Post event report

Strategic Sponsors

Education Seminar Sponsors

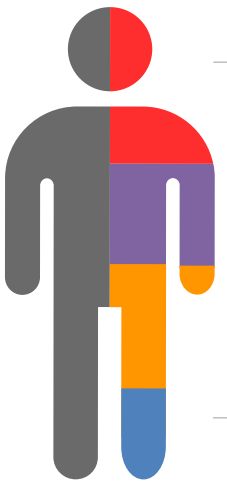
Networking Sponsors

Inside this report:

Key themes

- Cloud incident response
- Solutions for CISO burnout
- Embracing risk management
- Re-thinking email and messaging: is there a better way?
- Fixing Cloud configuration
- Ransomware – dealing with the new normal
- From awareness to behaviour
- Managing insider threats at a time of crisis
- From cybercrime to cyberwar
- Streamlining tools and information: focus on insight
- NIS2 – changing the game in cybersecurity?
- Re-engineering the SOC: the problem of alert overload

Who attended?



Cyber-security
We have a 15-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

Matt Adams, Head of Security Enablement, **Citi**

James Allman-Talbot, Head of Incident Response and Threat Intelligence, **Quorum Cyber**

Jonathan Armstrong, Partner, **Punter Southall Law**

Jas Bassi, Head of Solution Delivery, **Gateley**

Stephen Beckett, Global Security and Business Continuity Director, **Dentons**

Simon Brady, Managing Editor & Event Chairman, **AKJ Associates**

Natalija Buldakova, Solution Architect, **Quest Software**

Phil Cambers, Commercial Director, **Trustack**

Maxime Cartier, Head of Human Risk, **Hoxhunt**

Richard Cassidy, Field CISO, **Rubrik**

Derek Charles, Senior Cloud Consultant, **Exponential-e**

Tim Collinson, Head of Information Security, **Walkers**

Jon Cranton, Legal Sector Lead, **Quorum Cyber**

Jonathan Freedman, Head of Technology & Security, **Howard Kennedy**

Ash Hunt, CISO, **Apex Group**

Valerie Jenkins, Chief Information Security Officer, **Clyde & Co LLP**

James Kwaan, CIO – GS&S, **Lloyds Banking Group**

Jamie Little, Chief Technology Officer, **EveryCloud**

Tom McVey, Sr. Solution Architect, **Menlo Security**

Peter Olivier, Head of Security Delivery, **Admiral Insurance**

Justin Pemberton, Senior Director of Sales

Jonathan Root, Head of Information Security, **Mishcon de Reya**

Francisco Sanches, Director of Cyber Consulting, **Mishcon de Reya**

Sarb Sembhi, Founder and Chair, **Mental Health in Cyber Security Foundation**

Martyn Styles, CISO, **Bird & Bird**

Mike Tewfik, Cyber & Tech Underwriter, **Beazley**

Agenda	
08:00	Breakfast & networking
08:50	Chair's welcome
09:00	**Foundations for security: Crafting a new security strategy and culture** **Tim Collinson,** Head of Information Security, Walkers • From Boardrooms to Bins: Where to find the information to get your strategy started • Department of Yes: Positioning the security team as friendly, approachable and helpful • InfoSec's Got Talent: How and where to get the best people and persuade them to join the team
09:20	**Cyber-insurance: The last line of defence** **Mike Tewfik,** Cyber & Tech Underwriter, Beazley • Key claims data and current insights • How AI is changing the cyber-risk landscape • Shedding light on risks and ways to boost your cyber-insurance protection • Boosting your insurability
09:40	**An overview of cyber-threats facing the legal sector, and using threat intelligence to mitigate risk** **James Allman-Talbot,** Head of Incident Response and Threat Intelligence, Quorum Cyber & **Jon Cranton,** Legal Sector Lead, Quorum Cyber • Protecting sensitive client information and proprietary data against increasingly targeted exploits by cybercriminals • Leveraging threat intelligence to effectively mitigate legal sector specific risks, provide robust protection and ensure the integrity and confidentiality of legal operations • Enhancing cybersecurity strategy and safeguarding your practice against evolving threats
10:00	**Cyber-resilience is not a breach challenge but a human challenge** **Sarb Sembhi,** Founder and Chair, Mental Health in Cyber Security Foundation This session will delve into the challenges faced by cybersecurity professionals and discuss potential strategies to address these issues and enhance cyber-resilience effectively. • Overcoming the limitations of conventional cyber-resilience strategies • Understanding the impact of cybersecurity challenges on professionals and consequently businesses • Exploring solutions and approaches for change
10:20	**Education Seminars | Session 1** **Exponential-e** **Cyber remediation – planning for failure** **Derek Charles,** Senior Cloud Consultant, Exponential-e **Hoxhunt** **How to design for any behaviour in security** **Maxime Cartier,** Head of Human Risk, Hoxhunt
11:00	Networking break
11:30	**EXECUTIVE PANEL DISCUSSION** **Managing supply chain security – Understanding the risks suppliers may pose to you and your wider supply chain and the sensitivity of information your suppliers may hold** **Jas Bassi,** Head of Solution Delivery, Gateley (Moderator); **Jonathan Root,** Head of Information Security, Mishcon de Reya; **Valerie Jenkins,** Chief Information Security Officer, Clyde & Co LLP **James Kwaan,** CIO – GS&S, Lloyds Banking Group • Do you really know the full extent of your supply chain? • How are suppliers managing risks to your contract and data effectively? • What are your rights to audit and what information should suppliers share about their supply chain? • What are your minimum security requirements for suppliers and do you treat all suppliers the same from a risk perspective? • How do you meet your own responsibilities as a supplier?

Agenda

12:00 — EXECUTIVE PANEL DISCUSSION — **Managing the response to a cybersecurity threat in an organised way**

Francisco Sanches, Director of Cyber Consulting, Mishcon de Reya (Moderator);
Tim Collinson, Head of Information Security, Walkers; **Martyn Styles,** CISO, Bird & Bird;
Jonathan Root, Head of Information Security, Mishcon de Reya;
Stephen Beckett, Global Security and Business Continuity Director, Dentons

An effective response requires a well-executed incident response and remediation strategy for before and after an incident to limit major disruption to business operations and financial harm

- Assessing the full impact across the whole organisation
- Implementing your incident response plan
- Managing the legal, technical, and operational considerations: containment eradication and recovery
- Crisis communication – a central part of crisis resolution

12:30 — **Education Seminars | Session 2**

Quest Software	Trustack
Managing security incidents: Prevention strategies and worst-case planning **Natalija Buldakova,** Solution Architect, Quest Software	**The recovery position** **Phil Cambers**, Commercial Director, Trustack

13:10 — Lunch & networking

14:00 — **Who's on your shoulder – our devices and our privacy**

Jonathan Freedman, Head of Technology & Security, Howard Kennedy

- What personal data are our mobile devices revealing?
- Keeping our data private
- Compromising mobile devices
- OSINT – just how much is out there?

14:20 — **Cybersecurity in crisis: Aligning compliance strategies to combat the triple threat of ransomware, data breaches, and extortion attacks in the legal sector**

Richard Cassidy, Field CISO, Rubrik

- Evolution of cyber-threats: Insights into how ransomware, data breaches, and extortion attacks are evolving and the unique risks they pose to the legal sector
- Strategic compliance: How compliance is transforming into a strategic imperative, ensuring your firm not only meets regulatory requirements but also fortifies its defences against cyber-threats
- Proactive cybersecurity planning: Moving beyond reactive measures to proactive strategies that provide your firm with a competitive edge in cyber-defence
- Balancing agility and security: Effective methods to maintain business agility while implementing robust security protocols that align with regulatory standards

14:40 — **Education Seminars | Session 3**

EveryCloud	Menlo Security
Go on the offensive by merging AI and human expertise for email security **Jamie Little,** Chief Technology Officer, EveryCloud & **Justin Pemberton,** Senior Director of Sales	**Browser security – the proven prevention layer for enterprise cybersecurity** **Tom McVey,** Sr. Solution Architect, Menlo Security

15:20 — Networking break

15:40 — **AttackGen: Leveraging AI for dynamic incident response testing**

Matt Adams, Head of Security Enablement, Citi

- AttackGen makes threat-driven incident response testing more accessible and efficient for organisations of all sizes
- It combines data from MITRE ATT&CK with Large Language Models to quickly generate comprehensive incident response scenarios for Red & Blue teams
- This talk will feature live demos that explore AttackGen's features

16:00 — EXECUTIVE PANEL DISCUSSION — **Managing personal legal and emotional challenges for CISOs**

Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator); **Jonathan Armstrong,** Partner, Punter Southall Law; **Peter Olivier,** Head of Security Delivery, Admiral Insurance; **Ash Hunt,** CISO, Apex Group

- With increasing personal liability for CISOs under UK regulations and the emotional toll of being held accountable for cyber-incidents – including potential fines and criminal charges – how do you balance legal accountability and personal responsibility?
- How can CISOs guard against their own liability?
- Are you worried about personal liability? Is insurance a consideration?
- Addressing ethical challenges such as balancing business interests with security needs along with the personal consequences of these decisions
- With the psychological impact on CISOs, does your organisation offer support for stress management and mental health and what's out there for CISOs?

16:30 — Drinks reception & networking — **17:30** — Conference close

Education Seminars	
EveryCloud **Go on the offensive by merging AI and human expertise for email security** **Jamie Little,** Chief Technology Officer, EveryCloud & **Justin Pemberton,** Senior Director of Sales	Attendees will learn: • How email security has evolved in the last decade • How AI is transforming traditional email security approaches • Integrating human insight with AI algorithms • Leveraging AI to create highly accurate and dynamic phishing simulations • The benefits of a holistic approach to secure law firms
Exponential-e **Cyber remediation – planning for failure** **Derek Charles,** Senior Cloud Consultant, Exponential-e	It takes an average of three months for law firms to recover from cyber-attacks, resulting in harm to their established brand reputation, loss of client trust, and a significant financial impact ranging from £10m to £50m. However, by implementing strategies to avoid ransom demands and quickly restoring critical data, law firms can resume operations in a matter of days rather than months. Attendees will learn: • The components of a robust prevention and remediation strategy to ensure minimised downtime and impact whilst restoring data effectively and securely.
Hoxhunt **How to design for any behaviour in security** **Maxime Cartier,** Head of Human Risk, Hoxhunt	Are there any risky behaviours you wish people in your organisation would just stop doing? Or secure actions you hope they would take more often? With the human element accounting for around 75% of breaches in 2023, we must evolve from traditional security awareness to real behaviour change. What attendees will learn: • A new model to design for any behaviour (referenced by 1,000+ academic publications) • How to apply the model to cybersecurity, with walkthrough of real-life examples such as reporting security incidents or using approved cloud platforms • Effective strategies for implementing learned skills into tackling human risk in your law firm, summarised in a physical handout given to participants
Menlo Security **Browser security – the proven prevention layer for enterprise cybersecurity** **Tom McVey,** Sr. Solution Architect, Menlo Security	According to Google, 98% of attacks originate from internet usage and 80% of those target end user browsers – sadly all too successfully. Combine this stark reality, with users' relentless demand for new SaaS and private applications, often collaborating with external stakeholders, and security pros are always running to stand still. Attendees will learn: • *Security* – The proven value of robust browser security across managed and unmanaged devices – automating browser configuration and establishing enhanced browser forensics • *Connectivity* – Your users and third parties need access to SaaS applications, private web apps and data, including the use of GenAI. We share how organisations are enhancing user protection and productivity while reducing the cost and complexity of solutions such as VDI • *Compliance* – How browser security supports organisations striving to comply with key NIS 2 requirements for incident management and prevention • We will provide real-world examples and case studies of how to increase cyber-prevention through improved browser security

Education Seminars	
Quest Software **Managing security incidents: Prevention strategies and worst-case planning** **Natalija Buldakova,** Solution Architect, Quest Software	With 74% of breaches involving the human element and ransomware attacks skyrocketing, safeguarding business identities has never been more crucial. Join us in this session as we explore the pivotal role of protecting your business from these threats. You'll gain actionable insights into potential consequences and effective mitigation strategies, alongside comprehensive worst-case scenario planning. Empower yourself to fortify your organisation's defences against evolving cyber-threats with practical knowledge and proactive measures. Attendees will learn: • Today's cybersecurity challenges • Implementing dynamic preventative measures • Developing robust strategy for worst-case scenarios
Trustack **The recovery position** **Phil Cambers,** Commercial Director, Trustack	The cybersecurity landscape is rapidly changing, driven by advancements in technology that are being exploited by bad actors coupled with evolving work models. As cyber-threats become more sophisticated, it is crucial for organisations to stay ahead by updating their security infrastructures and adopting next-generation technologies. For the legal sector, robust security practices are essential to protect sensitive client data and comply with regulatory requirements. Attendees will learn: Listen to real-world accounts of breaches our customers have encountered and the impact it had on their business. • *Identification:* How the breach occurred and the subsequent impact • *Containment:* How was the threat closed down? • *Recovery:* How long did it take to recover the customer? • *Lessons learned:* What could have been done to prevent the attack?