

Hear first about SASIG events and industry news

Follow us on:



## **Scotland SASIG: Resilience and Preparedness - Strengthening Scotland's Cyber Defences**

**In association with**



SASIG has been proud to visit Scotland for many years now and we are delighted to visit Glasgow for the first time to coincide once again with Cyber Scotland Week. We are being hosted most generously by Scottish Power and are delighted to organise the day in partnership with ScotlandIS, the membership organisation representing Scotland's digital technologies industry.

Scotland has a strong, collaborative cybersecurity community driven by partnerships among industry, academia and government. Key components of this ecosystem include dedicated organisations, a robust academic research base and numerous networking events.

So join us as we explore how together, we can better prepare for the future and connect with our peers across the Scottish cybersecurity community. All SASIG events operate under the Chatham House Rule, and there is no charge to attend. Our hosts will kindly provide lunch and refreshments.

**Tuesday 24 February 2026**

**9am to 3pm**

**Glasgow**

# Chair

Liz Murray Chief of Staff, The SASIG

---

9am **Registration, coffee and networking**

---

9:30am **Welcome and introductions**

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

**Ross Galbraith**, Onshore Construction & Operations Director, ScottishPower

9:45am **Keynote: Powering a resilient future: Scottish leadership in cybersecurity**

**Lynda McQuilken**, Chief Information Security Officer, ScottishPower

How can energy giants like Scottish Power drive cybersecurity innovation in a world of interconnected risks? We consider the bold strategies shaping resilience at scale, fusing sustainability, cutting-edge technology and collaborative partnerships. We'll explore how leadership in energy translates to securing critical infrastructure, empowering communities and setting benchmarks for the industry. With an eye on the future, we discover how Scottish expertise is redefining security leadership in a rapidly evolving landscape.

10.15am **“Don’t sack the juggler”: Issues at the interface between resilience, business continuity, and crisis management**

**Professor Denis Fischbacher-Smith** Professor of Risk and Resilience, University of Glasgow

Using Ison’s notion of the practitioner as a juggler, we’ll consider the implications of the range of task demands that are often imposed on risk and security professionals within their organisations. The question of whether organisations ask too much of the security and risk function is a key challenge for practitioners. Denis points forward the case for a systems-based approach to dealing with the management of security- and risk-related issues, especially in terms of detection (the response to weak signals of threats) and the processes that underpin response, both of which require a holistic approach.

11.00am **Inside the CISO mindset: Research results on balancing priorities and sacrifices**

**Craig Hartwell** Major Account Director, Exabeam

A new survey of global CISOs conducted by Ten18 Research by Exabeam, uncovers how cybersecurity leaders are preparing for a rapidly shifting financial and threat landscape heading into 2026.

This session will explore the critical questions on every cybersecurity leader’s mind: How will economic pressures impact cybersecurity budgets? Which strategic priorities are likely to take centre stage? And, perhaps most importantly, where might CISOs be forced to make cuts? The discussion will also highlight some of the most insightful findings from the new global survey.

We will explore the themes driving this research, including growing board expectations, the need to prove ROI, the tension between modernisation and cost control, and the impact of emerging technologies like AI on spending strategies.

We'll also discuss the areas where CISOs anticipate the greatest pressure, from talent and tooling to cloud expansion and resilience requirements.

Attendees will gain a high-level view of the key decision points and constraints influencing CISO strategies in 2026 and learn what organisations should be ready to confront head-on.

---

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

---

**11.45am**     **Cyber Skills Poverty in OT – Is it really a thing?**

**Tim Harwood** CEO, Siker

Cyber skills poverty in OT is a growing problem but is it really just a case of not doing workforce development properly? By addressing this as an organisational goal rather than an individual want, we can ensure that organisations get the best bang for their buck.

**12.30pm**     **Identifying and Tackling bulletproof RDP persistent threats across the internet**

**Nick Palmer** Technical Director, Censys

We explore Censys' groundbreaking research into identifying and tracking bulletproof and abused RDP infrastructure across the internet. Using their extensive internet-wide data and honeypot telemetry, we'll reveal persistent RDP exposures linked to mass exploitation campaigns, the reliance of attacker networks on VPS and residential systems and emerging trends in abuse-tolerant hosting that sustain hard-to-takedown, long-lived infrastructure. Together, these critical insights expose how attackers operate at scale, to take away what evolving strategies are required to mitigate these threats effectively.

---

**1.15pm**     **Networking lunch**

---

**2.00pm**     **Strengthening Enterprise Trust, Resilience and Decision-Making with C2PA**

**Jon Renshaw** Director Security Research Services, NCC Group

C2PA is a strategic control that helps organisations strengthen enterprise trust in the content they create and consume. By enabling verifiable provenance and authenticity across digital assets, C2PA provides a reliable basis for assessing whether content can be trusted, reducing uncertainty during high-stakes operational and security decisions and building trust with their customers and suppliers.

NCC Group outline how C2PA supports outcomes CISOs care about:

- Risk Reduction & Resilience
- Supply Chain Assurance
- Compliance & Regulatory Readiness
- Trusted AI Adoption

Addressing the practical boundaries of C2PA and where it fits within a modern security architecture, how authenticity and provenance controls can reduce

operational and cyber risk, improve decision-making under pressure, enhance organisational resilience and digital.

**2.30pm**

**Panel session: Resilience, continuity, compliance and cyber insurance**

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

**Adam Boynton** Senior Security Strategy Manager, Jamf

**Garry Dalton**, Account Executive, Keegan & Pennykid

**Laura Irvine**, Managing Partner, Davidson Chalmers Stewart

In light of recent incidents across British retailers, cyber insurers are taking a closer look at organisations requesting insurance. What should businesses have in place to be able to understand Insurance requirements? Do these differ from their business continuity requirements, and how do organisations ensure that they are consistently resilient, not just compliant at the time of answering the insurance questionnaires?

---

**3pm**

**Finish**

---

# 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...



BREACHRX

