Post event report

SECURING
THE LAW FIRM

Securing the Law Firm

20th January 2026, London

Strategic Sponsors

Akamai

CROWDSTRIKE

THREATLOCKER®
ZERO TRUST PLATFORM

Education Seminar Sponsors

ankura

harmonic

HOXHUNT

RAPID7

RISK LEDGER

tenable

Networking Sponsors

paloalto® NETWORKS

TENEO OPENING MINDS

Prompt: from SentinelOne

wavenet

Branding Sponsor

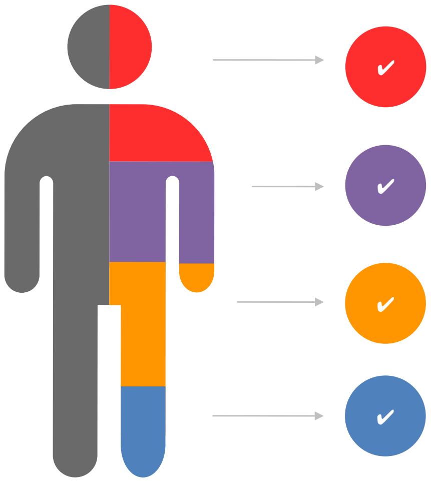
opentext™

Inside this report:

Key themes

- Achieving visibility across ecosystems
- Making the best use of threat intelligence
- Security posture management
- Adversary simulation and behavioural analysis
- Improving continuous attack surface discovery
- The power of automation
- Dealing with regulations
- Defending against the latest ransomware variants
- Transitioning OT to the Cloud?
- Pen testing for OT / SCADA
- OT and the regulations
- Why zero trust, isolation and segmentation are key

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

Joel Barnes, Senior Director, Security Engineering
Tenable

Simon Brady, Event Chairman
AKJ Associates

Steve Davies, Head of Cyber Security
DLA Piper

James Derbyshire, Cybersecurity Entrepreneur
Harmonic Security

Ethan Duffell, Head of Information Security
Clifford Chance LLP

Jonathan Freedman, Director of Technology & Security
Howard Kennedy

Melanie Hart, Partner – Contentious Information Law & Dispute Resolution
Kingsley Napley

Sam Hooke, Sales Director
Hoxhunt

Federico Iaschi, Information Security Director
Starling Bank

Thomas Jenkins, Account Executive
ThreatLocker

Justin Kuruvilla, Chief Cyber Security Strategist
Risk Ledger

Thom Langford, EMEA CTO,
Rapid7

Eleanor Ludlam, Partner – Cyber, Privacy and Technology Litigation,
Pinsent Masons

Ekow Oduro, IT Security Operations Lead
Forsters LLP

Will Packard, Director – Operational Resilience
Ernst & Young LLP

Mark Penlington, Head of Risk, Resilience and Internal Audit
Irwin Mitchell LLP

Ahsan Qureshi, Managing Director
Ankura

Ryan Rubin, Senior Managing Director – Cyber EMEA
Ankura

Adam Speker KC, Barrister
5RB

Anthony Stables, Chief Information Officer
Forsters

Martyn Styles, CISO
Bird & Bird

Jonathan Turner, Head of Cyber Security
Farrer & Co

Mark Ward, Senior Regional Sales Engineer
CrowdStrike

Stuart Winter, Senior Enterprise Security Architect
Akamai

Agenda

08:00	Breakfast networking break
09:00	Chair's welcome
09:10	**From cybersecurity to real, risk-based exposure management: The true power of resilience** **Steve Davies,** Head of Cyber Security, DLA Piper • What is exposure management and how does it differ from vulnerability management? • Managing the real-world risks associated with the modern attack surface • Maximising exposure management to reduce risks enterprise-wide
09:30	**Micro segmentation: Containing the spread of ransomware** **Stuart Winter,** Senior Enterprise Security Architect, Akamai • How ransomware infects your firm and rapidly spreads throughout your network as attackers search for your client's data • Understand what micro segmentation is, and how it helps prevent and contain the spread of it • How Akamai's Guardicore Micro Segmentation helps with auditing, attestation and with compliance and regulations across a hybrid environment
09:50	**Evolving threats to law firms: Adversary tactics, detection, and defence** **Ekow Oduro,** IT Security Operations Lead, Forsters LLP • How emerging threat actors are evolving their methods against the legal sector • How to uncover vulnerabilities across the wider legal supply chain • How to spot and disrupt hidden data exfiltration and C2 activity • How to strengthen resilience through threat-led testing and simulation
10:10	**Education Seminars | Session 1** **Rapid7** **Attacked at machine speed, defended at the speed of Dave in the SOC** **Thom Langford,** EMEA CTO, Rapid7 **Tenable** **Visible and verified: A new approach to AI risk and exposure management** **Joel Barnes,** Senior Director, Security Engineering Tenable
10:50	Networking break
11:20	**Collaborating securely: Addressing cyber-risks in chambers partnerships** **Eleanor Ludlam,** Partner – Cyber, Privacy and Technology Litigation, Pinsent Masons (Moderator); **Adam Speker KC,** Barrister, 5RB; **Melanie Hart,** Partner – Contentious Information Law & Dispute Resolution, Kingsley Napley; **Anthony Stables,** Chief Information Officer, Forsters • Supply chain risks when engaging barristers • Technical challenges of securing chambers • Navigating breach of confidence during a cyber-incident • Injunctive relief as a legal remedy
11:45	**European cyber-threats exposed: CrowdStrike threat briefing** **Mark Ward,** Senior Regional Sales Engineer, CrowdStrike • Exploration of key findings from the 2025 European Threat Landscape, highlighting the tactics and techniques used by leading threat actors • Insight into the strategic objectives of adversaries across e-crime, nation-state and hacktivist groups • Guidance on how understanding their playbook can inform stronger, more effective defensive strategies

Agenda

12:05	**Internal audit – Bridging the gap between aspirations and reality** **Mark Penlington,** Head of Risk, Resilience and Internal Audit, Irwin Mitchell LLP • Why internal audit is important: Learn why internal audit is essential to providing the assurance and confidence senior executives need to understand how teams actually operate in practice • What internal audit is: Understand the role of internal audit as an objective, constructive process that strengthens governance and accountability • How it enhances risk management and governance: Discover how internal audit bridges the gap between stated controls and actual practice by validating control effectiveness, uncovering hidden risks, and driving better decision-making • How to embed internal audit in a practical way: Learn practical approaches to implement and integrate internal audit to deliver meaningful insight, drive activity and provide lasting value
12:25	**Education Seminars | Session 2** **Ankura** **The intricacies of AI breach response** **Ahsan Qureshi,** Managing Director, Ankura & **Ryan Rubin**, Senior Managing Director – Cyber EMEA, Ankura **Hoxhunt** **Turning employees into your first line of defence** **Sam Hooke,** Sales Director, Hoxhunt & **Martyn Styles,** CISO, Bird & Bird
13:05	Lunch networking break
14:00	**Zero Trust controls at the endpoint** **Thomas Jenkins,** Account Executive, ThreatLocker • Discover how ThreatLocker applies Zero Trust at the endpoint, eliminating implicit trust by continuously verifying every application, executable, and action before authorisation • Learn how a deny-by-default, malware-proofing approach reduces ransomware risk, stopping unauthorised software and scripts even when other security layers are bypassed • Understand how least-privilege enforcement limits attacker capability, ensuring applications and users can perform only explicitly approved actions on enterprise devices • Explore how granular, policy-based endpoint control safeguards against modern threats, reducing enterprise exposure to ransomware and other advanced attacks
14:05	**FIRESIDE CHAT: Mitigating concentration risks in an interconnected business landscape** **Simon Brady,** Event Chairman, AKJ Associates (Moderator); **Ethan Duffell,** Head of Information Security, Clifford Chance LLP • Identifying and assessing concentration risk across vendors and technology ecosystems • Balancing operational efficiency with diversification and risk reduction • Communicating the importance of concentration risk to boards and stakeholders • Embedding resilience planning to address concentration risks in today's threat environment • Lessons from recent incidents such as Microsoft 365/Azure outages (2024), the 2024 CrowdStrike disruption, and the June 2025 Google Cloud outage
14:30	**Education Seminars | Session 3** **Harmonic Security** **Safe AI adoption for law firms: Guardrails that protect clients (and your firm)** **James Derbyshire,** Cybersecurity Entrepreneur, Harmonic Security **Risk Ledger** **Beyond questionnaires: Rethinking supply chain security in law firms** **Justin Kuruvilla**, Chief Cyber Security Strategist, Risk Ledger
15:10	Networking break
15:30	**PANEL DISCUSSION** **Beyond compliance — Building cyber-resilience that actually works** **Simon Brady,** Event Chairman, AKJ Associates (Moderator); **Jonathan Freedman,** Director of Technology & Security, Howard Kennedy; **Jonathan Turner,** Head of Cyber Security, Farrer & Co; **Federico Iaschi,** Information Security Director, Starling Bank; **Will Packard,** Director – Operational Resilience, Ernst & Young LLP • How do we turn risk appetite statements into real decision levers instead of paperwork? • With NIS2 and similar rules, what does 'appropriate and proportionate' really mean on the ground – and how can risk management steer the response? • What cyber-metrics really matter – and how do we prove our risk posture to the Board, to clients, and across the entire supply chain, right down to nth-party dependencies? • How does a resilience-first mindset transform culture – moving from blame and unrealistic prevention to readiness, adaptability, and fast recovery?
16:00	Chairman's closing remarks
16:00	Drinks networking reception
17:00	End of conference

Education Seminars

Ankura

The intricacies of AI breach response

Ahsan Qureshi, Managing Director, Ankura &
Ryan Rubin, Senior Managing Director – Cyber EMEA, Ankura

AI technologies are being adopted at a rapid rate within the law firm industry. Whilst many have been ironing out the flaws such as accuracy, IP and hallucinations, not many have come to grips with the security risks around the AI technology itself. It is only a matter of time before the next cyber-incident relates to a breach in the AI technology. Join us for an interactive session running through key areas to consider in responding to an AI technology related breach and some of the challenges this brings to organisations needing to do so. We will cover a combination of Agentic AI, chat-based AI and internal AI platforms that law firms may be using to support their business and share general lessons learned from breaches within the law firm industry as key take aways.

Attendees will learn:

- What happens when an AI agent goes rogue
- How AI breaches differ from standard cyber-breaches
- Lessons learned from supporting breaches within law firms
- Shining a light on Shadow AI
- Regulations and governance

Harmonic

Safe AI adoption for law firms: Guardrails that protect clients (and your firm)

James Derbyshire, Cybersecurity Entrepreneur, Harmonic Security

Legal teams are embracing AI to accelerate research, improve client service, and streamline operations. Yet as firms adopt tools ranging from GenAI assistants to AI-enabled practice software, they face a dilemma: how to encourage innovation while upholding strict client commitments, confidentiality obligations, and regulatory requirements.

This session explores how leading legal firms are moving quickly on AI adoption while implementing the controls needed to avoid data exposure, ethical missteps, and compliance violations. Attendees will learn where the most common governance gaps occur, the types of AI-related risks that frequently go unnoticed, and how to establish practical guardrails that protect sensitive information without slowing lawyers down.

Drawing on real patterns observed across law firms of all sizes, the talk outlines a clear framework for responsible AI enablement. You will leave with a deeper understanding of how to safely operationalise AI in a legal environment and how forward leaning firms are putting structure around experimentation, oversight, and continuous monitoring.

Attendees will learn:

- The most common AI driven exposure patterns in legal workflows and why they occur
- Where governance gaps arise as firms introduce both sanctioned and unsanctioned AI tools
- Practical guardrails that balance innovation with confidentiality, client commitments, and regulatory duties
- How progressive firms are enabling responsible internal AI use while maintaining full compliance

Education Seminars	
Hoxhunt **Turning employees into your first line of defence** **Sam Hook,** Sales Director, Hoxhunt & **Martyn Styles,** CISO, Bird & Bird	Humans remain one of the most targeted – and most exploited – elements of any organisation's security maturity. Despite continued investment in technical controls, phishing and social engineering attacks continue to succeed because they are designed to manipulate human behaviours rather than systems. This session explores how organisations can realistically address this challenge by strengthening the human layer of security without overwhelming already stretched Infosec teams. Co-presented by Bird & Bird and Hoxhunt, this talk combines real-world experience with practical insight into building effective, scalable security awareness programmes. The speakers will discuss why user error is inevitable, and why the goal of security awareness should not be perfection, but resilience – helping employees develop a strong 'suspicious bone' that enables them to recognise and respond appropriately to threats. Attendees will learn how security awareness can be delivered at scale with minimal ongoing effort, using automation and adaptive training to reduce administrative overhead while maintaining high engagement levels across the organisation. A key highlight of the presentation will be a live, practical demonstration of high-quality phishing simulation emails and the ease with which targeted security awareness training packages can be deployed. This hands-on walkthrough will show how realistic simulations, timely feedback, and automated training can work together to drive lasting behavioural change. **Attendees will learn:** • Humans and security – People will always be vulnerable to scams, so Infosec teams must focus on education and building a strong 'suspicious bone' • Low effort for Infosec – Hoxhunt largely runs itself, requiring minimal setup and ongoing management from busy security teams • Practical demo – Live demonstration of realistic phishing simulations and how easy it is to set up effective security awareness training
Rapid7 **Attacked at machine speed, defended at the speed of Dave in the SOC** **Thom Langford,** EMEA CTO, Rapid7	Budgets are tight, your team is stretched thin, and the business is (very) demanding. What CAN you do to get the most out of your people, investments and technology? How can you turn data into action; moving from drowning in alerts to executing precise, high-impact remediations. **Attendees will learn:** • Augmenting your response time with AI and human expertise • Shifting to Managed eXtended Detection and Response to unify visibility across your estate • Proactively staying on the right side of the regulators
Risk Ledger **Beyond questionnaires: Rethinking supply chain security in law firms** **Justin Kuruvilla,** Chief Cyber Security Strategist, Risk Ledger	Organisations across all sectors rely on increasingly complex digital supply chains, from cloud services and software providers to managed services and specialist vendors. Each connection introduces supply chain risk, yet many security and risk teams still depend on point-in-time assessments that struggle to reflect how risk changes over time. In this session, Risk Ledger will explore the fundamentals of supply chain risk and security, focusing on why visibility is often limited, where blind spots typically emerge, and how organisations can start to untangle complex supplier ecosystems. We will examine why questionnaire-led approaches alone are no longer sufficient, how external and continuous signals can complement existing governance processes, and what a more resilient, defensible approach to supply chain security can look like in practice. The session will also cover how organisations can prioritise effort, reduce noise, and focus on the suppliers that matter most. This session is designed for leaders looking to better understand supply chain risk, build stronger foundations for continuous assurance, and make more informed risk decisions regardless of sector. **Attendees will learn:** • A clearer understanding of how supply chain cyber-risk emerges and evolves • Insight into common visibility gaps and why they persist • Practical principles for moving beyond point-in-time assessments • A framework for prioritising suppliers and focusing on what matters most

Education Seminars

Tenable

Visible and verified: A new approach to AI risk and exposure management

Joel Barnes, Senior Director, Security Engineering, Tenable

As legal firms race to harness AI for critical cost savings and competitive advantage, the widening gap between rapid innovation and necessary governance is creating a volatile new landscape of risk. With fee-earners and internal teams deploying ‘shadow’ agents and onboarding unproven vendors to stay ahead of the competition, security teams are often forced to choose between obstructing business growth or accepting unchecked exposure. This session explores how a holistic exposure management strategy bridges this divide, providing the unified visibility needed to control AI-driven data risks, output accuracy, and vendor vulnerabilities.

Attendees will learn:

- Extending visibility to AI: How to incorporate AI applications and data flows into your existing Exposure Management view to ensure a complete picture of your attack surface
- Contextualising and prioritising risk: Integrating AI vulnerabilities into your broader risk scoring to understand their true impact on the firm’s security posture, rather than treating them in a silo
- Balancing speed with data control: Strategies to enable fee-earner innovation and efficiency while maintaining the data segregation and privacy standards required by client audits