THOUGHT LEADERSHIP

News and critique for security and risk professionals

In association with: Perpetuity Research and World Excellence Awards

[Global OSPAs](#) | [Country OSPAs](#) | [Cyber OSPAs](#) | [TECAs](#) | [SSEAs](#) | [Webinars](#) | [Research](#)

Thought Leadership - October 2023

Welcome to your new-look Thought Leadership newsletter!

You may have noticed that we have updated the look and feel of your newsletter. Our aim is to make it more useful and ensure it is packed full of thought-provoking content for you. We have put a lot of thought into it, but of course, we are bound to have missed something, so we would appreciate your feedback. If you have any questions or a suggestion for something we should cover, drop me an email and let me know!

– **Tom Reeve**, Thought Leadership editor – t.reeve@perpetuityresearch.com

Thinking about AI in security and risk management

Although AI has been around for decades in various forms, *generative AI* is taking the world by storm with ChatGPT, Google Bard, Microsoft Bing and other tools. Millions of people, who are by no means techy, are finding applications for it. These range from research and writing to editing video and generating images, and it has re-ignited interest in the use of AI to assist organisations with more complex activities.

What's changed is the development of large-language models (LLMs), sometimes described as predictive text on steroids, which use mathematical models to statistically generate text in response to user input.

Despite using statistics to basically guess the answer to questions, they are surprisingly right and are only getting better. They are variously described as your personal assistant and the most accessible, and therefore revolutionary, computer technology since the word processor and the spreadsheet.

AI – not necessarily generative AI – permeates security and risk management, finding applications in facial recognition and other forms of 'smart' CCTV, computer virus testing, network intrusion detection, fraud analysis, crime pattern analysis, and more. No doubt, generative AI is finding its way into reports, sales documents and tenders (but not this newsletter!).

While AI is obviously a tool for the good guys, the same applies to the bad actors who, the evidence shows, are already using the technology to automate existing avenues of attack and open up new fronts in their war against us.

Like any fast-moving technology, many organisations will suffer in the longer term because they fail to keep up with AI. It will also change the nature of work, simultaneously creating and destroying jobs and even entire industries.

At a corporate strategic level, there are many risks associated with managing the transition to AI, not least competitive analysis but also strategic and operational decisions around data infrastructure, model ownership, workforce structure and AI governance.

What do you think? What impact is AI having on your organisation, for good and bad? Do you know your organisation's medium and long-term strategy for AI? How will AI continue to shape security and risk management? Do you know who within your organisation is responsible for developing AI tools and for protecting against the associated risks – and are they the same people?

Read: The great acceleration: CIO perspectives on generative AI | MIT Technology Review
Read: The economic potential of generative AI: The next productivity frontier | McKinsey
Read: The Use of AI in Physical Security - Perpetuity Research

Event: The **Thought Leadership Summit**, co-located with the **Tackling Economic Crime Awards** (TECAs) on 1 November 2023 in London. The programme includes a presentation, **"The Art of War: When fraud met AI"** presented by Nicolai Thomson, CEO of Jenesys
Thought Leadership Summit | Tackling Economic Crime Awards (TECAs)

Stand by for radical changes to corporate criminal law

According to Barry Vitou, writing in City AM news, the Economic Crime and Corporate Transparency Bill, currently making its way through Parliament and expected to receive full Royal Assent during Autumn/Winter 2023, could be the biggest shakeup in corporate criminal law in a century.

Part of this Bill creates a new offence of 'failure to prevent fraud' by an employee or agent for an organisation's benefit, where that organisation did not have reasonable fraud prevention procedures in place.

At present, it is drafted to apply only to 'large' organisations, defined by specific level of turnover, the number of employees, or the value of their assets. If convicted, an organisation can receive an unlimited fine.

What do you think? Do you understand how the legislation will impact your organisation? Have you assessed the threats and opportunities it may open up?

Read: We're in for the biggest shake up in corporate criminal law this century – CityAM
Read: Economic Crime and Corporate Transparency Bill – Parliamentary Bills

Help us investigate how industry can help police tackle fraud

Perpetuity Research is undertaking research looking at counter-fraud activities in the private and not-for-profit sectors that the police might be able to use to tackle economic crime more cost effectively.

Economic crime costs society billions of pounds every year, but it is difficult to investigate and remains a low police priority.

With financial support from the Dawes Trust, Perpetuity, along with the Centre for Cybercrime and Economic Crime at Portsmouth University, will identify and map the types of activities and expertise that exist within the private and not-for-profit sectors for tackling the fraud problem that may benefit the police, identify any obstacles for working in partnership and highlight areas of best practice.

Please visit the Perpetuity Research website to learn more and find out how you could help us with this important research.

Read: New Research Launched – Enhancing Police Resources in the Fight Against Economic Crime Cost Effectively
Contact: Dr Janice Goldstraw-White at Perpetuity Research if you think you could be of assistance with this research.
j.goldstraw-white@perpetuityresearch.com

Latest UK government risk register is 'most transparent' yet

The UK government says the latest edition of the National Risk Register is the most transparent yet, sharing more previously classified assessments than ever before.
The risks with the greatest predicted consequences include another pandemic, a large-scale chemical-biological-radiological-nuclear (CBRN) attack, failure of the national grid, civil nuclear accident and radiation release from overseas nuclear accident. None of these risks are judged to be more than 5% likely to happen apart from another pandemic.

Looking at the most likely assessed risks, these include an international terrorist attack, major outbreak of plant pest Xylella fastidiosa, Northern Ireland related terrorism, assassination of a high-profile public figure, terrorist attacks in public venues, technological failure of UK financial infrastructure, disaster response in the Overseas Territories or an attack on a UK ally outside of NATO. However, the impact of these risks is rated as 'moderate' or less severe.

What do you think? Do you understand the benefits to your organisation of the government publishing these sensitive risk assessments? Has your board assessed how it can use this information in a meaningful way?

**Read:** National Risk Register 2023 – GOV.UK

Free template for project scope and requirements available from SRMBOK

Whether you're engaging an external consultant or managing an in-house evaluation, SRMBOK says its Security Risk Assessment Scoping Statement Template will help you develop a comprehensive assessment plan.

SRMBOK – the Security Risk Management Body of Knowledge based in Australia – offers a range of documents for security and risk management professionals, some free and some for a modest fee. This one is free, so definitely worth a look.

Read: Security Risk Assessment Scoping Statement Template | Srmbok
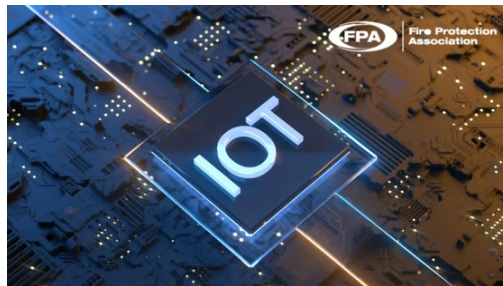
Guide to IoT risk management

IoT (internet of things) devices are widely used in security and fire protection, but the risks associated with them are not widely understood.

The Fire Protection Association (FPA) has published a free guide which, it says, highlights the main hazards, controls, guidelines and accreditations that make up the landscape for IoT devices.

Read: S35 Internet of Things – Connected Security Devices and Systems | Fire Protection Association

News from Perpetuity Research & World Excellence Awards

Recent Webinars

- Taking sustainability seriously: how common is 'greenwashing' and what can we do?
- Tackling healthcare fraud: the uncontrollable beast or the example of good practice?
- Robots: a security opportunity or a security threat?

Come Meet Us!

- **The Security Event – Birmingham NEC – 30 April to 2 May – Stand 5/Q70**
  The SSEAs take place at The Security Event on 30th April 2024!

World Excellence Awards Calendar

Event	Entries Open	Entries Close	Finalists Announced	Awards Presentation
Benelux OSPAs	Entries are closed.	Entries are closed.	Finalists Announced	4th October 2023
UK OSPAs	Entries are Open!	3rd October 2023	21st November 2023	22nd February 2024
Australia OSPAs	Entries are closed.	Entries are closed.	Finalists Announced	19th October 2023
Germany OSPAs	Entries are closed.	Entries are closed.	2nd October 2023	26th October 2023
Southeast Asia OSPAs	Entries are closed.	Entries are closed.	2nd October 2023	10th November 2023
Canada OSPAs	Entries are closed.	Entries are closed.	24th October 2023	30th November 2023
New Zealand OSPAs	22nd October 2023	30th January 2024	3rd March 2024	14th April 2024
Ireland OSPAs	27th November 2023	20th February 2024	26th March 2024	17 May 2023
TECAs	Entries are closed.	Entries are closed.	Finalists Announced	1st November 2023
Cyber OSPAs	Entries are Open!	6th February 2024	12th March 2024	23rd April 2024
SSEAs	Entries are Open!	1st February 2024	11th March 2024	30th April 2024