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

# CISO Summit 2026

## Navigating Systemic Change

### In association with

Which?

Join us as we bring CISOs and senior security leaders together to explore how organisations can build resilience, trust, and capability amid rapid technological change, geopolitical uncertainty, and accelerating AI adoption.

Deep technical expertise, long seen as the priority for a CISO, is no longer enough to influence organisations to invest in cybersecurity. The board-savvy CISO needs to persuade peers and senior leaders, whose priorities are business delivery-focused, of the need to embed cybersecurity practices through everything they do.

This needs mature people leaders who can speak to the strategic imperative as a business ally. Incidents bring CISO roles into sharp focus, and as much as protecting the business, there is a need to protect the people who work within cybersecurity. Maintaining a functioning team, from a mental health and well-being perspective, through a 24/7 fight to evict threat actors from systems, requires a leader who has the trust of their team, has considered a contingency plan, and can maintain a mature leadership posture throughout.

Throughout the day, we will be addressing the shifting role of the CISO - from technical authority to strategic leader - with a strong emphasis on influence, people, and organisational culture.

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 9 July 2026**

**9am to 4pm**

**London**

# Chair

**Prof. Andrew Clark**, Content Advisor, The SASIG

---

**9am** **Registration, coffee, and networking**

---

**9.30am** **Welcome and introductions**
**Prof Andrew Clark** Content Advisor, The SASIG
**Simon Turner** Head of Infosec & Technical Risk, Which?

**9.45am** **Keynote presentation**
**Rocio Concha** Director of Advocacy, Which?

Which? is at the forefront of consumer affairs, the trusted independent voice so many rely on. Their work also provides direct consumer advocacy input to government, including across protecting the population as consumers of online services and the safe use of data and AI. Rocio's keynote will set the tone for the day for our community.

**10.15am** **Panel Session: Conscious Uncoupling for resilience?**
Facilitated by **Liz Murray** Chief of Staff, The SASIG
**Gary Osborn** Head of Information Security, Amnesty International
**Ade Clewlow MBE** Senior Advisor, NCC Group
**Adam Boynton** Enterprise Strategy Manager, Jamf

Recent conversations about organisational resilience have focused on whether there is a collective over-reliance on Big Tech amid current geopolitical uncertainty. We will consider to what extent our internal dependency on large technical organisations providing organisational infrastructure and services could undermine our resilience. Is there a way for CISOs to build resilience by uncoupling from global providers yet still maintain the operating capability they need?

---

**11am** **Tea, coffee, and networking break**

---

**11.30am** **When AI Gets Personal: fraud Visibility, Nudges, and Compliance Together**
**Tim Ward** CEO & Founder, Redflags

Organisations are losing visibility into how AI tools across the enterprise are being used. Tim will explore why real-time visibility into AI usage is now essential for security and compliance teams, because it allows them to see *who* are using *which* tools, how they are using them, and *when* risk is emerging before sensitive data is exposed or regulatory obligations are breached.

Using real-time visibility, contextual nudges, and human-centric intervention, teams can embed compliance into day-to-day operational practice and behaviour that guides users toward safer choices at the point of risk, aligned with the organisation's security strategy and culture.

**12noon** **Cyber in the Boardroom: Is your SLT ready for a crisis?**
**Ade Clewlow MBE** Senior Advisor, NCC Group

We explore how CISOs can better prepare the boardroom for a cyber crisis, focusing on the actions that matter *before* an incident occurs. It looks at how CISOs can better prepare the Leadership Team to respond calmly and effectively when the inevitable happens. Drawing on over five years of delivering Gold Team crisis exercises across multiple sectors, Ade will share practical insights into how boards typically engage with cyber risk and where this often falls short.

This session will examine how CISOs can frame cyber resilience and preparedness in a way that resonates with time-poor senior leaders, supporting more effective strategic decision-making when it matters most.

**12.30pm** **Case study and discussion: What can CISOs learn from fraud victims that can protect their people before, during and after a breach?**
**Matt Niblett** Senior Policy Advisor, Which?

This session takes a people-first look at cyber incidents, exploring what fraud victims' experiences reveal about the real human impact of breaches. We'll examine the emotional and mental health effects of fraud, and highlight how better communication, empathy and support can help CISOs protect their people before, during and after an incident.

---

**1pm** **Networking lunch**

---

**2pm** **Phishing Isn't an Email Problem — It's an Enterprise Risk Problem**
**James Hickey** Principal Sales Engineer, Cofense
Phishing has evolved beyond the inbox into an enterprise risk that exploits people, processes, and technology simultaneously impacting every function across the organisation. As AI-driven attacks rapidly shift across email, Smishing, Vishing, and exploit collaboration platforms, many think of it simply as a tooling and operational challenge which creates a false sense of security.

Leading organisations are reframing phishing within enterprise risk and resilience strategies, aligning controls to frameworks such as NIS2 and ISO, and shifting measurement away from "blocked emails" toward organisational readiness: speed and accuracy of detection, confidence in escalation paths, process integrity, ease of reporting, and the ability to contain and recover quickly.

**2.30pm** **Prompt behaviour: Why AI governance fails without behavioural security**
**Oz Alashe** CEO & Founder, Cybsafe

AI governance has a behaviour problem most frameworks haven't caught up with yet. The policy exists. The tooling is being deployed. Employees are still using unsanctioned AI tools because the approved ones are too slow, pasting client data into public models because it saves twenty minutes, or feeding sensitive documents into summarisers without a second thought about where that data goes.

Oz explores what a behavioural security approach to AI governance looks like: How to instrument what people do, intervene with precision, and prove the outcome.

**3pm** **Interactive session: Leading change through collaboration**
**Simon Turner** Head of Infosec & Technical Risk, Which?
**Kerrie Grier** Consultant, Which?

In many organisations, cybersecurity strategy is still shaped by aligning to overarching business and IT strategies. On paper, this makes sense. In practice, it often falls short. These strategies are frequently developed at a distance, at a high-level, idealised, and disconnected from the operational realities where security risks actually exist. The result is a cyber strategy that looks coherent but struggles to gain traction, relevance, or adoption.

This talk challenges that traditional “top-down” approach. Drawing on real-world experience, it argues that effective cybersecurity isn't built in isolation or derived solely from executive strategy decks, it’s built through collaboration.

**3.45pm** **Closing remarks**

---

**4pm** **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