Hear first about SASIG events and industry news
Follow us on:

Cybersecurity Awareness SASIG

In association with

Cybersecurity is a human condition and we at the SASIG always enjoy returning to the fundamental reason for our being. Security Awareness. As more organisations realise that cyber is not a separate functionality, it's embedded across our lives, they work hard to ensure that their people, and customers, understand the risks, threats and issues with operating in an online, interconnected world.

Our hosts at BT have been industry leading with their methodology for engaging their diverse workforce. It's always a delight to have discussions that help Security Awareness professionals deliver innovation, and best practice, back to their own organisations. This event will share practical insights and valuable lessons learned in building informed, resilient workforces across diverse sectors.

Please join us, participate, add your voice to the day so that through the collaboration we can strengthen security awareness and shape a culture of resilience within your organisation and beyond.

All SASIG events operate under the Chatham House Rule, and there is no charge to attend. Our hosts will kindly provide lunch and refreshments.

Thursday 8 October 2026
9.30am - 4.15pm
London

Chair

Liz Murray
Chief of Staff, The SASIG

9.30am **Registration, coffee, and networking**

10am **Welcome and introductions**
Vic Djondo SRO, Security Culture & Education, BT

10.15am **Keynote Presentation**
Vic Djondo SRO, Security Culture & Education, BT
Rich Eyre Director Cyber Operations & Threat Intelligence, BT
Embedding a protective culture within an organisation is at the heart of what cybersecurity awareness professionals deliver on a daily basis. This is not without its challenges, especially where technology and the threat move faster than the ability to deliver traditional education.

10.45am **Interactive session: The devil is in the detail, but the detail is the devil. Prepare to help us build a practical session to deliver information that matters to a board that might not want to hear it**
Vic Djondo SRO, Security Culture & Education, BT Group
Nathan Linden Lead Cyber Security Incident Management Specialist, BT Group
John Scott Managing Director, Wildpark Security Consultancy
Liz Murray Chief of Staff, The SASIG

Reworking messaging to deliver inspirational sessions that land security best practice in a way that non-technical colleagues and board members can understand is a constant challenge for awareness professionals. In this interactive session we will take a current issue that boards need to understand and build a session with everyone's input that can be taken away and delivered.

11.45am **Tea, coffee, and networking break**

12.15pm **Cybersecurity is a team sport: Are we talking like it?**
Mike Whittle Human Cyber Risk & Culture Lead, SSE

If cybersecurity depends on everyone, why do we so often speak as though it belongs to a few? This session examines how language can either unite or divide teams, influencing trust, engagement, and security outcomes. Through practical examples, we'll explore how small changes in communication can help break down "us and them" thinking and create a culture where colleagues work together to reduce human cyber risk.

12.45pm **Your guide to secure behaviour management: Risk visibility, measurable behaviour change and simplified outcome-led compliance**
Tim Ward CEO & Co-founder, Redflags

As cyber threats and AI-related risks continue to evolve, organisations are moving beyond traditional awareness training towards Secure Behaviour Management. This session explores how security teams can better understand, measure, and influence human risk through greater visibility into employee behaviour, proactive intervention, and measurable outcomes.

To deliver practical insights in how to demonstrate the value of security programmes, we'll examine three key pillars: pre-emptive behaviour change to prevent incidents before they occur, visibility into hidden risks and vulnerabilities, and proof of compliance through audit-ready evidence and reporting.

1.15pm **Networking lunch**

Humans in the age of AI: How is the operating model likely to change for security by 2030?
2.15pm **Florian Pouchet** Head of Cybersecurity and Operational Resilience UK, Wavestone

As cyber threats accelerate to machine speed, organisations face a fundamental shift: it is no longer enough to optimise existing security models built for a slower, human-led world. The rise of AI is transforming how cyber activities are executed, requiring operating models to evolve in how they supervise and coordinate human and machine-driven processes - empowering people to stay in control while machines run at scale.

Trust at scale: Turning security awareness into measurable action
Harry Clark Governance, Risk & Compliance Subject Matter Expert, Vanta
2.45pm

Security awareness is easy to launch. Proving impact is harder. As organisations face growing demands around resilience, compliance, and trust, leaders need evidence that security programmes are changing behaviour and reducing risk. In this session, Vanta will explore how automation, continuous monitoring, and smarter controls can help turn awareness into measurable outcomes. We'll learn how leading organisations build confidence, demonstrate accountability, and create a culture of security that supports business growth.

3.15pm **Panel discussion: Moments that matter - turning cyber headlines into protective action**

Facilitated by Liz Murray Chief of Staff, SASIG
Vic Djondo SRO, Security Culture & Education, BT Group
Lilly Fogarty tbc
Nathan Linden Lead Cyber Security Incident Management Specialist, BT Group
Mike Whittle Human Cyber Risk & Culture Lead, SSE
Oz Alashe MBE CEO & Founder, CybSafe
John Scott Managing Director, Wildpark Security Consultancy

It can be tricky to get the attention of our non-technical colleagues, and indeed the hierarchy, until a cyber scare story breaks. Awareness professionals want to capitalise on external interesting events, yet often are bound by internal processes, comms cadence restrictions and rigid alignment with organisational policy. This panel will explore how teams can make the most of these “moments that matter”: turning topical events into timely, trusted awareness messages that land with the impact needed to protect our organisations. Can this work help us get ahead should a cyber incident occur?

4pm **Closing Remarks**

4.15pm **End of Meeting**

About

The Security Awareness Special Interest Group (SASIG)

SASIG is a subscription-free networking forum, membership now represents thousands of organisations of all sizes from across the world and from all sectors, public and private. Its 11,200+ membership is drawn from CIOs, CISOs and their staff with responsibility for cybersecurity within their organisations. Professionals from other disciplines (risk, HR, legal, supply, etc.) and representatives from government, law enforcement and academia are also being increasingly welcomed at events. The Chatham House Rule is strictly enforced and universally respected at all meetings, and vendors and the Press are routinely excluded. Thus, the level of debate is extraordinarily revealing and rewarding.

SASIG has a members' website at www.thesasig.com. Please register here for membership.

With thanks to our Supporters and Contributors…

01234 707 035
info@thesasig.com
www.thesasig.com