Post event report

Strategic Sponsors

BYTES

CROWDSTRIKE

Kiteworks

mimecast

THREATLOCKER

Education Seminar Sponsors

ARCTIC WOLF

gradian™

LayerX

RISK LEDGER

Networking Sponsors

runZero

secon.

wavenet

Branding Sponsor

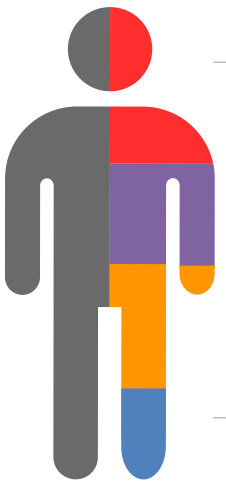
cyderes

Inside this report:

Key themes

- Using the right threat intelligence in the right way
- Managing insider threats at a time of crisis
- Automate your red-teaming and attack simulations
- How behavioural analytics is getting better
- Resilience IS proactive
- Can you really rely on the Cloud?
- Encrypt and tokenise the lot?
- Cloud incident response
- Embracing risk management
- Ransomware – dealing with the new normal
- From cybercrime to cyberwar
- NIS2 – changing the game in cybersecurity?

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

Damian Acklam, Founder & CEO, Gradian

Adam Avards, Principal for Cyber and Third-Party Risk Policy, UK Finance

Neil Bell, Information Security Manager, Forster LLP

James Burchell, Sales Engineering Manager, CrowdStrike

Scott Chenery, Regional Manager UK & Ireland, Kiteworks

Tim Collinson, Head of Information Security, Walkers

Steve Davies, Head of Cyber Security, DLA Piper

William Dixon, Associate Fellow, Royal United Services Institute and Senior Technology Cyber Fellow, The Ukraine Foundation

Luke Fardell, Lead Cyber Analyst, Tokio Marine Kiln

Rob Flanders, Head of Threat and Incident Response, BAE Systems

Khetan Gajjar, Field CTO, EMEA, Mimecast

Henry Glynn, Cyber Security Solutions Specialist, Bytes

Nathan Hayes, Director of IT, Three Crowns

Graham Holt, Regional Vice President (Sales), Arctic Wolf

Federico Iaschi, Information Security Director, Starling Bank

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

Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England

David Segev, VP Sales Global Strategic Accounts & International Markets, LayerX

Ali Shepherd, Director of Cyber & Operational Resilience (CISO), FCA

Ash Spencer, Head of IT and Security, Minster Law

Chris Worthy, Former Deputy Director, UK Home Office & Independent Consultant

Agenda	
08:00	Registration and networking breakfast
08:50	Chair's welcome
09:00	**Briefs and breaches: Why foreign States target law firms** **Chris Worthy,** Former Deputy Director, UK Home Office & Independent Consultant • State-sponsored espionage and where cyber fits in • Why would foreign States carry out espionage (including cyber) against law firms? • How they use the information gathered • The range of techniques used (including cyber and non-cyber methods)
09:20	**Bridging the cybersecurity skills gap. Are you part of the problem or part of the solution?** **Ash Spencer,** Head of IT and Security, Minster Law • What is the cybersecurity skills gap? • What problems or challenges do those gaps cause? • Some potential solutions to address the skills gap within your organisation
09:40	**Safeguarding your enterprise: Addressing human and insider risks in data loss prevention** **Henry Glynn,** Cyber Security Solutions Specialist, Bytes; **James Burchell,** Sales Engineering Manager, CrowdStrike; **Khetan Gajjar,** Field CTO, EMEA, Mimecast • Addressing both accidental and malicious data loss • The importance of managing human risk and insider threats • How to enhance user awareness to prevent accidental data loss • Securing collaborative platforms to prevent data breaches • Ensuring compliance with regulatory requirements to mitigate risks • Detecting anomalous user behaviour to identify potential insider threats and prevent malicious data loss
10:00	**Securing GenAI: Our journey & lessons learned** **Ali Shepherd,** Director of Cyber & Operational Resilience (CISO), FCA • Balancing innovation and risk • Embedding responsible AI • Addressing novel risks and threats
10:20	**Education Seminars | Session 1** Arctic Wolf **Security operations and the cloud: How to address the security staff shortage** **Graham Holt,** Regional Vice President (Sales), Arctic Wolf Gradian **Two sides of the same coin: How DLP and Zero Trust create unified data protection,** **Damian Acklam,** Founder & CEO, Gradian
11:00	Networking break
11:30	**PANEL DISCUSSION Managing elevated threats: Protecting clients, staff, and data** **Steve Davies,** Head of Cyber Security, DLA Piper (Moderator); **Chris Worthy,** Former Deputy Director, UK Home Office & Independent Consultant; **Neil Bell,** Information Security Manager, Forster LLP; **Luke Fardell,** Lead Cyber Analyst, Tokio Marine Kiln; **Tim Collinson,** Head of Information Security, Walkers • How is the firm addressing the risk of being targeted due to representing politically sensitive or high-profile clients? • What measures are in place to protect partners and employees during travel to regions with heightened security concerns? • How are we preparing for potential threats from activists, hacktivist groups, or state-sponsored actors targeting the firm or its clients?
12:00	**Data security, governance & consolidation for legal firms** **Scott Chenery,** Regional Manager UK & Ireland, Kiteworks • Your data, why is it so important? • Centralised data governance whilst maintaining end user experience • Possession less editing – why it's here and why you need it • Consolidation of data sharing applications

Agenda

12:20 — Cyber-leadership in an era of dis-cooperation

William Dixon, Associate Fellow, Royal United Services Institute and Senior Technology Cyber Fellow, The Ukraine Foundation

- How global trade fragmentation impacts the community
- How Western Government Foreign Policy changes could lead to cyber-instability
- Actions the cyber C-Suite can take

12:40 — Education Seminars | Session 2

LayerX	Risk Ledger
Securing the last mile – Rethinking browser security in the enterprise	**Supplier engagement is key to building supply chain resilience**
David Segev, VP Sales Global Strategic Accounts & International Markets, LayerX	**Justin Kuruvilla,** Chief Cyber Security Officer, Risk Ledger

13:20 — Lunch networking break

14:30 — Quantum leap – Preparing for a quantum-safe future

Steve Davies, Head of Cyber Security, DLA Piper

- What is quantum computing and what does it mean for the enterprise?
- What are the risks and how serious is the threat from quantum computing?
- How can you prepare for the post-quantum future, today?
- What does post-quantum readiness look like across technology service providers?

14:50 — Securing cloud adoption in law firms

Neil Bell, Information Security Manager, Forster LLP

- Why cloud adoption security is critical for modern legal practices – for efficiency, scalability, and business continuity
- Aligning cloud security strategy with firm-specific goals
- Understanding regulatory and jurisdictional impacts, such as GDPR, HIPAA, and attorney-client privilege obligations
- Developing a risk-based approach that integrates cybersecurity from day one, not as an afterthought and not losing sight of customer needs

15:10 — PANEL DISCUSSION: Operationalising threat intelligence in high-risk environments

Rob Flanders, Head of Threat and Incident Response, BAE Systems; **William Dixon,** Associate Fellow, Royal United Services Institute and Senior Technology Cyber Fellow, The Ukraine Foundation; **James Kwaan,** CIO – GS&S, Lloyds Banking Group; **Ash Spencer,** Head of IT and Security, Minster Law; **Nathan Hayes,** Director of IT, Three Crowns

- How can traditional cyber-intelligence be integrated into threats to legal practice?
- Can existing intelligence marking schemes (e.g. TLP) be easily fit with restrictions surrounding legal privilege?
- How can intelligence support the mitigation of attacks against VIPs, case leads, and privileged data?
- Which is of greatest concern to the legal sector – ransomware or targeted attacks?

15:50 — Networking break

16:10 — Ransomware in financial services: How AI-driven ransomware will trigger the next major breach

Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England

- LIVE DEMO - Inside the first AI-powered ransomware attack
- Why financial services is the perfect target – and how attackers are breaking in more easily than most think
- First-hand insights from real-world red team ops
- Why traditional security fails – compliance checklists and conventional tools don't stop modern ransomware
- What CISOs and security leaders must do now

16:30 — PANEL DISCUSSION: The quantum threat timeline: Migration challenges and strategic planning

Adam Avards, Principal for Cyber and Third-Party Risk Policy, UK Finance (Moderator); **William Dixon,** Associate Fellow, Royal United Services Institute and Senior Technology Cyber Fellow, The Ukraine Foundation; **Federico Iaschi,** Information Security Director, Starling Bank

- What is the current state of quantum computing and how soon must financial institutions act to mitigate quantum threats?
- What are the real-world implications of transitioning to quantum-resistant algorithms?
- How can organisations build roadmaps that align with regulatory and operational realities?

17:00	Chair's closing remarks	**17:00**	Drinks reception	**18:00**	Conference close

Education Seminars	
Arctic Wolf **Security operations and the cloud: How to address the security staff shortage** **Graham Holt,** Regional Vice President (Sales), Arctic Wolf	Cybersecurity continues to be a top priority for law firms – yet the operational burden, resource challenges, and fast-evolving threat landscape make it difficult to stay ahead. As more firms shift critical business functions to cloud-based SaaS platforms, it's time to ask: Should security operations follow suit? This discussion will bring together CISOs, CIOs, IT Directors, and Partners from the legal industry to explore key challenges. Attendees will learn: • Shortage of skilled security professionals and retention difficulties • The need for continuous, 24x7x365 monitoring across increasingly complex security stacks • Alert fatigue and dissatisfaction with existing tools-based approaches • Rising compliance demands and the growing cost of cyber-insurance
Gradian **Two sides of the same coin: How DLP and Zero Trust create unified data protection,** **Damian Acklam,** Founder & CEO, Gradian	Data loss prevention programmes and Zero Trust frameworks are essential initiatives of your organisation's modern cybersecurity strategy. Each embraces the fundamental need to successfully protect organisational data in an increasingly complex threat landscape. It is estimated that 35% of DLP Gen 1 implementations have failed due to them creating 'too much noise', meanwhile Zero Trust is (in some respects) considered 'revolutionary' to help drive user productivity in the face of changing mobility patterns. The modern enterprise now faces two challenges – how to protect your data whilst simultaneously enabling access to it! Attendees will learn: • How DLP and Zero Trust are two sides of the same coin • How 'tooling first' conversations are a hindrance rather than a help • How 'time' is your friend when it comes to being successful – the programmatic approach wins! • Why strong policy creation and ongoing policy management are so important • The only 3 outcomes that you should care about to define success
LayerX **Securing the last mile – Rethinking browser security in the enterprise** **David Segev,** VP Sales Global Strategic Accounts & International Markets, LayerX	Modern enterprises face an evolving threat landscape where the browser has become a significant point of vulnerability. Traditional security measures often fall short in addressing the unique risks associated with browser usage, including SaaS sprawl, the rise of shadow AI, and the proliferation of malicious browser extensions. This session will explore why the browser is now the riskiest application within the enterprise and demonstrate how LayerX provides a novel approach, transforming the browser into a controllable, visible, and secure workspace, moving beyond Zero Trust to achieve Zero Gaps security. Attendees will learn: • Understand the evolving risks that make the browser a prime target in today's enterprise environment • Identify the limitations of traditional security approaches in addressing modern browser-based threats • Learn about emerging threats such as SaaS sprawl, shadow AI, and malicious browser extensions that exploit browser vulnerabilities • Discover how LayerX offers a comprehensive solution to secure browser activity, enhancing visibility and control
Risk Ledger **Supplier engagement is key to building supply chain resilience** **Justin Kuruvilla,** Chief Cyber Security Officer, Risk Ledger	Supply chain risk management involves complex business relationships and vast data volumes, yet many organisations still rely on static spreadsheets in shared drives. We examine why Third-Party Risk Management (TPRM) often fails and how strategic collaboration can improve security across your entire supply chain. Attendees will learn: • Why traditional TPRM approaches fall short in today's interconnected threat landscape • How engaging suppliers directly can reduce friction and improve data quality • What 'good' looks like: practical steps to move from transactional to collaborative supply chain security