

Hear first about SASIG events and industry news

Follow us on:



## Scotland SASIG

### Building cyber resilience

#### In association with



We are delighted to return to Edinburgh for a second event hosted by Lloyds Banking Group this year. Understanding the delicate balance between awareness and resilience is paramount in a rapidly evolving cyber landscape. This event brings together experts to dissect the intricate relationship between these two pillars of cybersecurity. Our panel sessions and interactive simulations will provide invaluable insights into safeguarding critical infrastructure, protecting data integrity, and fortifying organisational defences.

We welcome several attendees from each organisation - security managers accompanied by their legal, HR, procurement/supply colleagues, etc. This combination has worked exceptionally well at a whole variety of SASIG events. It generates energised and productive discussions, and we know it has led to closer working relationships amongst those who have attended together. We wish to build upon this success, and your help will be most gratefully received. Join us as we explore how awareness and resilience converge to fortify our digital future against emerging threats.

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

**Thursday 5 September 2024**

**9.30am to 4pm**

**Edinburgh**

# Chair

Tarquin Folliss OBE Vice Chairman, The SASIG

---

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

---

10am **Welcome and introductions**  
Tarquin Folliss OBE Vice Chairman, The SASIG

10.10am **Opening keynote: Ensuring the integrity of critical national infrastructure (CNI) in the age of cyber threats**  
Malcolm Warr OBE Chair, CNI Scotland

Malcolm is a leading authority on cybersecurity CNI and will address the escalating cyber threats facing essential services and industries. With extensive experience, Malcolm will discuss critical topics, including the current cyber threat landscape, regulatory and policy frameworks, and future-proofing CNI.

He will share case studies and lessons learned from recent incidents, providing actionable insights for policymakers, industry leaders, and cybersecurity professionals. This keynote will emphasise the critical need for vigilance, collaboration, and strategic planning for our vital systems and services.

10.35am **Snapchat: Why your kids love it but you don't**  
Parven Kaur Founder, Kids n Clicks

As of September 2024, Snapchat boasts over 400 million daily active users, maintaining its stronghold among Generation Z. Known for its disappearing messages and creative filters, Snapchat remains a dominant force in the social media landscape, particularly among users aged 13-24, who make up nearly 60% of its user base. While the platform has evolved with new features like Stories and Spotlight, many outside its core demographic struggle to grasp its appeal and functionality.

Snapchat's popularity among younger users raises concerns about privacy, cyberbullying, and exposure to inappropriate content. Parven will delve into the hidden risks associated with Snapchat use by children and discuss strategies for parents to protect their kids, offering practical advice on monitoring app use and fostering open conversations about online safety.

11am **Panel session: How sure are you that you can trust your data?**  
Facilitated by Tarquin Folliss OBE Vice Chairman, The SASIG  
Arun Banerjee Cyber Risk Consulting Lead, Zurich Resilience Solutions  
James McGachie Partner, DLA Piper  
Jack Cavar Ethical Hacking Student, Abertay University

In an era of increasing cyber threats, data trustworthiness is paramount. This panel will delve into the cybersecurity aspects of ensuring data integrity, from preventing breaches to mitigating insider threats. We will discuss techniques for securing data, validating sources, and detecting anomalies. We'll also discuss best practices that fortify your data against cyberattacks and unauthorised access. We'll explore how robust cybersecurity measures can safeguard your data, ensuring it remains reliable and trustworthy.

---

**11.40am**     **Tea, coffee, and networking break**

---

**11.55am**     **Can a digital twin help you visualise and defend your network?**  
**Peter Hughes** Technical Director, Skybox Security

Large enterprise networks are so complex that gaining visibility and understanding of areas of risk can be almost impossible. Therefore, seeing – and fully comprehending – the organisational attack surface is critical to a successful security strategy.

A digital twin – effectively a working model of your network – could be the tool you need to identify threats and security weaknesses better. Discover how it provides a single source of truth and unprecedented visibility of the organisation's attack surface. Understand how modelling the network and creating a digital twin could help supercharge security and simplify compliance and change processes.

**12.20pm**     **Policing cybercrime – The challenges, ethical dilemmas, and possible solutions**  
**Detective Inspector Craig Potter** Police Scotland

Law enforcement faces many challenges when investing in cybercrime, including underreporting, poor engagement, lack of access to data, and legislative, jurisdictional, and international barriers.

How many decisions are made during the cyber incident response based on small-picture ethics, and how does this feed the cybercrime ecosystem? How could big-picture ethical decision-making impact the cybercrime ecosystem? What barriers could we remove to solving cybercrime and making the internet safer for everyone?

**12.45pm**     **Security Information and Event Management (SIEM) is not just for the brave**  
**Ben Oakley** Customer Solutions Engineer, Exabeam

There's a lot riding on the shoulders of your security operations team — protecting the organisation's reputation, safeguarding sensitive client information, and ensuring the ability to deliver products and services.

In this session, Ben will discuss the criticality of SIEM in building a strong defence against cyberattacks, whether you're a large enterprise with an experienced team or a smaller organisation with limited resources.

1.10pm

**Panel session: Awareness and resilience – two sides of the same coin**

Facilitated by **Professor Denis Fischbacher-Smith** Research Chair in Risk and Resilience, University of Glasgow

**Brett Taylor** SE Director, UKI, SentinelOne

**Dr Heather Anderson** Operations Director, Security and Resilience Research Centre, University of Strathclyde

**Kev Eley** VP of UKI, Exabeam

**Simon Hodgkinson** Strategic Advisor and ex-CISO BP, Semperis

A senior representative from the **Scottish Cyber Coordination Centre**

How can integrating awareness and resilience fortify your organisation against evolving cyber threats and ensure sustained security and operational continuity? We will look at resilience-building measures such as incident response planning, threat intelligence, continuous monitoring, and adaptive security frameworks.

---

1.50pm

**Networking lunch**

---

2.30pm

**Kaspersky Interactive Protection Simulation (KIPS)**

Facilitated by **Lee Rendell** Senior Pre-Sales Manager, and **Richard Porter** Head of Pre-Sales, Kaspersky

We will run an interactive simulation scenario based in Local Public Administration (LPA). This particular scenario was developed in partnership with the European Union Research and Innovation Program in accordance with GDPR compliance law.

Your team will represent a cybersecurity team responsible for protecting the Local Public Administration from cyberattacks and threats.

The LPA's most important asset is its reputation among its citizens. Can you protect your LPA from cyber threats, while also:

- Maintaining timely and efficient access to services?
- Protecting sensitive and personal information?
- Maintaining and operating LPA infrastructure within the confines of the law?

Your team's success will be measured based on its LPA's reputation. How will you fare against the attackers, scenarios, and other teams?

---

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 10,300+ 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...

