In association with: Perpetuity Research and World Excellence Awards

Global OSPAs | Country OSPAs | Cyber OSPAs | TECAs | SSEAs | Webinars | Research

Thought Leadership - December 2023

Welcome to the latest edition of Thought Leadership in which we highlight security and risk management research reports that might just provide a little food for thought for you in your job. In this edition:

- Identifying the drivers and barriers to achieving security convergence in large organisations
- How do you design a security system when you don't fully understand the threat or system performance?
- Parliament strengthens economic crime measures
- Altia joins with the TECAs to celebrate the fight against economic crime
- NatWest fraud survey warns against 'mod cons'
- Australian government releases action plan to become world's most cyber secure country
- When the experts don't agree on how to define risk and security terminology and practices

We're always on the lookout for new research reports, so if you see something good, please drop me a line and let me know.

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

Parliament strengthens economic crime measures

26 October 2023, the Economic Crime and Corporate Transparency Act (ECCTA) officially obtained Royal Assent after more than a year of extensive parliamentary deliberation and modifications. This substantial legislation contains a range of measures to tackle economic crime and improve corporate transparency. The majority of the measures outlined in the ECCTA will be implemented through secondary legislation, the specifics of which remain uncertain at present.
Measures in the new law include:

- **Reform of Companies House** – the Government will change its statutory role from being a largely passive recipient of information to a much more active gatekeeper over company creation

and custodian of more reliable data.
- **Reform of Limited Partnerships**
- **Creation of the Register of Overseas Entities** – aims to increase transparency in land ownership and reduce the risk of money laundering via UK property.
- **Improvements to criminal confiscation powers in relation to crypto assets**
- **Loosening information sharing regulations** – to allow businesses to take a more proactive approach to preventing, investigating, and detecting economic crime
- **New sanctions for legal professionals who facilitate economic crime**
- **A new failure to prevent fraud offence** – to hold organisations to account if they profit from fraud committed by employees.
- **New protections against Strategic Lawsuits Against Public Participation (SLAPPs)** – aims to provide defendants with greater protection when faced with SLAPPs.

What do you think? Is your organisation prepared for the ECCTA reforms? How will your organisation manage any enhanced compliance and monitoring requirements that might apply to your business sector? What burdens and opportunities do you foresee in the new legislation?

Read:

- The Act: Economic Crime and Corporate Transparency Act 2023 - Parliamentary Bills
- Explanatory notes of the Act (well worth reading the page headed 'Policy background'): https://publications.parliament.uk/pa/bills/lbill/58-03/096/en/5803096en01.htm
- Factsheet: Economic Crime and Corporate Transparency Bill overarching - GOV.UK

Altia joins with the TECAs to celebrate the fight against economic crime

Fraud is thought to be the most common type of crime, and it is continuously evolving with technology, making it increasingly complex to investigate and prevent. Much of it is classified as serious and organised and may cost companies, government and individuals in the UK collectively up to £219 billion a year, according to the Annual Fraud Indicator.

Recognising efforts to reverse this damage, the Tackling Economic Crime Awards (TECAs) set out to spotlight the counter-fraud professionals who are making a difference in the fight against this pernicious crime. With 13 award categories, we celebrate the achievements of individuals and teams operating in the public, private and third sector with an annual awards ceremony and networking reception.

We are proud to have Altia as our headline sponsor for the awards.

Altia is a leading global provider of investigation and intelligence software. Its software solutions make the world a safer place by making investigations of any kind more efficient and effective.
From managing risk, right through to solving and prosecuting crimes, its Intelligence and investigation tools help teams work together to improve their processes and get the most out of data and insight to get results.

Altia's Solutions
Altia's solutions help solve challenges across the full lifecycle of an investigation:

- Information management – tools to manage intelligence and information
- Covert operation management – high risk, sensitive and confidential operation management
- Investigation solutions – tools to find trends and patterns in data

Most recently, it has added critical incident management and digital intelligence tools to its suite of solutions.
Based on this wide spectrum of solutions which have been developed and tried and tested over many years, it reliably provides industry-specific, legislatively, and evidentially compliant user-friendly products.

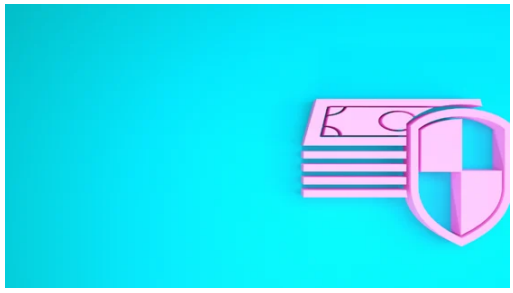
Financial investigations

Technology can help investigation teams manage the growing volume and complexity of economic crime.

Altia's Financial Investigator tools fully automate the process of converting paper-based information and its analysis to identify entities, trends, relationships, and investigative avenues. It helps teams perform work in hours which would otherwise take weeks or even months.

The latest web accessible investigation toolkit has interactive dashboards which, using machine learning, can highlight patterns and trends which may have been overlooked.

To get a free copy of Altia's guide to case management software, visit their website at www.altiaintel.com or email info@altiaintel.com.



NatWest fraud survey warns against 'mod cons'

The new study, conducted by OnePoll for NatWest, revealed that 13% of Brits have lost money to con artists, with 7% having lost as much as £5,000. A previous NatWest study revealed average losses are around £350 per person.

The survey found the top cons on the rise this year include purchase scams where criminals place false adverts for products and services that don't exist, with 24% of Brits seeing an increase in the number of these this year – and four in five of these have seen an increase in phishing scams, where false emails and calls are made from what seems to be from a legitimate company.

Eight in 10 of those polled are also concerned impersonation fraud may become harder to detect in the next five years because of the rise in AI - with 18% saying they have replied to a message from impersonator in the past, initially believing it to be a friend or family member.

According to 81% of adults, more should be done to stop scams at their source – though 83% of Brits also want to become more vigilant at recognising impersonator fraud themselves.

Questions: Where should responsibility for fighting economic crime lie, with customers, banks or the government/police?

What do you think? Are your staff aware of the changing tactics of financial fraudsters? Do you provide training for them on protecting their personal accounts as well as protecting the business? What steps are you taking to protect your organisation from impersonation fraud in the age of AI?

Read: https://www.natwestgroup.com/news-and-insights/news-room/press-releases/financial-capability-and-learning/2023/oct/most-common-financial-scams-of-2023-revealed.html

Australian government releases action plan to become world's most cyber secure country

The Australian government has released its 2023–2030 Cyber Security Strategy action plan, detailing how Australia will achieve the ambitious target of becoming the world's most cyber secure country by 2030.

To achieve this, it will implement six 'cyber shields' to protect citizens and businesses:

1. Strong businesses and citizens
2. Safe technology
3. World-class threat sharing and blocking
4. Protected critical infrastructure

5. Sovereign capabilities
6. Resilient region and global leadership

It says the strategy is ‘game-changing’ for Australia’s cyber security because:

- It is shifting cyber from a technical topic to a whole-of-nation endeavour
- It is delivering tangible action on the cyber security issues
- It is harnessing the whole country to tackle cyber problems, enabled by stronger public private partnerships

What do you think? Is your organisation taking advantage of government schemes to mitigate the risks from cybercriminals? Is your organisation’s cybersecurity strategy in sync with your government’s strategy?

Read: 2023-2030 Australian Cyber Security Strategy | Australian Government

Identifying the drivers and barriers to achieving security convergence in large organisations

Converged security risk management is an approach that addresses interdependencies between security-related business functions that have traditionally been managed by separate departments within organisations.

In this research report, the authors argue that it is a more effective means of addressing organisational security risks and threats than tackling physical and information security challenges separately, given that the boundaries between the two are frequently blurred.

However, fully converged security remains the exception rather than the rule, leaving organisations increasingly vulnerable as their adoption and reliance on digital technologies accelerates.
Through interviews with eight senior security professionals, this research identified key factors critical to effective converged security risk management, expressed as ‘drivers,’ ‘barriers,’ and ‘facilitators.’ The practitioners’ accounts illuminated how the modern threat landscape continues to drive further the need for such an approach, while the traditional separation of corporate security departments from the information security function in organisations remains a barrier.

A greater focus on training and education, as well as soft skills, were identified as key priorities in the drive for an effective converged approach.

What do you think? Do you understand the key factors for achieving converged security risk management within your organisation? Does your board understand the need for security convergence? What soft skills would you identify as key to driving more effective converged security?

Read: Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators - PMC

How do you design a security system when you don't fully understand the threat or system performance?

In their paper, entitled "Representing Uncertainty in Physical Security Risk Assessment", the authors observe that many security systems are designed without a quantitative analysis of the threats that the system will encounter in its lifetime. Security systems are often designed based only on vague data or expert knowledge, the authors say, leading to inherent uncertainties regarding threats and system capabilities.
Their research paper focuses on the impact of these uncertainties in security assessment and their consideration in system design. They compare the results of an evaluation that does not take into account uncertainties and another evaluation based on distributed input values.
Based on the example of a security risk assessment of an airport structure, they propose the concept of a security margin which accounts for uncertainty in threat analysis and actual system performance.
They say they have shown how this approach can be used for vulnerability assessment by applying it to the initially assessed configuration of the airport structure, demonstrating that the concept of the security margin can help reduce system vulnerability.

What do you think? How do you manage uncertainty in security system specification and design? What steps do you take to validate threat assessments and system capabilities?

Read: Representing Uncertainty in Physical Security Risk Assessment: Considering Uncertainty in Security System Design by Quantitative Analysis and the Security Margin Concept

When the experts don't agree on how to define risk and security terminology and practices

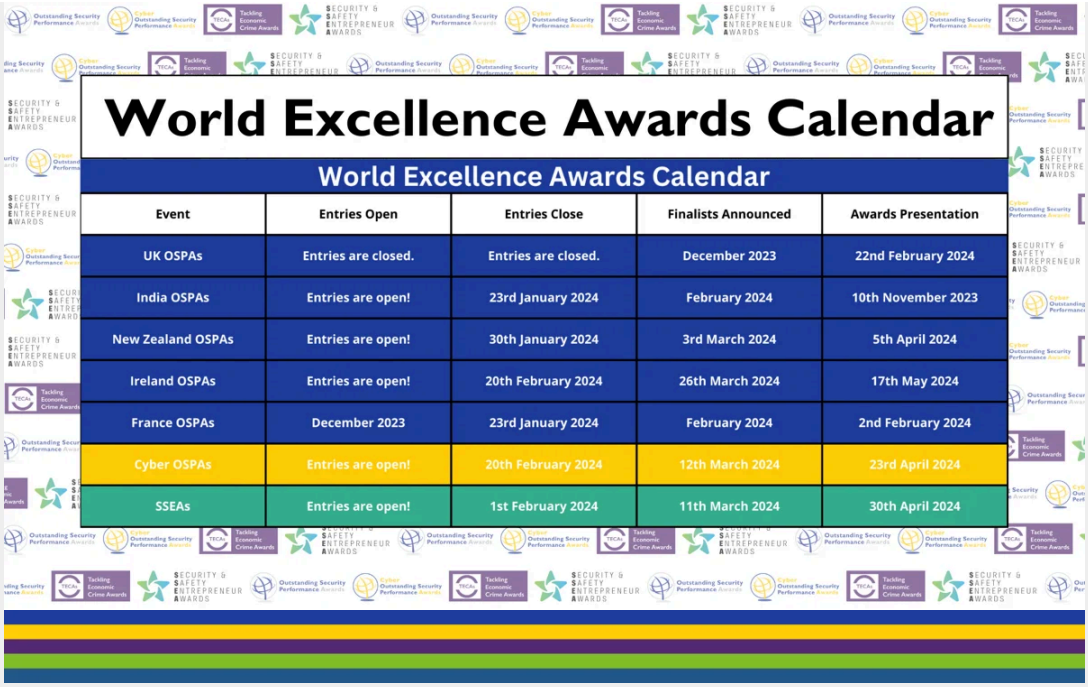
There are a number of standards and frameworks for security risk assessment, but it appears that their application and adaptation to real organisational practices are rather limited.
In this paper, the authors report results from inquiries into risk assessment practices of security professionals in Ireland.

The key findings show a lack of consensus on basic terminology when it comes to defining risk and risk assessment. The interviewed security professionals have developed varied approaches in practice and rather refer to their intuition and previous experiences.

While the paper focuses on Ireland, the lack of consensus regarding the definition, and use of security terminology and practices, especially in the area of security risk management, is not necessarily limited to Ireland.

What do you think? What is your approach to modelling security risk? What are the benefits and challenges of applying standards and frameworks to specific cases within your organisation?

Read: How do professionals assess security risks in practice? An exploratory study



Perpetuity Research and World Excellence Awards, 11a High Street, Tunbridge Wells, Kent TN1 1UL, United Kingdom, +44 (0)7739 179 161