Cyber leaders' summit
Laying strong foundations in a turbulent world

In association with

All businesses are reliant on technology to deliver their objectives. Innovation continues to advance, delivering technological capabilities that businesses must adopt to keep up with competitors. The velocity and scope of change are disruptive, but we also face an increasingly turbulent world producing new threats. Governments are responding to this by demanding that businesses put resilience front and centre in their strategy, making the emerging cyber threats business risks.

In our Cyber leaders' summit, we will consider the evolving regulatory and legal environment impacting how businesses view digital resilience, and how the board of directors' responsibility is growing to ensure that resilience is not just a performative exercise but an effective strategy to enable the business. We will also discuss how the threat landscape is in constant flux, as our adversaries exploit new technologies and a better understanding of us as targets to beat our defences.

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.

Friday 21 June 2024

9.30am to 4pm

Barbican, London

Chair

_____

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

_____

10am   **Welcome and introductions**
Martin Smith MBE Founder and Chairman, The SASIG
Ross McKean Partner, DLA Piper

10.15am   **Opening keynote: Governance – bringing order to an uncertain digital world**
Ross McKean Partner, DLA Piper

To stay ahead of the competition, there is a strong desire to deploy new technologies and to innovate. Launching quickly has been the norm, whilst safety and compliance have tended to be afterthoughts. The unprecedented availability and speed of adopting new technologies like large language model AI has also compounded this challenge. Greater dependency on IT and data also increases business resilience exposure. Regulators, customers and investors are more aware of and vocal about the need to effectively address these risks to ensure business resilience. In this session, Ross will consider how effective governance can help mitigate these risks and how effective governance is moving up the enforcement priorities for regulators.

10.45am   **Panel session: Regulation's implications on governance and risk**
Facilitated by **Benjamin Fellows** Legal Director, DLA Piper
Annick O'Brien General Counsel, CybSafe
Tom Russell Head of System Engagement, NHS England
Oliver Price Director - Cybersecurity Transformation, S-RM

Our panel will explore the intricate relationship between regulatory frameworks and governance-risk strategies. Through insightful discussions and real-world examples, our panel will comprehensively explain how evolving regulations shape organisational governance structures and risk management practices. We will delve into the challenges and opportunities of compliance requirements, highlight best practices for aligning regulatory compliance with broader governance objectives, and explore the dynamic landscape of regulation and its profound implications on fostering resilience, accountability, and sustainability within today's businesses.

_____

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

_____

12 noon   **Boards: It's time to step up and take ownership of cybersecurity**
Ursula Morgenstern Business Mentor and Advisor, Thinker Systems

In today's digital landscape, cybersecurity threats are evolving rapidly, posing significant risks to organisations worldwide. Boards must recognise their role in safeguarding their organisations against these threats. Despite challenges like technical expertise gaps, boards must integrate cybersecurity into agendas and collaborate with leadership and IT teams. We'll uncover knowledge and tools to take proactive steps in addressing cybersecurity risks and protecting your organisation's assets and reputation in today's digital landscape.

12.30pm   **What does the evolution of identity-based attacks mean for your data?**
Luke Jennings VP, Research & Development, Push Security

The leading cause of breaches remains identity-based attacks, with four out of five involving identity-based techniques. Whilst these types of attacks have been recorded as a key cyber risk for many years, the shift away from traditional networking to cloud-native and SaaS applications has increased both the likelihood and impact of identity-based attacks. Many of these techniques have been historically labelled 'unsophisticated', but recent high-profile breaches demonstrate how these techniques remain as effective as ever, and how attackers are moving away from conventional methods to target identity infrastructure. It's vital that organisations recognise these shifts to be able to detect and respond effectively.

_____

1pm   **Lunch and networking break**
_____

1.45pm   **Panel session: Adapting your response in an ever-changing threat landscape**
Facilitated by **David Cook** Partner, Contentious Cyber Security and Data Protection, DLA Piper
Peter Hughes Technical Director, Skybox Security
Keith Poyser AVP Northern Europe, SentinelOne
Further panellists to be announced

This panel session will navigate the complexities of cybersecurity in an ever-changing threat environment. Our panel will share insights into the adaptive strategies necessary for effectively responding to emerging threats. Through real-world examples and interactive discussions, they will demonstrate how to identify, assess, and mitigate evolving cyber risks. The session will delve into the importance of agility in incident response frameworks, emphasising the need for continuous learning and proactive adaptation. Our panel will also explore innovative approaches and best practices for staying ahead of the curve in the face of relentless cyber challenges.

2.30pm   **What is Zero Trust?**
A senior representative from **Commvault**

From foundational concepts to practical implementation strategies, this session will explore how Zero Trust challenges traditional perimeter-based security models and offers a paradigm shift towards continuous verification and least-privilege access. Commvault will unravel the essence of Zero Trust and uncover how organisations should embrace this transformative mindset to safeguard their digital assets against evolving threats.

_____

3pm   **End of meeting and networking**
_____

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 9,900+ 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