

Hear first about SASIG events and industry news

Follow us on:



SASIG of the North

Preparing people for technology's challenges

In association with



Technology is evolving at a dizzying pace. The emergence of AI in the popular imagination – thank you, ChatGPT! – has raised the spectre of machines replacing humans to the point of our extinction, but Skynet is not here yet, nor will it be for the foreseeable future. People will always be important in the risk equation. How we address the rise of machines has become a perennial question for society. How do we improve our awareness of the increasing threats in cyberspace? How do we identify and develop the new skills emerging technology demands? And how do we change our mindset to better prepare ourselves as organisations and individuals for the worst while continuing to hope for the best?

We are delighted our SASIG of the North is once again hosted by Unilever in the historic and beautiful surrounds of Port Sunlight, which exemplifies why people matter. We're also opening this event to non-SASIG members. Our speakers and panellists will consider how we can take the initiative on skills, make ourselves more resilient, and normalise incidents to tackle them more effectively. We will look at recently adopted technologies, their insecure legacies, how we can best mitigate this, and why the fundamentals of digital hygiene remain a constant that we must aspire to achieve.

All SASIG events operate under Chatham House Rule, and there is no charge to attend. Lunch and refreshments for the day are kindly provided by our hosts.

Tuesday 23 July 2024

9.30am to 3pm

Port Sunlight, Liverpool

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

Charlie Sinclair Cyber Security Senior Awareness & Engagement Manager, Unilever

10.15am **Opening keynote: The history of Unilever**

Matthew Powell Director of Cyber Centre of Excellence, Unilever

Looking back at the history of Unilever and how culture has been integral to its development.

10.35am **Fake IDs & bad behaviour: Does cyber maturity contain determined attackers?**

Dominic Carroll Director of Portfolio, e2e-assure

Would your cyber infrastructure stop a threat actor who has multi-factor authentication credentials? In this session we will explore the expanding market of stolen user credentials and how threat actors are utilising them to bypass multi-factor authentication. We will cover the most recent tactics threat actors are using to capture these details and break down the importance of speed in these scenarios to contain and disrupt attackers before damage can be done. We will also look at attack disruption scenarios and a model for gauging your current Threat Detection & Response maturity.

11.05am **Panel session: Developing resilience through your workforce**

Facilitated by **Tarquin Folliss OBE** Vice Chairman, The SASIG

Kerry Harrison Digital Skills Partnership Coordinator, Lancashire Enterprise Partnership

Caroline Palmer Security Engagement Manager, BT Group

Florian Pouchet Head of Cybersecurity & Operational Resilience UK, Wavestone

Robert O'Brien Founder and CEO, MetaCompliance

As technology evolves so must we. Innovation brings change not just in the way we carry out our business but the threats we face. Resilience is the buzzword now but we have to work at it, no more so than in developing the skills sets of our workforce to meet the challenges of tomorrow. The panel will explore how developing people is key to improving an organisation's resilience: upskilling the existing workforce, attracting and retaining new talent, developing a culture of learning and a community approach to cyberspace's shifting threat landscape.

11.45am **Tea, coffee, and networking break**

12 noon

Meet the North West Cyber Resilience Centre

Dan Giannasi Head of Cyber and Innovation, North West Cyber Resilience Centre

The Cyber Resilience Centres are police-led, not-for-profit organisations focused on reducing the vulnerability of SMEs and third-sector organisations to the most common types of cybercrime. We'll talk about current and future threats and how the centres have assisted UK businesses in protecting against and responding to fraud and cybercrime.

12.25pm

Panel session: Incident management – Preparation makes perfect

Facilitated by **Tarquin Folliss OBE** Vice Chairman, The SASIG

Dan Giannasi Head of Cyber and Innovation, North West Cyber Resilience Centre

Ted Cowell Director, S-RM

Dai Davis Partner, Percy Crow Davis & Co

How an organisation responds to an incident determines the speed of its recovery. Much of the spadework to be 'battle-ready' is done well in advance of an incident. Our panel will discuss the importance of preparation when it comes to incident management and what that means for an organisation: the importance of planning, defining roles and responsibilities, practising and having the right culture in place. 'Train hard, fight easy', as the military says, may prove to be the best way to minimise a breach's impact.

1.05pm

CNAPP for the hybrid cloud security

Mark McDaid EMEA Channel Business Manager, Uptycs

Many organisations transitioned to cloud computing using either one or more public clouds, some left on-premises, some of the environments that couldn't move to the cloud, or it just didn't make sense to move them to the cloud (commercially or technically). After about a decade of companies using the cloud, some workloads are being brought back to on-prem. Many CISOs aspire to secure the environment wherever it is on the journey (from code to runtime) constantly and at the same level with one tool.

In this session, Mark will explain how the same in-depth level of protection can be applied across the whole environment while controlling risk and compliance.

1.30pm

Networking lunch

2.10pm

Creating a strong in-market cyber presence

Rosse O'Neill Business Information Security Officer (BISO), Corporate Functions and AI, Unilever

In this session, Rosse will discuss the in-market cyber presence and how it is crucial for maintaining robust cybersecurity defences, enabling real-time monitoring and swift response to local threats. This proactive approach can help to safeguard sensitive data and ensure operational continuity in an increasingly digital world.

2.35pm

We are the champions

Tom Pool Culture Change and Engagement Lead, Unilever

Security champions play a vital role in fostering a culture of cybersecurity awareness within an organisation, bridging the gap between technical teams and other departments. In this session, Charlie and Tom will discuss how advocating for best practices and continuous education can help mitigate risks and enhance overall security posture.

3pm

End of meeting

About

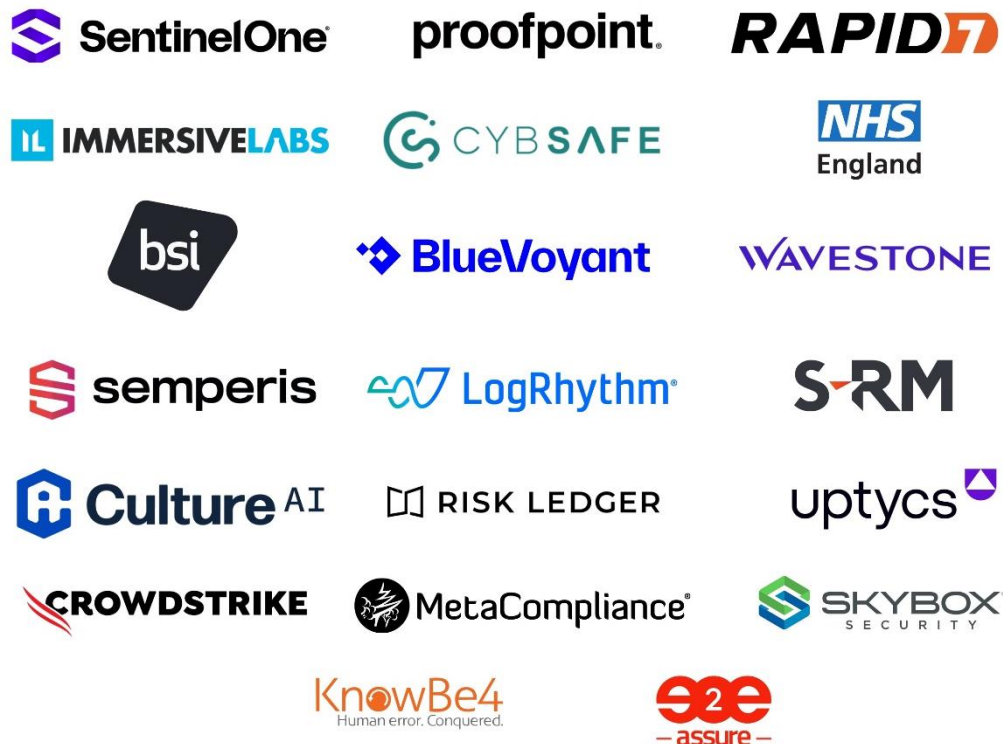


The Security Awareness Special Interest Group (SASIG)

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 10,200+ 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...



01234 707 035
info@thesasig.com
www.thesasig.com