



CYBERISLE 2023

Event Programme

Time Agenda

8:30 **Breakfast**

9:00 **Welcome to CYBERISLE**

Hon. Jane Poole-Wilson MHK, Minister for Justice and Home Affairs
Kurt Schrauwen, Director, Riela Group

9:20 **NCSC Threat Update**

Outlining the latest cyber threats facing the UK and Isle of Man, delivered from the UK's technical authority for cyber threats.

NCSC Representative

9:50 **Apollo 13 and the art of Cybersecurity**

Our secure systems are under massive external attack, the alarms are blaring and we are reeling under the assault, trying desperately to regain control. It is suggested it is time for us to stand back, as mission controller Kranz did, and look at all of this from a position of status if we are not to lose credibility in the eyes of our Boards who foot the enormous bills for our work and yet still see things going wrong. As it stands, poor security could become the greatest disaster the cyber industry has yet faced. But let's get it right, and as Kranz said "I do believe this will prove to be our finest hour"

Martin Smith MBE, Founder and Chairman - Security Awareness Special Interest Group (SASIG)

10:30 **Coffee Break sponsored by Rowany Solutions**

11:00 **Welcome to the Matrix: Red vs Blue Pill Cyber Security**

Welcome to the Matrix, where we will be showcasing the strategies used by both cyber security 'Red' and 'Blue' teams. We will be exploring the Red Team tactics typically used to open up and exploit company networks, alongside the Blue Team techniques to mitigate these attacks across a range of different company sizes. Which pill, or team, will you choose?

Lee Wagenheim & Kurt Schrauwen - Riela Cyber

11:30 **From Blame to Betterment: Punishment as a Last Resort to Improve Workplace Cybersecurity**

Join us as we critically examine the notion of employing punishment as a means to bolster cybersecurity defences. Through an exploration of alternative approaches and their potential to cultivate a more secure digital culture, we will delve into why punishment might not always yield the desired outcomes. Drawing from real-world scenarios, we'll uncover the limitations of punitive measures and shed light on innovative strategies that prioritise education, proactive prevention, and collaboration among employees.

Dave Cartwright, CISO and Head of IT Risk and Operations - Santander

12:00 **Minds and Machines: A Debate on Training vs Technology for Staff Security Awareness**

As organisations grapple with the need to secure their digital defences, this discussion will discuss the balance between training and technological solutions in bolstering staff vigilance against cyber threats. Our panel will share their insights on cost efficiency and effectiveness when trying to foster an organisation-wide culture of security consciousness.

Dave Cartwright (Santander), Kurt Schrauwen (Riela Cyber), Stewart Haynes (ICO), Andy Cuff (CND)

Time Agenda

12:30 **The Psychology of Cyber Deception & Frontier Technologies**

Explaining the psychology of deception and how it is applied in the cyber domain. What methods are now employed to counter such deception.

Dr Francis Gaffney, Senior Director of Mimecast Labs and Future Engineering

13:00 **Lunch**

14:00 **Keeping an AI Open for Opportunistic Attacks**

Delve into the world of cybercrime and the role of AI-driven tools in forensic investigations. Explore the motivations behind criminal activities and AI-driven toolsets pivotal role in forensic investigations. Highlighting the key benefits of AI, we proceed with a compelling case study involving an opportunistic attack on a bank, detailing the bank's size and complexity and providing an overview of the incident. We discuss the extortion demands and present our customised methodology, showcasing AI in action. This includes the use of AI to identify suspects, create a web of connections, harness open-source intelligence, harvest data, connect the dots, delve into cryptocurrency forensics, and employ social engineering through sentiment and behavioural analysis.

Peter Allwright, Head of Suntera Forensics

14:35 **Binary Battlefield: Exploring the Threats and Opportunities of AI in Cybersecurity**

In this discussion, we will uncover how AI can be used both by cybercriminals to launch attacks and by defenders to strengthen digital security. Join us to gain insights into the challenges and opportunities that AI presents in the realm of cybersecurity, and learn how this evolving technology is shaping the way we protect our digital landscape.

Kurt Roosen (DfE), Peter Allwright (Suntera Global), Adolf Mugandiwa (PwC Isle of Man) Dr. Joseph Ikhalia (Utmost Group)

15:05 **Guarding the Gates: Cybersecurity Risks in Outsourced Operations'**

In the face of massive attacks through third-party services such as MOVEit, explore the complex landscape of outsourcing and its implications for digital security. In this session, we will delve into the challenges, vulnerabilities, and best practices associated with entrusting third-party operations with sensitive data and critical processes. Gain valuable insights on mitigating risks, identifying accountability, and safeguarding your organisation's digital assets.

Panellists tbc

15:35 **Island Shield: Delivering the National Cybersecurity Strategy**

What is the Cyber Security Centre for the Isle of Man (CSC) doing to help individuals, business and community groups 'shield' themselves from cyber-attack and build resilience. How does this support the delivery of the National Cyber Security Strategy and how does partnership working help the CSC in helping us to develop and improve our activities.

Mike Haywood, Interim Director - OCSIA/CSC

Time Agenda

10:30 **Coffee Break sponsored by Rowany Solutions**

11:00 **Cyber: Detect & Investigate**

In this discussion, we explore some of the methods and tools cyber professionals use to detect and investigate cyber fraud.

Jae Ho Shin & Neil Hathi (Deloitte)

11:30 **Incident Response**

Join us as we take a look at incident response. Discussing case studies, we discover the most effective ways to organise a response to an incident and how to recover.

Jeff Ames, Chief Technology Officer - Computer Network Defence (CND)

12:00 **A Plan of Attack: Data Breach**

When a data breach happens, what's the best response? This session will explore the logistical and technical challenges of responding to, and recovering from, a data breach.

Sarah Simon & Felix Newman (Deloitte)

12:30 **Change of Duty: Public Service to Private Sector**

Join Nick Downing as he discusses his cybersecurity journey, from working as one of the UK's most senior detectives to Director at Deloitte. Listen to Nick's insights into the approaches of the public and private sector towards cybersecurity, and what lessons can be learned.

Nick Downing, Director - Deloitte

13:00 **Lunch**

14:00 **5 Things Your Small Business can do to Stay Secure**

Fed up of hearing horror stories, people trying to sell you "silver bullets" and presentations that tell you all the problems with none of the solutions? Then this session is for you. We will look at 5 things your business can do to improve its security. Simple explanations of how each reduce risks and how some can even be free.

Lee Williamson, Chief Information Security Officer (CISO) - EIP

14:30 **Cybercrime: Who Carries the Responsibility?**

What role does the Government, business and individuals have in combatting Cyber-crime? How does the public and private sector work together to tackle cyber-crime? This session will explore where there are more opportunities to work together and the role we all play in combatting cybercrime.

Phil Hunkin (FIU), Steve Maddocks (IOM Constabulary), Alan Chambers (OCSIA), Richard Williams (Deloitte)

THANK YOU TO OUR SPONSORS



Deloitte.



manx telecom

