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

Operational Resilience

Using the tools at your disposal to prepare for the worst

In association with

"Train hard, fight easy" is a quote attributed to the 18th-century Russian general Alexander Suvorov, and it has become the mantra for militaries worldwide. But how many organisations do this, or indeed have the capacity to? It is an overused cliché in cybersecurity that there are two groups of organisations: those who have been hacked and those who don't know they've been hacked. Like all cliches, this is laden with lazy assumptions but also an element of truth. For all organisations, it is not just a matter of if a cyber event will occur but when. This may be a grim thought, but there are many ways to minimise the disruptive impact of cyber events. So what other tools are in our armouries to enable us to better prepare for the inevitable?

We are delighted to work in association with Ernst and Young for our SASIG event on Operational Resilience. We will explore how understanding the regulatory environment can help you improve your cyber posture and how a transparent and collaborative approach to the security of your supply chains can help expose and mitigate vulnerabilities. We'll also look at the implications of emerging technology on resilience, why understanding your network and who access it is still key, and why prior planning and preparation can prevent poor performance on a crucial day.

All SASIG events operate under Chatham House Rule, and there is no charge to attend.

Tuesday 9 January 2024

10am to 2.15pm

Now online only, exclusively for our members

Chair

Tarquin Folliss OBE Vice Chairman, The SASIG

10am **Welcome and introductions**
Tarquin Folliss OBE Vice Chairman, The SASIG
Dominic Fortescue Partner, EY Financial Services

10.15am **Keynote presentation: DORA, regulation and what it means for operational resilience**
Gunjan Sharma Senior Manager, EY Technology Solutions

A raft of new regulations are on the horizon, not least the EU's Digital Operational Resilience Act, which will impact how organisations operate in the UK and the European Union. DORA is an ambitious attempt to mandate operational resilience, particularly around incident response and recovery. Our keynote speech will highlight the implications of DORA for businesses and its hoped-for influence on an organisation's resilience and approach to cybersecurity.

10.45am **Operational resilience benchmark 2023 results and 2024 outlook: What will operational resilience look like towards 2026**
Roxane Bohin Manager, Cybersecurity UK, Wavestone
Suman Dogra Gaur Manager, Cybersecurity UK, Wavestone

In this session, Roxane and Suman will present the key market insights from their annual Operational Resilience Market Benchmark, published in 2023. They will cover a case study of a global firm balancing regulatory compliance initiatives across multiple jurisdictions and the challenge of scoping a set of priorities for the next strategic cycle towards 2026. They will conclude by laying out their view on the short to medium-term future of the market.

11.15am **Panel session: Insights into supply chain vulnerability**
Facilitated by **Tarquin Folliss OBE** Vice Chairman, The SASIG
Jon Leather Head of European Supply Chain Defence Advisory, BlueVoyant
Tynan Beresford-Wylie Director, EY Technology Solutions
Sharon Penfold Interim Director, Independent
Helen Barge Cyber Security Representative, Federation of Small Businesses

Supply chains are key to most if not all, organisations. We are increasingly dependent on them in the physical and virtual worlds to provide specialist capability and our basic needs to function. But do organisations fully understand their supply chain, where the vulnerabilities exist and how they can compromise business as usual? Our panel will consider how best to understand one's supply chain, the importance of transparency, the role of threat intelligence in identifying risk, and how best to communicate information and best practices to mitigate the threat nascent in our third-party providers.

---

12 noon **Tea, coffee, and comfort break**

12.15pm **From 2023's reality to 2024's possibilities**
David Emm Principal Security Researcher, Kaspersky

In this session, Kaspersky reveals their 2024 cybersecurity predictions and reflects on last year's forecasts, identifying significant topics that weren't anticipated. Join us to discover what's on the horizon and gain insights into ever-evolving cybersecurity aspects.

12.45pm **The never-ending game**
David Hitchen Senior Solutions Architect, Semperis

The never-ending game of operational resilience and how frameworks like DORA and NIS 2 help everyone, from culture to processes. But what happens when it all goes wrong? In this session, David will discuss the essential business services that must be protected and how to adapt to the ever-changing threat landscape constantly.

1.15pm **Panel session: Why exercising and incident response plans are so important?**
Facilitated by **Tarquin Folliss OBE** Vice Chairman, The SASIG
Stewart Room Global Technology Sector Leader, DWF Law
Alessandro Frenza Director, Cyber Security, Financial Services, EY Technology Solutions
Daniel Potter Sr Director of Operational Resilience, Immersive Labs
Elizabeth Green EMEA Advisory & Cyber Lead, Dell Technologies

Responding swiftly and effectively to a cyber incident can be the difference between disaster and recovery. Playbooks, incident response, business continuity, and disaster recovery are part of most organisations' GRC packs, but for those who must put them into effect during a crisis, how familiar are they? Dusting down your playbook as an event materialises is hardly a recipe for resilience. Our panel discusses the importance of preparing for an incident, the value of proactive testing and exercising and how practice does indeed make perfect.

2.15pm **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 9,100+ 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…

ESET · SentinelOne · proofpoint · IMMERSIVELABS · CYBSAFE · NHS England · bsi. · BlueVoyant · Redflags from ThinkCyber · Valarian · TESSIAN · The Positive Way WAVESTONE · semperis · LogRhythm · S-RM · Culture AI

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