

Hear first about SASIG events and industry news

Follow us on:



Financial Services SASIG

Managing change in an ever-changing world

In association with



Much has changed (and much has not) since our last Financial SASIG. The UK has a new government with a significant mandate. Donald Trump, against the odds, was elected for a second presidential term in the United States. Meanwhile, the wars in Ukraine and the Middle East continue to rage and political crises stalk Germany and France. In the business world, emerging technology continues to pose risks as well as present opportunities. Generative AI is firmly established as a business driver but presents its unique challenges. Cybercrime remains a growing problem, with fraud arguably replacing ransomware as its most damaging manifestation.

The requirement for organisations to improve their resilience against external shocks has never been greater. AI is making threats more complex and enabling bad actors to spot vulnerabilities more quickly. Data integrity is even more critical now that it underpins the decisions AI makes, and on which we are increasingly reliant. We understand that resilience is underpinned by preparedness and collaboration, but both of these present their own challenges to many organisations. In all these areas, the financial sector leads others. We are delighted to host our Financial SASIG with Evelyn Partners and to learn from the sector's experience so that we can manage change while continuing to keep ourselves resilient and our clients secure.

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 30 January 2025

9.30am to 5pm

City of London

Chair

Martin Smith MBE Chairman and Founder, The SASIG

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

10am **Welcome and introductions**

Martin Smith MBE Chairman and Founder, The SASIG

Mark Hendry Partner, Evelyn Partners

10.15am **Fireside chat: Cyber resilience in 2025 and beyond - the CISO and the advisor**

Mark Hendry Partner, Evelyn Partners

Steve Hill Former CISO, Credit Suisse

Financial services lead the economy in cyber resilience, setting the standard for other sectors. However, the industry must continuously adapt to a rapidly changing landscape of threats, risks, regulatory pressures, and evolving technological capabilities. In this fireside chat, we will explore these critical issues through the unique perspectives of a seasoned CISO and a trusted advisor. Together, they will discuss how financial organisations can stay ahead of emerging challenges, enhance resilience, and navigate the complexities of modern cybersecurity.

10.45am **From risk to resilience: Safeguarding the financial services industry**

Dominic Carroll Director of Portfolio, e2e-assure

This session, presented by e2e-assure, is a masterclass in building the ultimate foundation of resilience and resistance tailored to the financial services industry. After identifying the key threats, we will gain a comprehensive understanding of the four core enemies of cybersecurity: volatility, uncertainty, complexity, and ambiguity. The session provides actionable insights on how to utilise cyber defence and threat intelligence within your business to not only mitigate these threats but actively combat them.

11.15am **Fireside Chat: The Institute of Chartered Accountants England and Wales' Story - using SIEM for SOC-cess**

Kev Eley VP UKI, Exabeam

David Graves Security Architect, Institute of Chartered Accountants England and Wales (ICAEW)

During this discussion, get a first-hand perspective of the journey taken by the ICAEW to manage and enhance its security operations center for faster and more efficient threat detection, investigation, and response of today's cyber threats. Hear about their day-to-day challenges and resolutions, as well as the best practices that have been implemented. Learn about how their SOC team is effectively utilising a SIEM solution with automation and advanced analytics to improve the organization's overall security posture, enabling it to protect its critical data with confidence.

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

12.15pm **Panel session: How is technological innovation impacting the financial sector?**

Facilitated by **Martin Smith MBE** Chairman and Founder, The SASIG

Florian Pouchet Associate Partner, Wavestone

Sofia Ylén-Buxton Associate Director, Cybersecurity Awareness and Training, FactSet UK Limited

Kulwinder Johal Head of Technology GRC, Coventry Building Society

The financial services industry is being transformed by tech, driving both opportunities and challenges. In this panel, our industry experts will explore how emerging technologies such as AI, blockchain, and automation are reshaping financial operations, customer experiences, and cybersecurity practices. We will focus on the risks and benefits of these innovations, including the impact on regulatory compliance, data security, and operational efficiency. Our aim will be to gain a deeper understanding of how to harness new technologies while safeguarding against potential vulnerabilities in a rapidly evolving landscape.

12.45pm **Communicating risk and securing your data**

Nick Palmer Technical Director, Censys

Companies in the finance and insurance sector face a complex landscape of risk management and third-party security. Security leaders are tasked with effectively managing their own risks as well as those of third-party providers, while protecting financial data from potential security threats.

Nick will highlight the urgent need for action, drawing on recent studies that explore threat trends such as compromised third-party providers, data theft, unpatched systems, outdated technology, data breaches, and vulnerabilities. We will gain insights into effective and DORA-compliant responses to threats and explore how to proactively identify and address risks.

1.15pm **Enabling cybersecurity automation**

Peter Hughes Technical Director, Skybox Security

TV and films often portray cybersecurity as a thrilling battle between good and evil. However, much of the work carried out by cybersecurity analysts is less glamorous, time-consuming, and repetitive. Organisations face common cybersecurity challenges, including:

- Complex IT, OT, and IoT infrastructures, on-premises and in the cloud
- An increasing number of threats and vulnerabilities
- Rising regulatory and compliance requirements
- A global shortage of cybersecurity skills

Automation helps organisations address many security processes, including visualising the attack surface, quantifying cyber risks, identifying vulnerabilities, ensuring compliance, and managing changes. Certain analyses, like exposure and access path analysis, would be nearly impossible without automation. By automating repetitive tasks, cybersecurity teams can focus on more dynamic challenges.

1.45pm

Networking lunch

2.30pm

Panel session: Protecting the integrity of your data

Facilitated by **Martin Smith MBE** Chairman and Founder, The SASIG

Haydn Brooks CEO, Risk Ledger

Simon Mair Independent CISO

Mark Hamill VP Product, MetaCompliance

Data integrity is vital for maintaining trust and compliance in the financial services sector. This panel will explore practical approaches to safeguarding data against evolving cyber threats, including third-party risks, insider vulnerabilities, and compliance challenges. We will discuss strategies for mitigating risks from compromised providers, ensuring robust governance, and leveraging automation to enhance accuracy and security. We will uncover how to protect sensitive financial information while meeting regulatory expectations.

3pm

Delivering cloud (public and private) security with real-time compliance for financial organisations

Ronnen Brunner SVP Global Sales, Uptycs

Financial organisations face unprecedented challenges in maintaining security and compliance amid rapid technological advancements, hybrid cloud adoption, and evolving regulatory demands. This session will explore strategies to achieve enhanced visibility across public and private cloud infrastructures, monitor compliance in real-time, and manage risks effectively.

Ronnen will share insights on how organisations navigate the complexities of multi-cloud security and prepare for regulatory frameworks like DORA, with case studies from industry leaders.

3.30pm

The cyberattack playbook: Malware, credential theft and social engineering

Derek Pillar Regional Security – Manager, Mastercard

Cybercrime and cyberattacks have emerged as major global threats, targeting individuals, businesses, and governments alike. These malicious activities encompass a wide range of actions, from data theft to large-scale attacks on critical infrastructure. The rapid advancement of technology and growing dependence on digital systems have made safeguarding sensitive information increasingly challenging. Effective solutions include enhancing cybersecurity measures, deploying robust encryption techniques, and raising public awareness about safe online practices. Collaboration between governments and the private sector is essential to establish effective regulations and response strategies.

4pm

Attackers don't hack in, they log in: The evolution of identity attacks

Luke Jennings Vice President, Research & Development, Push Security

The major cybersecurity stories from 2024 revolved around identity attacks, with infostealer campaigns and credential theft on an industrial scale, a booming underground marketplace for stolen data, and MFA-bypassing AitM and BitM phishing techniques becoming the new normal. In this talk, we'll discuss why attackers are increasingly focused on account takeover rather than traditional endpoint compromise, and demonstrate some of the techniques enabling attackers to turn identity attacks into mass data theft and extortion opportunities.

4.30pm

Panel session: Threat discovery is more than threat intelligence

Facilitated by **Lesley Charteris** Cyber Human Factors Manager, Canopus Group

Stuart Wiggins Specialist Sales Manager, CAO, CrowdStrike

Nick Palmer Technical Director, Censys

Tom Garnett CEO & Co-founder, Refute

Threat intelligence is crucial for identifying cyber risks, but effective discovery requires a comprehensive approach. Our panel will explore how organisations can combine intelligence, behavioural analytics, automated systems, and real-time monitoring to uncover hidden threats. Experts will discuss the limitations of traditional threat intelligence and share insights on leveraging advanced tools and methodologies to improve discovery and response. Learn how to enhance your security posture with a holistic approach to threat detection.

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...

