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

SASIG Midlands leadership conference

Collaborating to improve resilience

In association with

BT Group

People remain the primary vector through which organisations are attacked. Nearly all breaches involve human error or malicious intent. In a digital world overloaded with data, human mistakes continue to cause the majority of compromise. Emerging technologies will accelerate data flow and give bad actors more sophisticated tools to deceive us, making human risk management more critical than ever.

We are delighted to host this event in partnership with BT Group, where we will focus on human risk management and the power of collaboration. Throughout the day, we'll look at ways to assess and refine our approach to digital resilience. We will explore how we can transform employees into our strongest line of defence and measure the effectiveness of security awareness, risk mitigation, and engagement strategies.

Our discussions will revolve around how we can adapt our organisations' culture to the evolving threat landscape, ensuring security awareness is not just a box-ticking exercise, as well as how collaboration across teams and industries strengthens security posture.

We look forward to welcoming you to Birmingham, the City of a Thousand Trades, to explore these crucial topics and drive forward the conversation on human risk management.

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 22 May 2025
9.30am to 3.30pm
Birmingham, West Midlands

Guest chair

Keith Hayes ISACA Board Member, ISACA Central UK Chapter

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

10am **Welcome and introductions**
Keith Hayes ISACA Board Member, ISACA Central UK Chapter
Vic Djondo SRO Security Culture & Education, BT Group

10.15am **Keynote presentation: From awareness to action - Turning human risk into organisational resilience**
A senior representative from **BT Group**

Security awareness alone is not enough – understanding human behaviour and embedding security into organisational culture is key to reducing cyber risk. As attackers continue to exploit human vulnerabilities, businesses must move beyond traditional awareness training and focus on practical, measurable strategies to influence secure behaviour at scale.

This keynote will explore how to bridge the gap between awareness and action, turning employees into active defenders rather than passive risks. We will examine real-world insights on behaviour-driven security, discuss the psychology behind decision-making in security, and outline actionable steps to build a culture of resilience. By shifting from reactive to proactive human risk management, organisations can reduce insider threats, improve security engagement, and enhance overall resilience.

10.45am **Panel session: Human risk in cybersecurity - Understanding and managing the weakest (and strongest) link**
Facilitated by **Vic Djondo** SRO Security Culture & Education, BT Group
Tim Ward CEO & Co-founder, Think Cyber
Florian Pouchet Head of Cybersecurity & Operational Resilience UK, Wavestone
Raj Atwal Vice President, ISACA, Central UK Chapter
Ashley Lloyd Security Education and Culture Manager, BT Group

People are often described as the weakest link in cybersecurity, but they can also be an organisation's greatest defence. Managing human risk requires more than just security awareness training, it demands a deeper understanding of behaviour, decision-making, and how people interact with security controls.

This panel will explore practical strategies for identifying, assessing, and mitigating human risk. We will discuss how behavioural science, targeted interventions, and a culture of accountability can transform employees from potential security vulnerabilities into proactive defenders against cyber threats. Our panellists will share insights into the latest approaches to reducing human risk and strengthening organisational resilience.

11.30am **Tea, coffee, and networking break**

---

12 noon **Measuring what matters – Enhance security awareness through behavioural science and data**
Tim Ward CEO & Co-founder, Think Cyber

Traditional security awareness metrics often focus on surface-level indicators, such as training completion rates or phishing click rates, that fail to capture meaningful behavioural change. The key question is: Are you measuring performance or real impact? In this talk, Tim will discuss how to transition toward metrics that reflect genuine behavioural changes while ensuring compliance and effectively measuring the impact of your security awareness initiatives.

Tim will cover what to measure to provide deeper insights into security culture, the tools available for tracking progress over time, and how to present these findings effectively to leadership. By leveraging behavioural science and meaningful data, organisations can move beyond compliance and successfully influence employee behaviours, thereby reducing operational risks and enhancing their overall security posture.

12.30pm **Building cyber resilience: Protecting businesses in an evolving threat landscape**
Detective Inspector Michelle Ohren Managing Director, The Cyber Resilience Centre for the West Midlands

Small and medium-sized businesses are increasingly targeted by cybercriminals, yet many lack the resources and expertise to defend themselves effectively. In this session, Michelle will explore the latest cyber threats facing organisations and practical steps to strengthen resilience. This session will highlight real-world case studies, discuss common vulnerabilities exploited by attackers, and provide actionable guidance on threat prevention, incident response, and working with law enforcement. We will gain insights into how businesses can build stronger security postures, navigate emerging risks, and access support to enhance their overall cyber resilience.

1pm **Networking lunch**

1.45pm **Arctic Wolf Threat Report 2025: Threats and trends from the cyber frontline**
Ant Wells Senior Sales Engineer, Arctic Wolf

The 2025 Arctic Wolf Threat Report highlights how cybercriminals are evolving their tactics to bypass stronger security measures. Ransomware attacks now involve data theft in 96% of cases, reflecting a growing shift towards double extortion. Business Email Compromise (BEC) scams are becoming increasingly sophisticated, particularly targeting industries reliant on digital transactions. Attackers are also exploiting known vulnerabilities to infiltrate organisations worldwide.

Learn more from the report, including why it underscores the need for robust security operations, continuous monitoring, and proactive threat intelligence to strengthen organisational defences against these escalating threats.

2.15pm **Critical building blocks of resilience: People, relationships and culture**

Dr Morgan Bailey Senior Applied Behavioural Scientist and Psychologist, Social Machines

A significant part of cybersecurity often appears to have little to do with either "cyber" or "security". In this talk, Midori, an organisational psychologist, will explore how the foundations of an organisation's cyber resilience can stem from the attributes of its people, their relationships, and the culture they cultivate together. Drawing on behavioural science research and real-world case studies, she will examine how broader collaboration across disciplines and functions can contribute to building and sustaining this essential foundation.

2.45pm **Panel session: Working together to enhance resilience**

Facilitated by **Keith Hayes** ISACA Board Member, ISACA Central UK Chapter
Detective Inspector Michelle Ohren Managing Director, The Cyber Resilience Centre for the West Midlands
Thomas Owen CISO, SoSafe
Paul Spruce Principal Security Authority, BT Group
Jaimon Thomas Senior Director - Customer Engineering, Kudelski Security
Jonathan Randall Doctoral Student, Loughborough University

Resilience is no longer just an organisational priority, it's a shared responsibility across industries, supply chains, and sectors. As cyber threats grow more sophisticated and interconnected, collaboration has become essential in strengthening security postures and mitigating risks.

This panel will discuss how organisations can work together to enhance resilience. We will explore best practices for threat intelligence sharing, cross-sector collaboration, and strengthening supply chain security. Our panellists will share real-world examples of successful partnerships and the challenges that must be overcome to build a more secure, resilient digital ecosystem.

3.30pm **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 10,800+ 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…

Redflags from ThinkCyber
exabeam
WAVESTONE
sosafe
Qualys.
CROWDSTRIKE
RAPID7
semperis

Bridewell
CYBSAFE
censys
Vanta
elastic
S&W
jamf
Communicate
KUDELSKI SECURITY
ARCTIC WOLF
SOPHOS

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