Oscar Krane

WE ARE ENGAGEMENT

EVENT PROGRAMME

Wednesday 7th & Thursday 8th October

EXCELLENCE IN SECURITY AND RISK MANAGEMENT

British Business Bank · University of East London · AVENTUM · Cabinet Office Digital · dnata · S&W · ARCUS FACILITIES MANAGEMENT · Two Rivers Housing · Chelmsford City Council · MoneyGram HAAS F1 TEAM

Technology has enabled us to do many things which were once thought impossible and there is not a single aspect of our lives which hasn't been touched by it. Just when we think it can't do anymore it proves us wrong and takes another leap.

Remote working for entire companies was merely a pipe dream 2–3 years ago but is now a reality, being able to access information on the move whilst away from home or office seemed a mere theory a decade ago is now a given, but with these incredible advances in how we communicate and work has come even greater risks. Data and information, often seen as more valuable than currency, is exchanged and available in seconds rather than hours and can be accessed anywhere in the world, but has the means to keep these highly valuable assets safe kept pace?

With the constantly changing landscape it is hard to adapt, it feels that just as organisations think they've got their security and risk management plans in place they must start all over again. So how do you solve a Rubik's cube which unsolves itself whilst you are trying to solve it? What do organisations and individuals need to do to stay ahead of threats?

Join us at the Excellence In Security and Risk Management event to hear from senior industry leaders from the public and private sectors about how they and their organisations have overcome challenges in this arena and what they feel others should be on the lookout for.

Topics to be discussed include:
• Cloud Security and Tool Consolidation • Evolving Risk Management Frameworks • AI-Driven Threats and Governance Gaps • Geopolitical Instability and Cyberwarfare • Escalating Cyberattacks and Ransomware • Funding Instability for Cybersecurity Programs • Cybersecurity Talent Shortage and Workforce Stress • Regulatory Fragmentation and Compliance Complexity

Oatlands Park Hotel
146 Oatlands Dr,
Weybridge KT13 9HB

WEDNESDAY 7TH OCTOBER

15:00 – 18:00 HOTEL CHECK-IN AND FREE TIME

18:45 – 19:30 REGISTRATION AND DRINKS RECEPTION

19:30 – 22:00 NETWORKING DINNER

THURSDAY 8TH OCTOBER

07:45 – 08:20 REGISTRATION, TEA, COFFEE & PASTRIES

08:20 – 08:30 CHAIR'S WELCOME AND OPENING REMARKS

Phillipa Nazari, *Director Data and Information Governance*

British Business Bank

08:30 – 09:00 CYBER RESILIENCE, AI GOVERNANCE, AND THE ACCOUNTABILITY GAP

Most boards still talk about AI as something they're about to adopt. They're not. It's already embedded in the tools their staff use every day, in the SaaS contracts they've already signed, in the copilots quietly summarising confidential documents, in the vendor platforms they've outsourced risk to without realising.

The new Cyber Security & Resilience Bill could make this issue a significant regulatory risk. If the board is formally accountable for cyber resilience, the AI systems already running through the organisation stop being an IT problem and become a governance failure waiting to be named.

This session is a practical, unexcited read on what the legislation actually changes, what boards are already carrying that they don't yet recognise, and what to do about it in the next twelve months. No vendor pitch, no alarmism, no future-gazing just a practical, pragmatic approach to address the problems in the present.

Craig Clark, *Chief Information Security Officer*

University of East London

09:00 – 09:30

FROM TOOLS TO TRUST: USING RISK MANAGEMENT AND ASSURANCE TO BUILD CONFIDENCE IN CYBERSECURITY

Many organisations invest heavily in security tooling yet continue to struggle with confidence in their cyber risk position. This session explores how strengthening risk management and assurance can bridge the gap between security controls and executive trust.

We will examine how clear risk articulation, outcome-focused metrics, and effective assurance mechanisms enable better oversight and decision-making. Drawing on practical experience, the session will show how aligning security tooling to business risk and assurance outcomes helps boards move from tool reliance to trusted, defensible cybersecurity decisions.

Temi Onanuga, *Group Head of IT*

AVENTUM

09:30 – 10:00

MAKING RISK VISIBLE: HOW THE CABINET OFFICE BUILT A DATA-DRIVEN VIEW OF CYBER EXPOSURE

When organisations lack a clear consolidated picture of their cyber risk exposure, even well-intentioned investment decisions can miss the mark. This talk charts our journey at the Cabinet Office from disparate data and limited visibility to a structured, evidence-based view of risk that now drives meaningful conversations at the most senior levels of the Department.

Christopher Whitehead, *Head of Information Security*
Sharon Watts-Tucker, *Head of Information Security*

Cabinet Office Digital

10:00 – 10:30

CASE STUDY PRESENTATION

10:30 – 11:30

TEA, COFFEE & NETWORKING BREAK

11:30 – 12:00

THE BLUEPRINTS OF TRUST: REIMAGINING CYBER RESILIENCE IN THE AGE OF AI

To achieve Excellence in Security, organisations must focus on transition from reactive defence to "Architected Trust." As AI-driven threats accelerate at machine speed, risk management shifts from simple prevention to building systems that absorb shocks and maintain integrity. This session provides a strategic blueprint for navigating the AI frontier, focusing on the convergence of automated defence and human-centric trust.

We will explore the erosion of traditional perimeters and the rise of the "AI vs. AI" conflict. Attendees will gain actionable insights into strategic governance for managing the AI attack surface and move from traditional silos to a resilience roadmap, transforming AI from a risk into a primary tool for operational excellence.

Noman Qureshi, *Cyber Security Manager*

dnata

12:00 – 12:30

THE IMPORTANCE OF LEADERSHIP AND ITS IMPACT ON SECURITY

I will talk about the importance of leadership, how good and bad leadership impacts security and what the consequences can be. I will also talk about the traits of good leaders and how they impact team and delivery. I will also talk about why strategy and alignment matter in security, how leadership behaviours (especially communication and psychological safety) shape outcomes, and what you can do to build a security culture that actually works day-to-day.

You can expect a few real examples (including where things went wrong), plus practical takeaways you can use whether you're leading a team or influencing without the title. Because in cyber, lack of clarity and lack of speak-up culture don't just hurt morale—they create blind spots, wasted effort, and sometimes incidents. If we can align security to what the business is trying to achieve, and create teams that communicate early and challenge safely, we reduce risk and deliver faster, with less friction.

Daniela Waugh, *Head of Information Security (CISO)*

S&W

12:30 – 13:00

CASE STUDY PRESENTATION

13:00 – 13:45

LUNCH

13:45 – 14:15 TEA, COFFEE & NETWORKING BREAK

14:15 – 14:45 CYBER SECURITY ROI – ALIGNING BUSINESS SECURITY INVESTMENT WITH BUSINESS OUTCOMES

Sajid Iqbal, *Information Security Manager*

ARCUS FACILITIES MANAGEMENT

14:45 – 15:15 AS INDUSTRY TALKS ABOUT THE USE OF AI AND WE GET ON THE BAND WAGON THAT AI WILL DO EVERYTHING

- What should the different types of AI be used for
- Use of AI by hackers
- Are humans becoming obsolete?

Adam Huselbee, *Assistant Director Data & Technology*

Two Rivers Housing

15:15 – 15:45 CASE STUDY PRESENTATION

15:45 – 16:30 TEA, COFFEE & NETWORKING BREAK

16:30 – 17:00 ESCAPE THE DRUDGERY – INFOSEC TRAINING

This presentation addresses the current shortcomings of information security training, critically examining why organisations "train people so badly". Using humor and memes, it challenges standard compliance metrics ("KPwhy?") and argues that employees are not inherently the problem. Instead, the presentation leverages scientific principles to rethink cybersecurity awareness and training methods.

Finally, it outlines the practical strategy implemented by Chelmsford City Council—detailing what actions they took and the rationale behind them—to move away from traditional corporate drudgery toward an evidence-based, effective security culture.

Michael Sage, *Head of DDaT and Transformation*

Chelmsford City Council

17:00 – 17:30 THE GOVERNANCE IMPLICATIONS OF INTEGRATING AI ACROSS OUR SYSTEMS

AI is evolving at an extraordinary pace, whereas operational F1 tends to move more deliberately, with resources and investment consistently prioritised towards on-track performance gains.

It's clear that AI is already being explored and applied in a variety of ways, often without fully established controls or governance. This raises important questions: who owns the data when tools like Copilot are embedded into workflows? Where are prompts and queries being stored, and how are they being used or analysed?

This is an exciting and rapidly developing space but operational is Formula 1 looking deeply enough at the governance implications of integrating AI across our systems?

Harry Minns, *Data Governance Engineer*

MoneyGram HAAS F1 TEAM

17:30 – 17:40 CHAIR'S CLOSING REMARKS AND EVENT FINISH