the dialogue touched upon the challenge of gaining managerial support for employees taking on the additional role of a security champion. Embedding the champions' responsibilities into their performance goals and objectives helps mitigate concerns about diverting attention from their primary duties.

Another critical factor for the success of the champions network is continuous education and training. Providing champions with the necessary knowledge, mostly around security culture rather than technical skills, is crucial. The organisation offers various training resources and recognises different levels of expertise, such as bronze, silver, and gold accreditations, which champions can showcase as part of their professional development.

Finally, the discussion underscored the importance of having a top-level executive championing the security initiative. This high-level support can significantly influence the programme's success, ensuring that it receives the necessary attention and resources. A strong advocate at the board level can drive the message across the organisation, emphasising the critical nature of cybersecurity and data privacy.

Final thoughts

The challenges of fostering a robust security culture within an organisation should not be underestimated. While some argue for collective responsibility and vigilance among all employees, others emphasise the difficulty of changing human behaviour and the need for realistic strategies. The consensus is that security requires a balance of intrinsic motivation, clear guidance, and organisational resilience to effectively mitigate risks and adapt to evolving threats.

The discussion also underscored the complex interplay between organisational culture, employee behaviour, and security practices. It emphasised the need for continuous effort, informed judgement, emotional consideration, and transparent communication to cultivate a robust security environment across diverse industries.

Furthermore, the intricacy of implementing effective phishing tests and training programmes means that a balanced approach that combines education, relevance, senior leadership involvement, and a supportive culture to achieve meaningful improvements in cybersecurity awareness and resilience.

Lastly, integrating cybersecurity and data privacy efforts through a well-structured champions network, supported by continuous training, recognition, and top-level advocacy, can create a robust security culture within an organisation. The approach balances the need for local adaptation with the strategic goals set by central leadership, ensuring that security measures are both effective and culturally appropriate.

For more critical insights into workplace cybersecurity awareness and behaviours, download this free KnowBe4 whitepaper now: UK Cybersecurity Practices at Work Report