Post event report

Strategic Sponsors

Akamai

Bridewell

censys

CLAROTY

> “ Really enjoyed the presentations and sessions that offered a deep dive into emerging threat vectors and strategic imperatives facing CNI operators. The summit not only broadened my understanding of current cybersecurity challenges but also reinforced the importance of embedding security and operational responsibility across all layers of infrastructure. ”
>
> **Senior Operations Engineer, Scottish Power**

> “ The summit was very insightful. The sessions were all impactful and have given me new perspectives to apply to my work. My key takeaway was the emphasis on moving beyond vulnerability management to exposure management particularly in the OT landscape. ”
>
> **IT Auditor, Transport for London (TfL)**

Inside this report:

Key themes

- Regulation – changing the game in cybersecurity?
- Securing Arm's Length Bodies – a systemic issue
- A better approach to outsourcing cybersecurity
- Managing insider threats at a time of crisis
- Securing legacy technology
- From cybercrime to cyberwar
- Developing a risk-based approach to the Cloud
- The ultimate third-party problem
- Upskilling security teams
- Ransomware – dealing with the new normal
- Embracing risk management
- Cloud incident response

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

Bec McKeown,
CPsychol
Mind Science

Elliot Gidley,
EMEA Field CTO
Claroty

Emran Ali,
Associate Director – Cyber Security
Bridewell

Manit Sahib,
Ethical Hacker
The Global Fund

Matthew Rogers,
Industrial Control Systems
Cybersecurity Expert
CISA

Nick Palmer,
Technical Lead, EMEA
Censys

Peter Drissell,
Director Aviation Security
UK Civil Aviation Authority

Peter Kaela,
Lead Cybersecurity Architect
Scottish Power Energy Networks

Richard Meeus,
Senior Director Security Technology and Strategy, EMEA
Akamai

Agenda	
09:25	Chair's welcome
09:30	**FIRESIDE CHAT: Making UK aviation cyber-safe – a regulator's perspective** **Peter Drissell,** Director Aviation Security, UK Civil Aviation Authority • How the CAA has developed cybersecurity oversight of UK aviation • Achieving effective cybersecurity for UK civil aviation • How the regulator can become more oil than glue • What's challenges lie ahead?
10:00	**It's not the breach. It's the spread: Improving cyber-resilience in your organisation** **Richard Meeus,** Senior Director Security Technology and Strategy, EMEA, Akamai • This session will explore the critical role of cyber-resiliency in helping organisations withstand and recover from today's evolving threats • We will dive into strategies for reducing attack surfaces, visualising networks, and securing critical IT assets, while also examining how compliance regulations can enhance security and safeguard sensitive data • Attendees will come away with actionable insights for strengthening their security posture, minimising vulnerabilities, and preparing their organisations to face future challenges in an increasingly complex threat landscape
10:20	**Defending critical infrastructure from rising cyber-threats** **Nick Palmer,** Technical Lead, EMEA, Censys • The digital attack surface is growing at an unprecedented pace – and essential systems are under mounting threat • Censys has examined thousands of real-world cyber-exposures, from vulnerable third-party services and unpatched systems to insecure IoT devices and recurring data breach patterns across the region • The verdict is clear: critical sectors – finance, energy, healthcare, transport, and government – face escalating cyber-risk • In this session, we break down the latest threat landscape, highlight the hidden risks most organisations miss, and share practical approaches for safeguarding both enterprise and national infrastructure
10:40	**Ransomware in healthcare: The growing threat to patient safety** **Manit Sahib,** Ethical Hacker, The Global Fund • Why healthcare is the #1 ransomware target – why attacks are increasing and how ransomware gangs break in more easily than expected • Real-world hacking insights – first-hand stories from ethical hacking operations and the biggest security gaps in healthcare, including legacy tech, access control, and the lack of real-world testing • Why traditional security fails – the limitations of compliance checklists and why conventional security tools don't stop ransomware • Building real ransomware resilience – what healthcare CISOs and IT leaders must do NOW to avoid becoming the next headline
11:05	Comfort break

Agenda

11:10	**Mind the gap: Uncovering decision bias in cybersecurity** **Bec McKeown,** CPsychol, Mind Science • Understanding the role of cognitive biases in security decisions • Identifying key biases impacting security outcomes • Mitigation strategies for reducing bias in security practices • Mitigating concentration risks in an interconnected business
11:25	**Strengthening CNI through future-ready supply-chain security** **Emran Ali,** Associate Director – Cyber Security, Bridewell • Why supply-chain security matters for CNI • Heightened reporting & oversight • Building a holistic supply-chain security programme
11:45	**OT cloud architecture, security and resilience by design** **Peter Kaela,** Lead Cybersecurity Architect, Scottish Power Energy Networks • The journey to cloud native, asset-centric security • Platforms and cloud zoning – a defence in depth approach • Unified security strategy, across cloud, OT and CNI considerations
12:05	**Beyond detection: Prioritising risk in OT for national infrastructure protection** **Elliot Gidley,** EMEA Field CTO, Claroty • Understand why exposure management is essential to safeguard critical OT systems • Learn the core principles that build an effective exposure management programme • Discover proven strategies to prioritise and reduce risk in CNI
12:25	**Prioritising CNI security investments for long-term resilience** **Matthew Rogers,** Industrial Control Systems Cybersecurity Expert, CISA • What long-term security investments to prioritise • Targeted security controls that can improve resilience during the transition • How a CNI entity can take advantage of the increasing number of vendor and supplier regulatory requirements
12:45	Chair's closing remarks