Hear first about SASIG events and industry news
Follow us on:

Managing risk in cyberspace

What risk quantification can teach us

In association with

LLOYD'S

Cybersecurity is often viewed through the lenses of threats and vulnerabilities. However, understanding cyber risk should also involve balancing impact and probability. Discussions about cyber risk are frequently bogged down by technical jargon about exploits, malware, and vulnerabilities, making it difficult for executive decision-makers to grasp and manage these risks effectively.

To address this, we need to quantify cyber risk and make it align with our business strategy. By doing so, we can make informed decisions about security investments and enhance our resilience. Quantifying risk allows us to better understand the weighted potential impact and likelihood of cyber threats, enabling leaders to prioritise scarce resources and develop strategies more efficiently. This approach not only helps in managing cyber risk but also in improving overall organisational resilience. This event will explore these critical topics and provide insights into a more effective approach to cyber risk management.

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.

Thursday 24 April 2025

9.30am to 5pm

City of London

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
A senior representative from **Lloyd's of London**

10.10am **Keynote presentation: Security metrics - The journey towards risk quantification**
Aris Matthidis Group CISO, Tokio Marine Kiln

Effective cybersecurity decision-making relies on meaningful metrics, yet many organisations struggle to measure performance beyond compliance checklists and technical indicators. As cyber threats grow more complex, shifting from traditional metrics to risk-based quantification is becoming essential. In this session, Aris will explore the evolving role of security metrics in risk management, the challenges of generating insightful measurements, and how automation can improve these frameworks. We will gain insights into how data-driven approaches can enhance risk assessment, support more informed decisions, and bridge the gap between security teams and business leaders.

10.40am **Fireside chat: Human-centred security - the role of behaviour in risk reduction**
Pierre Noel Group Chief Resilience Officer, CISO and Chief Privacy Officer, Le Collectionist
Simon Culliton Sales Director, SoSafe

With over 35 years of experience in cybersecurity, Pierre has advised global organisations on managing digital risk. As a SoSafe customer, he joins Simon to discuss the critical role of human behaviour in risk reduction. Drawing from his work across finance, technology, and government, Pierre will share insights on embedding security awareness into corporate culture. This fireside chat explores how organisations can proactively reduce risk by turning employees into a resilient first line of defence.

11.10am **Panel session: Insuring the digital age - Quantifying cyber risk**
Facilitated by **Dr Lucy Fraser** Senior Policy Adviser, General Insurance Policy, Association of British Insurers (ABI)
Henry Skeoch Cyber Exposure Management Lead, Beazley
Luke Fardell Lead Cyber Analyst, Tokio Marine Kiln
Elspeth Robertson Cyber Risk Advisor, Lockton

As cyber threats evolve, organisations face growing pressure to quantify cyber risk. Cyber insurance is crucial for managing financial impacts, but without clear risk metrics, securing the right coverage and demonstrating ROI is challenging.

Our panellists will explore how businesses can assess and quantify their cyber risks, the role of data-driven risk modelling, and the impact of evolving threats on cyber insurance. We will gain insights into building a risk-aware culture, aligning security investments with business priorities, and navigating the complexities of cyber insurance today.

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

12 noon **Future proofing risk management through quantification: Practically applying the FAIR methodology**
Rob Moore Vice President, Mastercard Technology Risk

This session explores how organisations can future-proof their risk management strategies by adopting a quantified approach using the FAIR (Factor Analysis of Information Risk) methodology. Rob will cover practical applications of FAIR, demonstrating how businesses can move beyond qualitative assessments to measurable, data-driven risk decisions. He will highlight real-world examples, benefits of risk quantification, and how FAIR can improve communication with stakeholders and enhance strategic decision-making.

12.30pm **Panel session: Innovation and risk quantification in cyber**
Facilitated by **Tarquin Folliss OBE** Vice Chairman, The SASIG
David White President, Axio
Peter Dyson Head of Analytics, Kovrr
Justin Jones Managing Director, Social Machines
James Hanbury Global Lead Director, KPMG Cyber Risk Insights

As cyber threats evolve, organisations must adopt innovative approaches to risk quantification to better understand, manage, and mitigate potential impacts. Traditional methods of assessing cyber risk often fall short in translating technical vulnerabilities into meaningful business insights.

This session will explore the latest advancements in cyber risk quantification, highlighting how data-driven models, automation, and emerging technologies are reshaping risk assessment. Our panel will discuss how organisations can leverage innovation to enhance decision-making, improve resilience, and align cybersecurity strategies with business objectives.

1pm **Why bother with security awareness? Delivering measurable behaviour change**
Lucy Finlay Delivery Director for Secure Behaviours and Analytics, Think Cyber

In this presentation, Lucy will explore the reasons behind implementing security awareness programmes in organisations. Is it simply about compliance, or does it play a deeper role in empowering employees to protect both sensitive information and themselves?

Lucy will address the fundamental question: Why invest in security awareness training? She will examine how to ensure these programmes are effective by focusing on the science behind how people learn and retain security knowledge. Using insights from behavioural science, she will discuss how organisations can drive meaningful behaviour change, reduce operational risks, and strengthen overall security resilience.

1.30pm **Networking lunch**

2.10pm **From words to figures and back: The art of cyber risk management**
Ivan Milenkovic VP Cyber Risk Technology, Qualys

Ever faced the "And so what?" wall? Learn how to bridge the gap between qualitative insights and quantitative analysis to enable business-aligned cyber risk management. This session will explore practical techniques to translate stakeholder concerns into actionable risk scenarios using qualitative methods and then quantify those scenarios to demonstrate tangible impacts that resonate with business leaders.

We'll also focus on how to effectively communicate quantified insights through clear, compelling narratives that engage stakeholders. It's the Q^3 sandwich: turning qualitative insights into a quantitative risk register and then translating those numbers back into influential stories and qualitative scorecards that support informed cybersecurity decision-making.

2.40pm **Risky business: The prejudices and pitfalls of cyber risk planning**
Jonathan Mattey Head of Cyber Security, Forge Holiday Group

Effective cyber risk planning is often hindered by unconscious biases, flawed methodologies, and reliance on qualitative assessments that lack precision. These challenges can lead to misjudged threats, misplaced investments, and poor communication between security teams and business leaders.

In this session, Jonathan will explore how unconscious biases shape risk perception, the limitations of traditional qualitative approaches, and how they impact decision-making. He will also discuss practical steps towards risk quantification, demonstrating how a data-driven approach can enhance clarity, improve security investments, and strengthen organisational resilience. We will gain insights into refining cyber risk strategies to make more informed, objective, and effective security decisions.

3.10pm **The exposure evolution: Transforming vulnerability management through proactive risk assessment**
Jamie Cowper Director of Product Marketing, Rapid7

This session aligns Gartner's exposure management framework with current security practices, highlighting the strategic role of Cyber Asset Attack Surface Management (CAASM). Shift from reacting to threats to preventing them. Jamie will explore how to gain complete visibility of your systems, understand your risks, and address vulnerabilities before they can be exploited.

3.40pm **Tea, coffee, and networking break**

4pm **Validating cybersecurity strategy and tracking risk reduction: Making company decisions with CRQ**

Michael Paisley Chief Security & Resilience Officer, Mimecast

Cyber risk quantification (CRQ) is transforming how organisations validate their cybersecurity strategies and measure risk reduction. This session will explore how businesses can leverage CRQ to make data-driven security decisions, prioritise investments, and demonstrate the impact of their cybersecurity efforts. Attendees will gain insights into best practices for tracking risk reduction, aligning security with business objectives, and improving overall resilience.

4.30pm **Closing keynote: Learning from the mistakes of others – A retrospective review**

Stephen Bonner Deputy Commissioner, Information Commissioner's Office

Cybersecurity is horrifically complicated. Isn't it? But through transparency, cooperation, and simply sticking to the script, organisations can significantly reduce their risk.

External threats are on the rise, yet many cybersecurity incidents still stem from poor decision-making by those trying to defend against them. Why does the narrative so often see the innocent becoming victims while bad actors escape unscathed?

Stephen will share real-world examples of the alarming situations he encounters in his work and reveal how many of these incidents could have been avoided.

(Warning: this presentation may contain the use of frighteningly bad passwords.)

5pm **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 10,700+ 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…

SentinelOne · exabeam · RAPID7

Redflags from ThinkCyber · SKYBOX SECURITY · KnowBe4 Human error. Conquered.

CROWDSTRIKE · semperis · WAVESTONE

sosafe · MetaCompliance · e2e assure

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