Post event report

SECURING FINANCIAL SERVICES

Securing Financial Services

20th January 2026, London

Strategic Sponsors

Akamai

censys

rubrik

THREATLOCKER® ZERO TRUST PLATFORM

Education Seminar Sponsors

COFENSE

harmonic

invicti

opentext™

Networking Sponsors

1Password

BITSIGHT

CONCENTRIC AI

CYBER VIGILANCE

CYERA

Executive Roundtable Sponsor

CDW

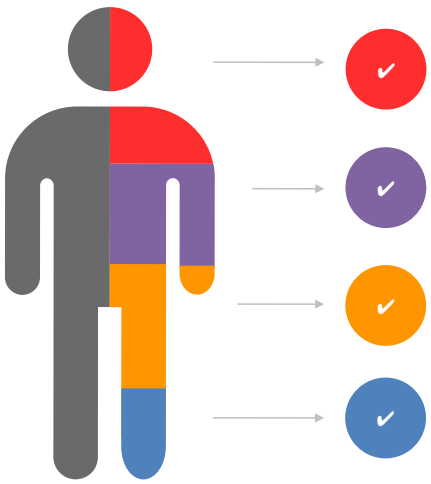
rubrik

Inside this report:

Key themes

- Securing the AI supply chain – a new 3rd party problem
- Embedding AI in the security stack
- Adversarial threats and AI exploits
- Protecting critical data in the age of AI
- Securing agentic AI
- AI everywhere: mapping the new attack surface

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

Steve Armstrong-Godwin, Lead of Security Incident Response and Threat Management, **Danske Bank**

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

Guy Batey, Head of Specialist Engineering EMEA, **Rubrik**

Simon Brady, Event Chairman, **AKJ Associates**

Sven Dehnert, Principal Solutions Consultant, **OpenText**

James Derbyshire, Cybersecurity Entrepreneur, **Harmonic Security**

Paul Fearns, Senior Enterprise Security Architect, EMEA, **Akamai Technologies**

Gill Fenney, Former Head of IT Risk Governance, **Bupa**

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

James Hickey, Principle Sales Engineering, **Cofense**

Federico Iaschi, Information Security Director, **Starling Bank**

Raphael Marranghello, Account Executive, **ThreatLocker**

Ioan Nascu, GenAI Security Assurance specialist, **Citi**

Will Packard, Director – Operational Resilience, **Ernst & Young LLP**

Nick Palmer, Technical Lead, **Censys**

Steph Phelps, Global Operational Resilience Specialist, **RGA**

Mark Schembri, Field Software Engineering Manager, **Invicti Security**

Claire Schrader, Senior Cyber Security Specialist, **Lloyds Banking Group**

Jonathan Turner, Head of Cyber Security, **Farrer & Co**

Ryan Virani, Founder, **Cyber Moves Ltd**

Evie Wild, Information Security Officer, EMEA Region, **LBBW Bank**

Agenda

08:00 Breakfast networking break

09:00 Chair's welcome

09:10 **Defining and securing AI responsibilities in financial service**

Ioan Nascu, GenAI Security Assurance specialist, Citi

- Introducing a pragmatic framework that clarifies cybersecurity accountabilities between financial institutions and AI providers
- Leveraging familiar IaaS, PaaS, and SaaS structures to map security responsibilities for AI systems
- Applying the model to Foundation Models to support secure and responsible AI adoption
- Enabling a flexible, high-level approach tailored to the financial sector's evolving needs

09:30 **The imperative for cyber-resilience in financial services**

Guy Batey, Head of Specialist Engineering EMEA, Rubrik

- Attack reality: Hyper-innovation and Industrialised AI are accelerating attacks, rendering traditional prevention ineffective and expanding the regulatory/technological attack surface
- Strategic mandate: The security posture must adopt the 'Assume Breach' Mandate, acknowledging inevitable compromise
- Shift in focus: Security emphasis must move from perimeter control to robust in-network capabilities
- Core pillars: The strategy hinges on rapid Detection, effective Response, and, most critically, Rapid Recovery of business operations post-compromise
- Ultimate metric: Cyber-resilience – the capacity to withstand the attack and reliably recover – is the only meaningful metric for protecting firm stability and meeting regulatory obligations

09:50 **Getting supply chain risk management right**

Evie Wild, Information Security Officer, EMEA Region, LBBW Bank

- How to build a culture that drives quality awareness and early risk detection
- How to apply focused due diligence and tiering to target the highest-impact risks
- How to empower SMEs and shift left to influence decisions before they solidify
- Getting supply chain risk management right
- How to control hidden risks by addressing shadow IT/procurement and gating spend before payment

10:10 **Education Seminars | Session 1**

Cofense	Open Text
Transparent AI & automation: Taking control of phishing defence	**Beyond compliance: Securing AI-driven financial services against insider risk and emerging threats**
James Hickey, Principle Sales Engineering, Cofense	**Sven Dehnert,** Principal Solutions Consultant, OpenText

10:50 Networking break

11:20 **The calming of the 'Cs'**

Gill Fenney, Former Head of IT Risk Governance, Bupa

- Compliance – the ever increasing burden on financial services
- Complexity – the nuances of various compliance commitments
- Cost – the cost of attaining and maintaining compliance
- Chaos – the risk of an unstructured approach

11:40 **Mapping criminal infrastructure: Reducing financial exposure from abused RDP and bulletproof hosting**

Nick Palmer, Technical Lead, Censys

- Criminal groups use resilient hosting and abused remote access to sustain ransomware and fraud
- Censys + honeypots map patterns in exposed RDP and bulletproof hosting
- Persistent infrastructure increases ongoing financial risk
- Actionable signals help prioritise mitigation despite unclear attribution

12:00 **The rise of AI-assisted attacks on APIs**

Paul Fearns, Senior Enterprise Security Architect, EMEA, Akamai Technologies

- Recognise emerging AI-enabled attack patterns in financial ecosystems
- Learn controls that prevent prompt-injection, model-poisoning, and synthetic automation
- Understand frameworks to align AI security with FFIEC, NIST, and OWASP guidance

Agenda

12:20 — **Zero Trust controls at the endpoint**

Raphael Marranghello, 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

12:25 — **Education Seminars | Session 2**

Harmonic Security	Invicti Security
Adopting AI across the workforce with confidence	**Shadow API: Find them, test them, fix what matters**
James Derbyshire, Cybersecurity Entrepreneur, Harmonic Security	**Mark Schembri,** Field Software Engineering Manager, Invicti Security

13:05 — Lunch networking break

14:00 — **Securing the AI revolution in banking, insurance and asset management**

Adam Avards, Principal for Cyber and Third Party Risk Policy, UK Finance (Moderator); **Steph Phelps,** Global Operational Resilience Specialist, RGA; **Claire Schrader,** Senior Cyber Security Specialist, Lloyds Banking Group; **Gill Fenney,** Former Head of IT Risk Governance, Bupa; **Ioan Nascu,** GenAI Security Assurance specialist, Citi

- For security leaders, the challenge is stark: how do you secure these systems, ensure compliance, and maintain resilience when the technology itself is evolving faster than the controls designed to protect it?
- Future-proofing security: Designing adaptive governance and security frameworks that evolve alongside AI, rather than always playing catch-up
- DORA and AI compliance: How the Digital Operational Resilience Act reshapes resilience expectations in banking, insurance, and asset management, especially for fast-evolving AI systems
- Securing the AI supply chain: Managing third-party and model risks, from external data providers to cloud-based AI platforms, in line with DORA's ICT risk requirements
- Balancing innovation and control: Embedding resilience testing and security guardrails without stifling AI-driven innovation

14:30 — **Keeping security teams sharp in the absence of incidents**

Steve Armstrong-Godwin, Lead of Security Incident Response and Threat Management, Danske Bank

- Experience-led insights into keeping security teams sharp when incidents are rare but stakes remain high
- Practical methods for building confidence and coordination through low-friction, high-impact exercises
- Design principles for simulations and training that fit real-world constraints, not fantasy budgets
- Tactics to avoid drift, burnout, and complacency – without waiting for a crisis to galvanise the team

14:50 — **The new CISO deal**

Ryan Virani, Founder, Cyber Moves LTD

- CISO and Head of Security briefs have changed in the last 2–3 years
- What 'good' now looks like in successful CISO appointments, from a talent and behaviours perspective
- Snapshot of current salary and day-rate ranges for CISOs and Heads of Security
- Where mandate, support and reward are misaligned, and what CISOs are now asking for before they say yes

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	
Cofense **Transparent AI & Automation: Taking control of phishing defence** **James Hickey,** Principal Sales Engineering, Cofense	In today's rapidly evolving threat landscape, email remains a primary attack vector for cybercriminals. Whilst AI tools seem an ideal solution, the reality is that they come with risks and limitations leaving organisations vulnerable. Join us for an insightful session where we will explore how to build resilient phishing defence that stays ahead of emerging threats by balancing automation and human expertise. **Attendees will learn:** • The power of live threat data: Learn why real-time threat intelligence is critical for robust email protection and how it can help you stay one step ahead of attackers • Crowdsourced intelligence without the risks: Discover how to leverage the collective power of crowdsourced threat data while mitigating potential privacy and security concerns • AI and automation in phishing defence: Understand the optimal roles of AI and automation in detecting, preventing, and responding to email-based threats
Harmonic Security **Adopting AI across the workforce with confidence** **James Derbyshire,** Cybersecurity Entrepreneur, Harmonic Security	Organisations across industries are accelerating their use of AI to improve efficiency, remain competitive, and empower employees. Financial services firms, in particular, face mounting pressure to innovate while adhering to strict regulatory expectations and protecting highly sensitive data. As AI becomes woven into everyday workflows through sanctioned tools, embedded features, and a long tail of unsanctioned applications, leaders must determine how to safely enable broad adoption without introducing new operational, compliance, or security risks. This session examines the real patterns emerging inside enterprise environments as AI usage expands. Drawing on observed behaviour across hundreds of companies, we will break down why legacy assumptions about control no longer hold true. Employees increasingly rely on personal accounts, free tier tools, and AI powered SaaS features, often without awareness of where their data is going or how it may be retained. These shifts create new exposure pathways, from inadvertent sharing of regulated information to interactions with models that train on user inputs. Building on these insights, the session offers a practical framework for safe, scalable AI enablement. Rather than relying on restrictive blocks that inadvertently drive shadow adoption, organisations are beginning to apply intelligent guardrails that monitor AI usage, detect sensitive data, and enforce policy in real time. This approach supports responsible experimentation while ensuring regulatory alignment and reducing the likelihood of costly data mishandling. Attendees will leave with actionable guidance for operationalising AI governance in complex, regulated environments and a clear understanding of how leading firms are balancing innovation with risk. **Attendees will learn:** • The realities of enterprise AI adoption and why usage is now distributed and often unsanctioned • The most common exposure patterns and governance gaps emerging across financial services and other regulated industries • How to establish guardrails that detect sensitive data, understand user intent, and enforce policy without hindering productivity • A practical framework for enabling responsible AI use that supports innovation, oversight, and continuous monitoring

Education Seminars	
Invicti Security **Shadow API: Find them, test them, fix what matters** **Mark Schembri,** Field Software Engineering Manager, Invicti Security	Financial institutions are rapidly expanding their API ecosystems to power banking, payments, trading, and partner integrations. Yet many security teams still lack complete visibility into the APIs operating across their environment. Undiscovered or 'shadow API' introduces hidden risk – creating pathways for data exposure, fraud, and non-compliance. In this session, you will learn how you can apply Invicti's multilayered approach to API discovery and schema reconstruction. Once discovered, you test these APIs with the industry's best API DAST. Validating difficult-to-find vulnerabilities like BOLA and BLFA, business logic errors, and the presence of weak authentication with proof-based scanning to achieve AppSec's charter that only secure APIs reach production. **Attendees will learn:** • Discover hidden APIs • Improve governance • Identify unmanaged APIs • Align with OWASP Top 10 for API
OpenText **Beyond compliance: Securing AI-driven financial services against insider risk and emerging threats** **Sven Dehnert,** Principal Solutions Consultant, OpenText	AI is transforming UK financial services, but it's also expanding the attack surface faster than traditional controls can adapt. Under the FCA's Operational Resilience framework, firms must evidence resilience across critical services while managing new risks introduced by AI models, agentic workflows, and opaque supply chains. This session goes beyond compliance to show how behavioural analytics and insider-risk detection can safeguard AI-enabled operations without drowning SOC teams in alerts. Delegates will leave with a clear roadmap for aligning insider-threat detection with FCA resilience requirements while addressing emerging AI-driven risks that traditional rules and signatures simply can't catch. **Attendees will learn:** • The new insider-risk challenge in an AI-first world: Why credential misuse, lateral movement, and data exfiltration now intersect with adversarial AI exploits and model drift • Bridging FCA resilience mapping with NCSC insider-risk guidance: Practical steps to embed detection into SOC workflows and demonstrate resilience • Behavioural AI in action: How OpenText Core Threat Detection & Response (Core TDR) integrates with Microsoft Defender for Endpoint and Microsoft Entra ID to deliver MITRE-aligned, plain-language insights that accelerate investigations and cut through noise