

Post event report



Strategic Sponsors



Education Seminar Sponsors



Branding Sponsor



“ Thanks for another thought-provoking event. Some useful insights into technical security in terms of implementing cloud security controls, and assessing the risk of open source code in our applications, and implementing Policy as Code. And also more general resilience approaches. A day well spent. ”

Head of Information Security,
Salary Finance

- Inside this report:
- Sponsors
 - Key themes
 - Who attended?
 - Speakers
 - Agenda
 - Education Seminars



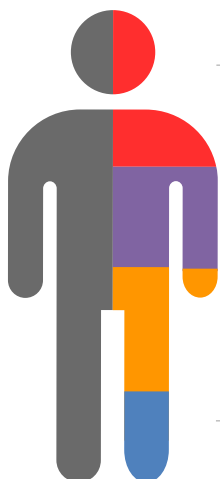
Speakers

- Muhammad Ali, Cyber Security Solutions Engineer, **Exponential-e**
- Adam Avarids, Principal for Cyber and Third Party Risk Policy, **UK Finance**
- Brett Ayres, VP of Product, **Teneo**
- Zsuzsanna Berenyi, Senior Cyber Security Third-Party Risk Manager, **LSEG**
- Chantal Constable, Head of Financial Services & Insurance, **NCC Group**
- Marcus Corry, Director, Tech&Ops, **AFME**
- Greg Duffy, M.Eng., Product Marketing Director, EMEA, **Cato Networks**, on behalf of **Wavenet**
- Gill Fenney, Head of IT Risk Governance, Bupa; Tanya Layng, Contract Lawyer, **IQ-EQ**
- Orlando Fernandez, Senior Technical Specialist at the Recovery, Resolution & Resilience team, Prudential Policy Directorate, **Bank of England (BoE)**
- Leor Golan, Sales Director, **Blink Ops**
- Chris Greany, Director of Security & Technology Risk, **Pay.UK**
- Michael Jefferson, Head of Financial Services Public Policy UK, Middle East, Africa and Switzerland, **Amazon Web Services (AWS)**
- Siân John MBE, Chief Technology Officer, **NCC Group**
- Yonatan Khen, Security Research Team Leader, **Hunters**
- Danielle Kinsella, Technical Advisor EMEA, **Gigamon** on behalf of **Fortem-IT**
- Mehran Koushkebaghi, Head of Product Security, **Nationwide Building Society**
- Justin Kuruvilla, Chief Cybersecurity Strategist, **Risk Ledger**
- James Kwaan, CIO – GS&S – Chief Security Officer, **Lloyds Banking Group**
- Rory Malone, Principal, Global Privacy & Security Regulatory Compliance, **Cloudflare**
- Nick Palmer, Senior Solutions Engineer, **Censys**
- Ketan Pyne, Pre Sales team for UK&I & Matthew Santos, **Thales Group**
- Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, **Bank of England**
- Ryan Searle, Director, Product Management, **Snyk**
- Praveen Singh, Head of IT Risk and Cybersecurity, **ICBC Standard Bank**
- Peter Smith, Chief Information Security Officer, **Allica Bank**
- Alistair Wardell, Director, Cloud Security, **Deutsche Bank**
- Steven Wills, Senior Engineer, **Abnormal Security**

Key themes

- Reining in third parties
- Securing the technologies of the future
- Where does AI make most sense?
- From cybercrime to cyberwar
- The rise and rise of effective cybersecurity regulation
- From Cloud security to Cloud incident response

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

Agenda		
08:00	Breakfast & networking break	
08:50	Chair's welcome	
09:00	Implementing security controls at scale in Google Cloud	
	<p>Alistair Wardell, Director, Cloud Security, Deutsche Bank</p> <ul style="list-style-type: none"> • How we built up our cloud security controls, layer by layer • What we learned on the way • What we will work on next 	
09:20	A risk-based approach to prioritising software supply chain finding	
	<p>Ryan Searle, Director, Product Management, Snyk</p> <ul style="list-style-type: none"> • Security backlogs are growing larger each day • Why traditional prioritisation approaches no longer cut it • How to focus on the issues that matter and prevent them earlier in the SDLC 	
09:40	FIRESIDE CHAT: Securing the future of financial services	
	<p>Chantal Constable, Head of Financial Services & Insurance, NCC Group (Moderator); Siân John MBE, Chief Technology Officer, NCC Group; Chris Greany, Director of Security & Technology Risk, Pay.UK</p> <ul style="list-style-type: none"> • We're living through a digital revolution. Artificial intelligence, quantum computing, connected devices – these technologies promise immense potential, but introduce new risks • Siân and Chris will explore the complexities the UK's financial services sector faces when preparing for risks (both known and unknown) in 2025 and beyond: <ol style="list-style-type: none"> a) securing emerging technologies, b) managing governance and expanding regulations c) achieving and maintaining operational resilience • You'll come away from the session knowing how to design and build a resilient digital future for your organisation 	
10:00	Harnessing Policy-as-Code for embedding security controls in CI/CD pipelines	
	<p>Mehran Koushkebaghi, Head of Product Security, Nationwide Building Society</p> <ul style="list-style-type: none"> • What is Policy-as-Code, and what are its benefits in the context of security policies? • Leveraging Policy-as-Code for automating policy evaluation & enforcement in SDL • Components of a Policy Enforcement System • Integrating the Policy Enforcement System into the CI Pipeline • How does it work in practice? A sample implementation 	
10:20	Education Seminars Session 1	
	<p>Abnormal Security Defending financial services: Stopping sophisticated email threats in their tracks Steven Wills, Senior Engineer, Abnormal Security</p>	<p>Thales Financial services cyber-success – 2025 and beyond Ketan Pyne, Pre Sales team for UK&I & Matthew Santos, Thales Group</p>
		<p>Wavenet SASE, past present and future – a new look at what's important for securing today's financial services companies Greg Duffy, M.Eng., Product Marketing Director, EMEA, Cato Networks, on behalf of Wavenet</p>
11:00	Networking break	
11:30	What does DORA mean for cybersecurity within financial services	
	<p>Marcus Corry, Director, Tech&Ops, AFME (Moderator); Gill Fenney, Head of IT Risk Governance, Bupa; Tanya Layng, Contract Lawyer, IQ-EQ; James Kwaan, CIO – GS&S – Chief Security Officer, Lloyds Banking Group</p> <ul style="list-style-type: none"> • The uplift to banks' cyber-controls • How cyber-attacks across the supply chain will in future be mitigated • Information sharing with authorities as part of a firm's response to an incident 	

Agenda			
12:00	AWS gone wild: How attackers exploit your cloud and how to outsmart them		
	<p>Yonatan Khen, Security Research Team Leader, Hunters</p> <ul style="list-style-type: none"> Uncover the anatomy of a real-world AWS attack, including credential exposure, lateral movement, privilege escalation, and persistence techniques Discover practical strategies for detecting threats, securing IAM policies, and monitoring API access patterns to mitigate risks Learn actionable lessons from an incident response case study to strengthen AWS defences, tailored for cloud engineers, security analysts, and incident responders 		
12:20	Leveraging DORA TLPT (Threat-Led Penetration Testing) to enhance cyber-resilience		
	<p>Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England</p> <ul style="list-style-type: none"> How DORA TLPT aligns seamlessly with TIBER-EU, CBEST & DORA to enhance cyber-risk management Discover the benefits of an EU-standard approach to threat-led testing See how DORA TLPT boosts readiness for live system testing Learn how to start using DORA TLPT for ongoing cyber-resilience and regulatory compliance 		
12:40	Education Seminars Session 2		
	<p>Blink Ops</p> <p>Enhancing security through automation: Key strategies and best practices</p> <p>Leor Golan, Sales Director, Blink Ops</p>	<p>Risk Ledger</p> <p>DORA is here: What financial firms can do now, and achieve resilience beyond compliance</p> <p>Justin Kuruvilla, Chief Cybersecurity Strategist, Risk Ledger</p>	<p>Teneo</p> <p>Are you truly secure? Answer these three key questions</p> <p>Brett Ayres, VP of Product, Teneo</p>
13:20	Lunch & networking break		
14:20	Prioritising cybersecurity as a strategic component of resilience		
	<p>Praveen Singh, Head of IT Risk and Cybersecurity, ICBC Standard Bank</p> <ul style="list-style-type: none"> Understanding the critical role of cybersecurity in operational resilience Strategic integration of cybersecurity into overall risk management and operational strategies Understanding the investment priorities to enhance cybersecurity Practical insights along with actionable steps for implementation 		
14:40	What's next for the internet and financial services in 2025: Trends, regulations, and Cloudflare's perspective		
	<p>Rory Malone, Principal, Global Privacy & Security Regulatory Compliance, Cloudflare</p> <ul style="list-style-type: none"> Notable attacks and trends in 2024 against financial services, as seen through the Cloudflare Network Will the Cyber Security and Resilience Bill criminalise ransomware payments? The impact of 2025's cybersecurity, privacy, and operational resilience regulations Insights and predictions for 2025, and how we plan to help build a better internet 		
15:00	How to manage your risks and protect your financial data		
	<p>Nick Palmer, Senior Solutions Engineer, Censys</p> <ul style="list-style-type: none"> Gain insights into the evolving risk landscape, including threats from compromised third-party providers, unpatched systems, outdated technology, and data breaches Learn strategies for effective threat response and compliance with DORA regulations using modern cybersecurity solutions Explore how to leverage the Censys Internet Map for proactive risk identification and mitigation 		
15:20	Education Seminars Session 3		
	<p>Exponential-e</p> <p>Room for improvement – Securing financial services with a robust privileged access management strategy</p> <p>Muhammad Ali, Cyber Security Solutions Engineer, Exponential-e</p>	<p>Fortem-IT</p> <p>Strengthening operational resilience: Navigating regulatory compliance with Gigamon</p> <p>Danielle Kinsella, Technical Advisor EMEA, Gigamon on behalf of Fortem-IT</p>	
16:00	Networking break		
16:20	Partnerships or pitfalls? Mastering third-party risk		
	<p>Adam Avars, Principal for Cyber and Third Party Risk Policy, UK Finance (Moderator); Orlando Fernandez, Senior Technical Specialist at the Recovery, Resolution & Resilience team, Prudential Policy Directorate, Bank of England (BoE); Peter Smith, Chief Information Security Officer, Allica Bank; Michael Jefferson, Head of Financial Services Public Policy UK, Middle East, Africa and Switzerland, Amazon Web Services (AWS); Zsuzsanna Berenyi, Senior Cyber Security Third-Party Risk Manager, LSEG</p> <ul style="list-style-type: none"> Insights from the PRA, end-users, and suppliers on managing third-party risks Navigating the evolving regulatory landscape and its influence on third-party partnerships Strategies to identify and mitigate third-party risks Transforming strong risk management practices into a competitive edge 		
17:00	Drinks reception & networking break		18:00 Conference close

Education Seminars	
<p>Abnormal Security</p> <p>Defending financial services: Stopping sophisticated email threats in their tracks</p> <p>Steven Wills, Senior Engineer, Abnormal Security</p>	<p>The financial services industry is under constant attack from sophisticated email threats, from invoice fraud to executive impersonation and credential harvesting. Join Abnormal Security as we explore real-world examples of email attacks targeting financial services organisations and demonstrate how our advanced AI-powered solution proactively detects and stops these threats.</p> <p>Attendees will learn:</p> <ul style="list-style-type: none"> • Understand the threat landscape: Insight into the most prevalent and damaging email attacks affecting financial services today • Real-world case studies: Examples of successful and thwarted attacks to highlight vulnerabilities and risks • Achieving operational efficiency: Save time for IT and security teams while improving overall email security posture
<p>Blink Ops</p> <p>Enhancing security through automation: Key strategies and best practices</p> <p>Leor Golan, Sales Director, Blink Ops</p>	<p>As cyber-threats grow in sophistication and volume, organisations face mounting challenges with alert fatigue and security talent shortages. This short presentation examines how modern security automation transforms defensive capabilities through AI-powered, no-code solutions. We'll explore essential automation tools, practical implementation strategies, and high-impact use cases in threat detection, vulnerability management, and cloud security. Attendees will learn how to identify automation opportunities, design effective workflows, and measure ROI. The session concludes with actionable steps for leveraging automation to strengthen security posture while enabling teams to focus on strategic priorities.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • Security challenge & urgent need • Evolution to modern solutions • Automation implementation strategy • Measuring success
<p>Exponential-e</p> <p>Room for improvement – Securing financial services with a robust privileged access management strategy</p> <p>Muhammad Ali, Cyber Security Solutions Engineer, Exponential-e</p>	<p>The evolving threat landscape, driven by advancements in AI and the proliferation of data, demands advanced solutions. While AI-based perimeter defences have significantly strengthened security, insider threats continue to pose a critical challenge.</p> <p>As highlighted by CBEST (2024), weak privileged access controls in the financial sector underscore the need for robust privileged access management solutions to mitigate risks such as lateral movement and supply chain attacks.</p>
<p>Fortem-IT</p> <p>Strengthening operational resilience: Navigating regulatory compliance with Gigamon</p> <p>Danielle Kinsella, Technical Advisor EMEA, Gigamon on behalf of Fortem-IT</p>	<p>Operational resilience is essential for organisations navigating mandates from the PRA, FCA, Bank of England, and new legislation such as DORA to ensure service continuity. It relies on systems that enhance visibility, control, and security across hybrid infrastructures to maintain stability, protect assets, and ensure compliance.</p> <ul style="list-style-type: none"> • Learn how unified visibility detects anomalies to safeguard operations • Explore risk management strategies to minimise downtime and protect services. • Understand how compliance frameworks bolster stability and stakeholder confidence

Education Seminars	
<p>Risk Ledger</p> <p>DORA is here: What financial firms can do now, and achieve resilience beyond compliance</p> <p>Justin Kuruvilla, Chief Cybersecurity Strategist, Risk Ledger</p>	<p>With DORA now in full force, financial institutions are facing new challenges in how they are expected to safeguard their digital supply chains. This session will explore how DORA's enforcement affects third-party risk management, provide practical strategies for what to do next even if you are not yet fully compliant, and explore options to enhance individual firms' operational resilience and supply chain cybersecurity beyond DORA compliance.</p> <p>Attendees will learn:</p> <ol style="list-style-type: none"> 1. What does DORA say about TPRM and supply chain security 2. If you are not yet compliant, this is what you should do next 3. We help FS firms really improve their operational resilience and spot concentration risks and empower you, not like regulators
<p>Teneo</p> <p>Are you truly secure? Answer these three key questions</p> <p>Brett Ayres, VP of Product, Teneo</p>	<p>Financial institutions face relentless and sophisticated cyber-threats, creating a need for a multi-layered defence essential to safeguarding critical systems and sensitive data. This presentation introduces our three-part strategy to identify, protect, and maintain security, offering actionable insights to stay ahead of evolving risks.</p> <p>Attendees will learn:</p> <p>The three key areas to evaluate:</p> <ol style="list-style-type: none"> 1. Identify: Who and what is on my network? Secure access for human and non-human identities. 2. Protect: Who has access to what? Manage networks securely with Aruba EdgeConnect, incorporating end-to-end segmentation and separate overlays. 3. Maintain: How do we stay secure? Ensure resilience through automated auditing, patch management, and validation.
<p>Thales</p> <p>Financial services cyber-success – 2025 and beyond</p> <p>Ketan Pyne, Pre Sales team for UK&I, Thales Group & Matthew Santos, Thales Group</p>	<ul style="list-style-type: none"> • Compliance is not just about avoiding penalties; it's an opportunity to build trust with customers and stakeholders. Financial institutions can enhance customer confidence, improve operational efficiency, and attract investors by demonstrating a commitment to security. • The year 2025 marks a pivotal moment for the financial services industry. The enforcement of DORA and the new PCI DSS 4.0 requirements demand a proactive and comprehensive approach to compliance and security. By addressing these challenges head-on and adopting best practices, financial institutions can meet regulatory obligations and strengthen their resilience against an ever-evolving threat landscape. • Traditional encryption used today would be vulnerable to attacks by powerful quantum computers in the near future. • By proactively transitioning to PQC algorithms now, we ensure our critical data and communication channels are secured well in advance of this potential threat. • The time to act is now!
<p>Wavenet</p> <p>SASE, past present and future – a new look at what's important for securing today's financial services companies</p> <p>Greg Duffy, M.Eng., Product Marketing Director, EMEA, Cato Networks, on behalf of Wavenet</p>	<p>SASE is the modern network and security architecture for digital businesses. But there is one fundamental requirement for SASE to be successful for today's financial services companies.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • Using an example illustrating the single most important thing to get right when building a SASE service • The four transformational impacts from getting it right • A scary vision of what getting it wrong might look like