

Hear first about SASIG events and industry news

Follow us on:



SASIG of the North

Securing Critical Infrastructure in an AI world

In association with



We are delighted to return to Manchester for SASIG of the North, hosted by NCC Group.

As the world becomes increasingly AI-enabled and more dispersed in the way it operates, securing AI and using it safely means organisations require a clear view of their AI architecture and emerging agentic capabilities. AI delivers greater speed and efficiency but the convergence of IT and OT within the agentic space raises important questions about how far it may extend organisational risk.

Similarly, the recent Government focus on the North-West highlights the depth of capability beyond the capital. Does regional dispersal strengthen resilience or dilute security capacity. How far is business continuity enhanced, or is cyber posture endangered by moving away from a centralised London powerhouse where investment is attracted? Join us as we explore resilience, regional capability and security practice.

Thursday 19 November 2026

9.30am to 3.30pm

Manchester

Chair

Liz Murray Chief of Staff, The SASIG

9.30am Registration, coffee, and networking

10.00am Welcome and introductions

A senior representative of **NCC Group**

10.15am Keynote presentation: **Connected, automated, exposed? Navigating security and resilience in the IT/OT era**

Ray Robinson Global Director - OT Security, NCC Group

Euan Birch Head of Cyber Security Operations, Scottish Power

Explore how the convergence of IT and OT is reshaping the risk landscape for critical infrastructure organisations. From increased connectivity and remote operations to expanding supply chain dependencies and AI-enabled technologies, organisations are facing a new reality where cyber incidents can have direct operational, financial and safety consequences.

The session will examine why traditional approaches to security are no longer sufficient and how organisations must adapt their governance, resilience and risk management strategies to operate securely in a converged environment.

10.45am Panel discussion: **AI adoption is accelerating rapidly, but what does 'AI-ready' actually look like and how many organisations are truly there?**

Facilitated by Liz Murray Chief of Staff, SASIG

Dr Liz James Managing Security Consultant, NCC Group

Vladimir Kolla CSO & Co-founder, Patrowl

Florian Pouchet Head of cybersecurity and resilience UK, Wavestone

Fraser Whitfield VP Product, Qevlar AI

Does your organisation have a clear view of where AI is being used in its technical infrastructure? The guidance is to be “AI ready”, but what does readiness look like? Are we already past “AI Ready” to managing the AI environment that exists? This panel will look at the gap between ambition and operational maturity, the security implications of agentic and embedded AI, and the practical steps organisations can take to adopt AI safely, responsibly and resiliently.

11.30am Tea, coffee, and networking break

12pm

Rethinking Microsoft 365 security: Seven myths to leave behind

Sharon Breeze Manager, Sales Engineering, EMEA, Coreview

Here's a contradiction: the accounts that can rewrite your entire tenant, read executive mail, grant a rogue app persistence, or self-assign Global Admin - are often the least defended.

Findings from CoreViews 2026 survey of IT and security leaders show that while MFA is one of the most basic security controls, only 55% of organisations enforce MFA across 75 – 100% of their admin accounts. If it's not consistently enforced on the accounts with the largest blast radius, what else are you assuming is covered that isn't?

Join us to challenge common assumptions and show where mature Microsoft 365 programs often still have hidden gaps.

12.30pm

Cyber resilience for an AI world: The need for enterprise-grade security for all

Andy Lyon Senior Solutions Engineer, BroadCom, *brought to you by Arrow*

How has the rise of AI driven attacks changed both the threat landscape, and the approach businesses must take to protect themselves and their data? This presentation will provide an overview of the issues businesses face and provide advice on how to position themselves to combat the emerging threats.

1pm

Networking lunch

1.45pm

From blind spots to action: Rethinking risk-based exposure management

Fireside chat with a senior representative of **Qualys** and a **customer** representative

Security teams are drowning in vulnerability data but starving for clarity on what actually matters. As cloud adoption accelerates, identities multiply, and supply chains grow more complex, traditional vulnerability management struggles to keep pace with the true scale of organisational risk.

Risk-based exposure management helps security leaders move beyond endless patch lists to a prioritised, business-context view of exposure - spanning cloud, identity, and third-party risk. Drawing on real-world examples, we'll look at how regional security teams can build the operational resilience needed to detect, prioritise, and remediate what matters most, before attackers find it first.

2.15pm Mitigating risk in your supply chain. How insights into your 3rd parties can support compliance and risk management

Nick Palmer Technical Lead, Solutions Engineer, Censys

As organisations become increasingly dependent on third-party suppliers, their external attack surface can introduce risks that traditional supplier assessments struggle to identify. This session explores how security teams can move from periodic, questionnaire-led reviews towards continuous, evidence-based supplier risk management. We'll examine how internet intelligence can provide an outside-in view of suppliers' exposed infrastructure, vulnerabilities and potential security weaknesses. This visibility can help prioritise supplier risk, support more informed conversations with vendors, and enable security teams to identify emerging issues across their supply chain before they become incidents.

2.45pm Panel discussion: Shaping a resilient future: The North's role in securing the UK

Facilitated by Liz Murray Chief of Staff, SASIG

David Brown Associate Director and Senior Advisor, NCC Group

Prof Andrew Schofield Chair for North West Regional Defence and Security Cluster

Dan Giannasi Director, Cyber Resilience Centre for the North West

Geoff Hodge Head of Security, CMA

A recent governmental focus shift to the North West has highlighted the capability found outside of London. Is this providing resilience or diluting protection? The panel will consider the strategic implications for CNI, public and private sector in dispersing capabilities regionally.

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 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...



020 4583 5030

info@thesasig.com

www.thesasig.com