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

Artificial Intelligence:

Understanding implications for digital resilience

Artificial intelligence constantly makes the news, but AI and machine learning are not new phenomena. Although the majority of 'pundits' issue dire, apocalyptic warnings about their impact on the future of humanity, these technologies have been with us for some time, whether as algorithms to beat chess grandmasters or as software capable of analysing vast amounts of data with an accuracy and speed beyond that of a human. AI is, in many ways, an accurate cybernetic technology.

Generative AI's evolution has accelerated the public debate and will undoubtedly continue to impact the global economy and our societies significantly. But history has taught us that the threat is how humans implement and evolve technology, not the technology itself. AI will certainly further enable bad actors with adaptive malware, deep-fake phishing campaigns and accelerated brute-force attacks, to name but a few. However, it will also enable defences, improve our resilience, maximise our ability to answer challenges and deliver further technological advances. In the aftermath of the International AI Summit at the National Museum of Computing on 2 November, this conference will discuss AI's good and bad implications and explore how we can maximise this evolving technology to enhance our security.

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.

Kindly hosted by

FT FINANCIAL TIMES

Thursday 23 November 2023

9.30am to 3pm

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
Michael Heritage Vice President Cyber Security, Financial Times

10.15am **Keynote presentation: AI, what it means and its implications for security**
Dr Andrew Rogoyski Innovation Strategy Lead, The Surrey Institute for People-Centred AI, University of Surrey

In what promises to be the most disruptive year in the field of AI, Andrew will talk about developments in AI over the last 12 months, exploring developments that have surprised people and others that have not. He will explore some of the implications of AI for digital security, highlighting some new threats but also reminding us that some of the problems are age-old and, as ever, depend on the behaviours of human beings.

10.45am **Cybersecurity in the age of generative AI: Risks, opportunities, and practical solutions**
Florian Pouchet Head of Cybersecurity and Operational Resilience UK, Wavestone

Join Florian as he dives into practical aspects of AI adoption. Consider adopting the "secure by design" approach to assess AI-related risks and effectively establish tailored AI-specific controls. Witness a live demo of CISO-GPT, a generative AI Chatbot helping the CISO question the content of its documentation corpus.

11.15am **Panel session: The lazy chimp – AI and humans**
Facilitated by **Dr Andrew Rogoyski** Innovation Strategy Lead, The Surrey Institute for People-Centred AI, University of Surrey
Boris Taratine Cybersecurity Thought Leader
Michael Heritage Vice President Cyber Security, Financial Times
David Hitchen Senior Solutions Architect, Semperis
Dan Linder Senior Director of Data Science, Tessian

AI has emerged as the ‘next big tech thing’ in the public’s mind with all the attendant hyperbole. The focus is on technology and what it will mean for good or bad, but there is a danger we overlook, yet again – the relationship between technology and humans. Regarding technology adoption, the lazy chimp in us loves convenience to the exclusion of deep understanding. What are the risks of this approach? And what can we do to minimise them?

---

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

12.15pm **AI and deception in cybersecurity**
Boris Taratine Cybersecurity Thought Leader

Boris will discuss the interplay between AI and deception as a powerful means for adaptation in attack and defence, from four essential aspects: deception against user; deception against AI; AI-based deception; and AI-based defence. Underpinned by fully-referenced academic research into technology and human behaviour – the susceptibility of human traits, machines, and algorithms to deception – this session focuses on manipulating the user-computer interface to breach a computer system's information security through user deception and the 'other way around'.

12.45pm **Panel session: AI: New challenges, new mitigations?**
Facilitated by **Tarquin Folliss OBE** Vice Chairman, The SASIG
Liz Banbury CISO, Hiscox Insurance
Dai Davis Partner, Percy Crow Davis & Co
Jenna Franklin Partner in Data, Privacy, Cyber, AI and Ethics, Stephenson Harwood
Richard Bach Partner, Heligan

AI is evolving at an extraordinary pace, presenting both opportunities and challenges. So, what should the CISO consider when it comes to AI? Governments are waking up to the threats AI may deliver, hence the recent diplomatic initiatives to achieve consensus on developing AI safely and responsibly. Our panel will discuss the challenges and opportunities we can see, explore what may arise in the future, and consider how best to mitigate and exploit AI's risks and benefits to ensure we remain resilient as organisations and as societies.

1.30pm **Case study: AI voice cloning and financial fraud**
Jake Moore Global Cybersecurity Advisor, ESET

In a recent case study, Jake employed AI voice cloning technology to simulate the voice of a CEO. With the CEO's consent, he sent a voice note to the company's Finance Director, requesting funds transfer to a specified bank account. The request was approved without further verification due to several factors:

- Jake had successfully spoofed the CEO's phone number, leading the Finance Director to believe in the authenticity of the request.
- Meticulous research into the CEO's daily activities through social media allowed Jake to craft a convincing narrative, aligning with the day's events.
- The voice note produced with AI voice cloning technology was so convincing that it was indistinguishable from the CEO's voice.

This case underscores the growing threat of AI-driven fraud and the critical need for organisations to bolster their cybersecurity measures to combat such sophisticated attacks.

2pm **End of meeting and networking lunch**

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 9,000+ 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 and this event.

With thanks to our Supporters…

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