Post event report

Strategic Sponsors

censys

KnowBe4

Red Helix

RISK LEDGER

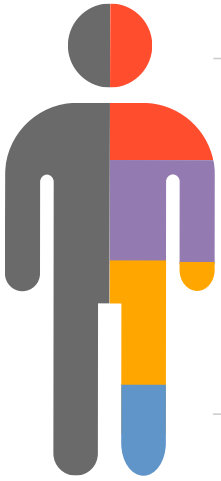
> "A very informative session."
> **OT/ICS Cyber Architect, Uisce Éireann Irish Water**

Inside this report:

Key themes

- Defeating ransomware and malicious malware
- From security to resilience
- Maximising the utility of threat intelligence
- The answer really is zero trust, isn't it?
- Evolving incident response: lessons from the past
- Upskilling security teams
- Why regulation will drive CNI security
- Reducing your attack surface
- The dangers of digitalisation – securing IoT and OT ecosystems
- Securing third-party tech
- Developing the next generation of security leaders
- Detect / prevent malicious insiders

Who attended?



Cyber-security
We have a 20-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Luay Baltaji,
Principal Architect
National Gas Transmission

Simon Brady,
Event Chairman
AKJ Associates

Tom Exelby,
Head of Cyber
Red Helix

Emily Hodges,
COO
Risk Ledger

Charlie Kemp,
Cyber Security Risk and Compliance Analyst
Manchester Airports Group

Javvad Malik,
Lead Security Awareness Advocate
KnowBe4

Bec McKeown,
CPsychol
Mind Science

James Mockford,
Cyber Security Operations Lead
Wessex Water

Nitin Natarajan,
Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA)
Department of Homeland Security, USA

Nick Palmer,
Senior Solutions Engineer
Censys

Ian Thompson,
Head of Cyber Threat Intelligence
BP

Agenda

09:00	Chairman's welcome
09:10	**Bridging digital divides – Navigating IT-OT convergence in critical infrastructure** **James Mockford,** Cyber Security Operations Lead, Wessex Water • The drive towards interconnectivity and its benefits • Overcoming challenges arising from IT-OT interconnectivity • Specific vulnerabilities in hyper-connected environments • Strategies for secure IT-OT integration • Futureproofing CNI security • Case studies
09:30	**Internet exposed industrial system: Protecting UK critical infrastructure and preventing high-risk cyber-attack** **Nick Palmer,** Senior Solutions Engineer, Censys • As critical infrastructure becomes increasingly connected to the internet, securing Industrial Control Systems (ICS) and Operational Technology (OT) is more vital than ever. In this session, we explore the latest research by Censys, which highlights significant security risks associated with UK critical infrastructure • Censys' recent findings reveal over 1,500 publicly accessible control systems in the UK, spread across sectors like water and wastewater management. Alarmingly, a substantial portion of these systems is exposed to the public internet, with weak or default credentials, making them vulnerable to potential exploitation. The session will focus on: ◦ The state of ICS/OT vulnerabilities in the UK and key industry sectors at risk ◦ How over 80% of exposed administrative interfaces relate to building controls ◦ Key protocols at risk, such as EtherNet/IP and DNP3, and the dangers of unprotected human-machine interfaces (HMIs) ◦ Practical steps organisations can take to safeguard critical infrastructure from emerging threats
09:50	**Best practice in building human resilience in cybersecurity environments** **Bec McKeown,** CPsychol, Mind Science • The psychology behind resilience • The research into 'Best Thinking' • Cross-functional communication • Building high-performing teams
10:10	Comfort break
10:15	**The importance of international cybersecurity co-operation in securing critical national infrastructure** **Nitin Natarajan,** Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security, USA • Defining the scope of critical national infrastructure and the increasing interconnectedness globally • Understanding the worldwide threat landscape: Cybersecurity threat actors and their preferred attack methods • How can professionals in cybersecurity, risk management, and data protection use best practices to work together on a global scale? • The benefits of international cooperation; setting the stage for future collaboration
10:35	**The nuances of protecting critical national infrastructure** **Tom Exelby,** Head of Cyber, Red Helix • Explore the latest security threats and solutions to protect the essential services your organisation delivers • The unique challenges of protecting critical national infrastructure • The emerging reliance on the Internet of Things (IoT) and Operational Technology (OT) • Creating perimeter security around your supply chain to combat third-party vulnerabilities • Addressing the risk of rogue devices on a vast and complex network

Agenda

10:55 **FIRESIDE CHAT: Securing our airports**

Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator);
Charlie Kemp, Cyber Security Risk and Compliance Analyst, Manchester Airports Group

- How do emerging cyber-threats, such as advanced persistent threats (APTs) and ransomware, specifically target critical airport infrastructure, and what strategies can be implemented to detect and mitigate these evolving risks?
- With the convergence of Information Technology (IT) and Operational Technology (OT) in airport systems, what are the key challenges in securing these interconnected environments, and how can airports balance the need for operational efficiency with robust cybersecurity measures?
- Considering the complex ecosystem of vendors, suppliers, and third-party contractors involved in airport operations, what are the best practices for managing supply chain cybersecurity risks, particularly in preventing vulnerabilities that could be exploited by attackers?
- In the event of a cyber-attack on airport systems, what are the critical steps in an incident response plan, and how can airports ensure a swift recovery while maintaining operational continuity and public safety?
- How can airports navigate the regulatory landscape and comply with international cybersecurity standards, such as the International Civil Aviation Organization (ICAO) guidelines, while also addressing local and regional requirements to create a unified and effective cybersecurity framework?

11:15 **The power of collaboration: How the UK water industry worked together to ease the burden of supply chain security**

Emily Hodges, COO, Risk Ledger

- Explore the growing challenges of securing the UK's critical national infrastructure (CNI), especially when it comes to supply chain security
- Using examples from the UK water industry and NHS Test and Trace, we'll show how working together can make all the difference in staying ahead of cyber-threats
- You'll pick up practical tips on improving supply chain visibility, managing third-party risks, and building a stronger, more resilient network by collaborating across industries
- Expect straightforward insights and real-world examples on how you can use collaboration to increase your supply chain security

11:35 Comfort break

11:40 **IAM in OT: A consequence-driven engineered approach**

Luay Baltaji, Principal Architect, National Gas Transmission

- The challenge of identification, authentication and authorisation in OT
- How did this manifest recent threat intelligence?
- Consequence-driven engineered design
- Data and delivery strategy for an efficient and effective implementation

12:00 **The human factor: The importance of cybersecurity and you**

Javvad Malik, Lead Security Awareness Advocate, KnowBe4

- We will explore the current landscape of cyber-threats targeting critical infrastructure. We'll examine how organisations compare to their peers in terms of risk reduction efforts and discuss what constitutes an unacceptable level of risk
- The social engineering threat landscape: Delve into the growing problem of social engineering attacks, with a particular focus on phishing
- Creating a security-aware culture: Learn actionable strategies to reduce cyber-risks by fostering a security-conscious organisational culture. We'll discuss practical tips for employee education, implementing effective security policies, and encouraging proactive security behaviours
- Measuring and improving human-centric security: Explore methods for assessing the effectiveness of human-focused security initiatives. We'll cover key performance indicators, ongoing training techniques, and ways to continuously improve your organisation's human firewall

12:20 **FIRESIDE CHAT: Beyond threat awareness to action – a necessary revolution**

Simon Brady, Event Chairman, AKJ Associates; **Ian Thompson,** Head of Cyber Threat Intelligence, BP

- Why do organisations need to change their approach to threat management?
- How can we evolve our security strategies to incorporate threat intelligence and counter-threat tradecraft as distinct and vital elements of our overall cybersecurity efforts?
- How do we separate threat management from traditional governance and policy frameworks in practice, and why is this essential in the evolution of security strategies?
- As we can't manage threat the same way we manage risk, how do we develop a deeper understanding of how threat actors operate and succeed?
- What specific tailored strategies for threat mitigation and management have you put in place in BP? What in your opinion, has had the biggest impact and how do you measure this?
- What practical advice would you give to those wishing to integrate threat intelligence and counter-threat strategies into their core security mission? Where do they start?

12:55 Chairman's close **13:00** Conference close