

Hear first about SASIG events and industry news

Follow us on:



## Boardroom, Metrics & Measurements

The environment's evolving; context is everything.

In association with



As legislative requirements of board members deliver greater personal accountability, cybersecurity leaders need to move beyond technical reporting to provide senior executives with more meaningful insight into business impact.

Join us at this event where cyber leaders and change experts explore how to translate cyber activity into board-level insight that supports governance, accountability and leads to better business decisions. The CISO's role is shifting; previous "traditional" metrics will not withstand scrutiny or deliver the required risk outcomes, especially where national and international policies require more board oversight, understanding of technical complexity, associated risk and the possible requirement for change programmes to ensure the organisation can deliver for all stakeholders.

**Thursday 22 October 2026**

**9.30am to 4pm**

**London**

## Chair

**Liz Murray** Chief of Staff, The SASIG

---

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

---

**10.00am** Welcome and introductions

**Liz Murray** Chief of Staff, The SASIG

**Gavin Cartwright** Partner, EY Technology Solution

**10.15am** Keynote presentation: Are your controls out of control: the new threshold for managing and reporting controls

**Gavin Cartwright** Partner, EY Technology Solution

Controls are multiplying. Confidence isn't. As boards face growing accountability for cyber resilience, reporting can no longer be a catalogue of activities, exceptions and technical metrics. This session explores how organisations can cut through control complexity, focus on what truly matters, and deliver assurance that stands up to scrutiny. Gavin Cartwright will examine the emerging threshold for control effectiveness, board-level reporting and risk-informed decision-making, helping leaders shift the conversation from compliance and coverage to measurable business outcomes, resilience and trust.

**10.45am** Interactive session: The boardroom conversation - From reporting to advising

**Led by Helen Rabe** CISO, Ashurst Perkins Coie

### Helping Boards Make Effective Cyber Risk Decisions

This interactive discussion explores how CISOs can communicate cyber risk in a way that helps boards fulfil their governance responsibilities. Beyond metrics and dashboards, we'll examine how to provide strategic context, explain uncertainty, build confidence, and enable better executive decision-making. We'll discuss what boards genuinely need to hear, what they don't, and how experienced CISOs adapt their communication to become trusted advisers rather than technical reporters.

---

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

---

**12pm**      **Managing human risk: the three questions modern security leaders are asking more and more**

**Oz Alashe** CEO & Founder, Cybsafe

Cybersecurity continues to earn its place in the boardroom, but the human side of it still arrives there in a different currency from everything else. Technical risk gets reported in likelihood, impact and control effectiveness. Human risk gets reported in completion rates and simulated phishing metrics. As a result, it's simply not valued in the same way.

That isn't a communication failure. It's a measurement one. For years the field reported what its instruments could see, and those instruments could see very little.

This session looks at three questions security leaders and business executives are increasingly asking about human risk, and why most organisations struggle to answer any of them. Oz will show how SebDB, the open, free and vendor-neutral database of security behaviours, has developed from a list into a structured model connecting behaviours to threats, vulnerabilities, controls and risk outcomes. He'll also show how that structure lets a programme move from activity to evidence.

You'll leave with the three questions, a practical way to start answering them, and a clearer sense of what board-ready human risk reporting actually looks like.

**12.30pm**      **Measuring Frontier Model Impact**

**Ivan Milenkovic** VP, Cyber Risk Technology, Qualys

Most cyber risk scores are built to alert, not to measure. That's a problem the moment your CFO and/or board asks whether the security budget is paying off, or whether you're managing risk as tightly as any other line of business.

This session walks through a framework for measuring exposure with rigor across vulnerability, identity, and beyond, tied directly to your frameworks coverage and real-world loss data. You'll see how exposure connects to a number your CFO can reason about, and how that number holds up over time and across the business.

---

**1pm**      **Networking lunch**

---

**2pm**      **One Risk Rating, Across Every Exposure Discipline**

**Mark Constable-Weathers** Solution Architect, Kudelski

Security teams face growing volumes of vulnerabilities, misconfigurations and cloud and operational technology exposures, often managed through separate tools, scoring methods and backlogs. This fragmentation makes prioritisation difficult and leaves remediation teams unclear about what to address first. This presentation explores a unified exposure-management approach that correlates findings with threat intelligence, attack paths and business context, creating a common risk view that supports clearer ownership, focused remediation and measurable risk reduction.

**2.30pm**    **Why the board cares: Risk visibility, outcome-led compliance, and the evolving AI threat**

**Tim Ward** CEO & Co-founder, Redflags

Boards increasingly want evidence that security programmes are reducing risk, not just delivering training. As AI reshapes the workplace, organisations need greater visibility into workforce behaviours, measurable compliance outcomes, and meaningful metrics that demonstrate progress.

This session explores how Secure Behaviour Management helps organisations move from activity-based reporting to actionable business insights. We'll discuss how to uncover hidden risks, measure behaviour change, strengthen compliance through data-driven evidence, and report outcomes that resonate with senior leadership. We'll also examine how to adapt security strategies for AI-related risks and demonstrate measurable improvements in resilience, risk reduction, and overall security culture.

**3pm**    **The Human Factor in Cyber Governance: Bias, Behaviour and Board Decisions**

**Lilly Fogarty** Specialist in human security and social engineering, ex British Army

The greatest challenge facing modern cyber governance may not be the board's inability to understand technology, but its failure to recognise how human behaviour, cognitive bias and social conformity influence the decisions through which technological risk is governed.

This interactive session will engage and challenge your thinking about how we work together, alone, and how decisions are truly made.

---

**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](http://www.thesasig.com). Please register here for membership.

## With thanks to our Supporters and Contributors...



01234 707 035

[info@thesasig.com](mailto:info@thesasig.com)

[www.thesasig.com](http://www.thesasig.com)