

SECURING FINANCIAL SERVICES



Securing Financial Services

January 19th, London, UK

Building sustainable, scalable security

More people and more tools are not a sustainable answer to today's security challenge. So how are financial services firms responding to a threat environment transformed by AI and geopolitics?

AKJ Associates

Breaking the link between security workload and security headcount

Simply adding more people and more tools is not a sustainable security strategy. As AI and geopolitics reshape the threat landscape, how can financial services firms combine technology, talent and new operating models to strengthen protection while keeping cost and complexity under control? How do they increase capacity sustainably?

Financial services firms have invested heavily in cybersecurity. The challenge now is to build on that investment: increasing the capacity and effectiveness of security teams as threats evolve, technology estates change and businesses introduce new digital services.

Core defences remain essential. In September 2026, Revolut reportedly disclosed sensitive customer information following fraudulent requests through an apparently legitimate government email account, while saying its internal systems and customer funds were unaffected. The incident illustrates the continuing importance of identity verification and well-designed processes, even in technologically sophisticated organisations.

The previous month, hackers launched a wave of sophisticated attacks on Wall Street firms targeting information systems at major money managers. The attack featured voice phishing, or vishing, in which cyber criminals use technology to mimic voices in phone calls or messages to trick employees into revealing sensitive information or granting access. (In KPMG's 2026 survey of 39 wealth and investment firms, 92% placed cyber among their top five risks, with 41% identifying it as their biggest threat.)

These attacks show that banks must continue to focus on core defences against credential theft and other 'traditional' forms of attack.

But their real challenge is increasing the efficiency and sustainability of their security operations as AI and other forms of automation scale up the volume and sophistication of those attacks.

Maintaining their foundations while developing new capabilities creates difficult investment and organisational choices. AI offers opportunities to accelerate detection, investigation and response, but deploying it effectively requires reliable data, appropriate access controls and clear accountability. Leaders must decide which activities to automate, where human judgement adds most value, and how to measure whether new capabilities actually improve protection and release team capacity.

Technology choices and operating models need to evolve together. Consolidating platforms may simplify operations but can also create dependencies or leave gaps in specialist capabilities. Managed services can provide expertise and additional capacity but require effective oversight and clearly allocated responsibilities. Embedding security expertise in product and engineering teams can support faster delivery, provided common standards and accountability remain clear.

Regulation gives these decisions a concrete timetable. New UK requirements for operational incident and material third-party reporting take effect on 18 March 2027, with different scopes for each regime. For affected firms, this makes reliable incident information, clear reporting responsibilities and visibility of supplier arrangements immediate priorities—and strengthens the case for integrating them into everyday operations.

The FCA has also highlighted the potential for frontier models both to strengthen cyber defence and amplify threats to customers, firms and financial stability. The challenge for leaders is deciding where automation delivers dependable protection and where human judgement remains essential. The boardroom conversation is evolving alongside these demands.

Security leaders need to explain what additional investment will achieve, which capabilities can be simplified, and how their decisions support business priorities. Measuring effectiveness, demonstrating resilience and managing dependence on major technology providers are central to that discussion.

Through practical case studies and candid peer discussion, Securing Financial Services will examine how firms can expand security capability without costs and complexity growing at the same rate—and build teams and systems ready to support the next phase of financial innovation.

Key Themes

AI and automation that deliver provable value

The market is moving from "AI-powered" to "AI-proven". Provable value starts with outcomes the customer already measures: mean time to detect and respond, analyst hours returned, false-positive rates, incidents contained before impact. **Can CISOs evaluate AI-enabled security solutions like this? And what about the costs?**

Changing the workforce pyramid

Cybersecurity has long been staffed as a pyramid: a broad base of junior analysts triaging alerts, narrowing to a small tier of senior specialists. **How can organisations redesign early-career roles around supervising, validating and tuning AI, so that automation elevates junior talent instead of eliminating the route to seniority?**

Data control and visibility when there is no perimeter

How can firms enforce confidentiality when data is constantly in motion across systems the firm does not fully control? For CISOs, does this mean that the focus must shift toward controlling data itself rather than the environments it resides in? **If so, what kinds of architectures and solutions can deliver security in that context?**

The future of the CISO

Cyber risk is now a board-level concern, but most CISOs still report into IT and get barely half an hour of board airtime a quarter. Meanwhile, risk, legal and GRC leaders are increasingly claiming ownership of cyber. **So, who should own cyber risk, what the CRO's growing influence means, and what CISOs must do to earn, and keep, a strategic mandate?**

Integrity and the AI-enabled supply chain

AI-native operating models imply dependence on a complex supply chain of foundation models, internal systems, and external APIs and orchestration layers that collectively produce legal work. Imagine the consequences of hacking such a system. **So how do CISOs stop that happening?**

Moving security's ROI

Can we truly quantify the value protection of cybersecurity? Harder, can we prove that security creates value, not just defends it? Does good security mean faster sales cycles, increased trust and so premium pricing, M&A readiness? **Can security vendors and their solutions help reveal and improve the ROI of cybersecurity?**

Key Themes

Transforming the SOC: a case-study in building capacity

Most SOC's are drowning: too many alerts, too few analysts, and burnout that turns recruitment into a treadmill. How should CISOs choose which work to automate, how to keep analysts in control of AI-driven triage and **how can they improve detection speed, reduce false positives and increase staff retention?**

Securing algorithmic insiders

What does "insider threat" mean when the actor is non-human? For CISOs, the focus shifts to monitoring the behaviour of agents as well as users, developing capabilities to detect anomalous machine activity, and establishing effective controls that balance guardrails, detection, and containment. **Do you need AI defences to do that?**

Solving sprawl: getting security tooling under control

Security teams run dozens of tools that overlap and are seldom fully used. The result is wasted budget, alert noise and analysts who spend more time switching consoles than stopping attacks. Now AI is adding a fresh layer. **So, what is the practical route to rationalisation and where do integrated platforms and outsourcing fit in?**

The power of automation

There's too much manual intervention in security. SOAR pulls data from SIEMs, EDRs, firewalls, cloud APIs, ticketing systems threat intelligence feeds, and even email servers and coordinates actions across tools via APIs and prebuilt integrations and intelligent playbooks. **Well, that's the theory. How does it work in the real world?**

The AI productivity paradox: what does it all cost?

AI-powered platforms promise productivity, but is anyone totting up the price? If you add up consumption pricing, data preparation, integration, governance, and the hours spent checking what the machine got wrong plus the cost of securing AI itself then what? **Is AI really the solution to sustainable scalability?**

Regulation latest

Prescriptive regulatory requirements risk forcing investment into compliance and reporting over real risk reduction. The push to land banks with liability for third-party and systemic failures looks disproportionate, despite their limited control over cloud providers and critical vendors. All this creates cost, accountability, and insurability challenges. **So, what are banks doing to mitigate costs and risks?**

Why AKJ Associates?



A History of Delivery

For more than 25 years, AKJ Associates has been running been the world's most sophisticated closed-door meeting places for senior cyber-security professionals from government, law enforcement, intelligence and business.

For example, our annual London-based e-Crime & Cyber Security Congress is still **the largest invitation-only, Chatham House rules**, gathering of the most senior information risk and security professionals from business and government in the world.

The UK Home Office sponsored the public sector delegation from 40 countries in 2002, and we are delighted to say they still do today.

Global Engagement

We have run hundreds of events in the **UK, across Europe, the Middle East and Asia**, attracting **tens of thousands of delegates** in cybersecurity, data security and privacy.

These delegates range from C-suite CIOs, CTOs, CROs and C(ISO)s, to heads of enterprise architecture, desktop and network. They encompass all the senior professionals whose input drives security and privacy solution purchase decisions.

And as well as cross-sector events for both private and public sector, we also design and deliver sector-specific conferences for high-value, high-sophistication sectors including the legal sector, financial services, manufacturing, retail, healthcare, CNI.

Unrivalled Relationships

Events like this have enabled us to build relationships of trust with **the most influential decision-makers** at the full spectrum of public and private sector organisations in the UK, Europe, Asia and the Middle East.

By providing this audience with valuable insights and business intelligence over the past 25 years, we have built up **the world's most significant community of professionals in cybersecurity**.

We use this to develop new events; to conduct research to understand what cybersecurity professionals are doing, thinking and buying; and to market our conferences and other services.

Smart Lead Generation

We have also developed and trained one of the **most effective marketing and telemarketing operations** in the cybersecurity space.

Our in-depth knowledge of the marketplace allows us to design marketing outreach that **consistently delivers the best audiences** for the providers of critical cybersecurity infrastructure and solutions.

We connect vendors directly with B2B decision-makers. By combining unrivalled reach, deep knowledge of specialist markets and sophisticated marketing we **engage buyers to deliver real results**.

Delivering your message direct to decision-makers



Plenary Speakers

The e-Crime & Cyber Security Congress Series events offer sponsors the opportunity to deliver content in a number of different ways.

Plenary speakers **deliver their presentations on the day of the event from a fully featured AV stage to a face-to-face audience.**

Their presentations can contain slides, video and audio and speakers can deliver their speeches from the podium or from any point on the stage.

Plenary presentations are 20 minutes long and take place in the main event auditorium guaranteeing access to the largest possible audience of cybersecurity professionals on the day.

Presentations are generally designed to be informative, topical and actionable, with the use of case studies and up-to-the-minute references to current developments.

Double-handed talks with clients are also welcomed.



Education Seminars

At pre-defined points in the day, attendees will be notified that the main plenary sessions are making way for a series of in-depth technical break-outs.

These sessions of up to 30 attendees are held in break-out rooms and delivered live to attendees.

They are an opportunity for vendors to deep-dive into a topical problem, technology or solution in front of a group of cybersecurity professionals who have self-

selected as being interested in the topic being discussed.

They are also the ideal venue for solution providers to go into technical detail about their own products and services.

These Seminars run simultaneously, and attendees choose which session to attend.

At the end of the Seminar, attendees are notified that Networking time is now available before the next Plenary session.



AKJ Associates

Your team and your resources in real time



Exhibition Booths

Sponsor packages that contain an Exhibition Booth give sponsors the opportunity to be present in the main networking area of the event.

At these booths, sponsor representatives can interact with delegates face-to-face, deliver messaging and technical information via video presentations, demo products using their own BYOD technology and to distribute printed marketing and product information.

Sponsors may wish to consider different ways to drive footfall to their booths.

For example, sponsors who have presented in Plenary or in an Education Seminar can close their presentations by directing the audience to their booths.

And there are additional gamification elements available, including sponsor-supplied prizes, that can effectively drive traffic to booths.



AKJ Associates

Delivering the most senior cybersecurity solution buyers



Our USP? We put buyers and sellers together

We understand that every vendor needs to sell more. That is the bottom line. This is even more necessary in the present situation.

You will have access to the most senior buying audience in the cyber-security market.

AKJ Associates has been building relationships with senior information risk and security professionals for 25 years and our cybersecurity community is the largest of its kind globally.

We know the senior executives who drive strategy from the top, we know the enterprise architects who often control the largest budgets, and we know the IT Security Leads and Engineers who so often dictate the purchase process.

All of these job titles attend e-Crime & Cybersecurity Congress events.

Getting access to the right people at the right time always increases lead generation and always increases profitable sales activity.



AKJ Associates

We deliver the most focused selling opportunity



Specific, actionable and relevant information for time-constrained industry professionals



The perfect platform for solution providers to deliver tailored advice to the right audience

Focus

Target growth

Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.

Leads

Boost sales

Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.

Choice

Meet commercial aims

We work with sponsors to ensure they meet their commercial aims. We offer a number of sponsorship options, each providing specific benefits.

Value

Showcase solutions

Our events provide sponsors with a unique platform to showcase solutions, as well as provide advice on how best to solve delegates' key challenges.

AKJ Associates

SECURING FINANCIAL SERVICES



Delegate Acquisition

- The e-Crime & Cybersecurity Congress has the **largest community of genuine cybersecurity stakeholders** to invite to our events.
- Our reputation for hosting **exceptional events with informative content, excellent networking opportunities and the best vendor partners** means delegates know they are attending a quality event and are willing to give up the time to attend.
- Our delegates are **invited by an in-house delegate liaison team** who call senior security and privacy professionals at public and private sector companies with a personal invitation to attend
- We **follow up all registrations** with further calls, emails on logistics requirements and reminders to **ensure the best possible attendance**.

Lead Sourcing

- The e-Crime & Cybersecurity Congress prides itself on **putting the key cybersecurity buyers and sellers together**
- To offer you the best prospects to network with, **we don't invite academics, job seekers, consultants, non-sponsoring vendors or marketing service providers** to this closed-door event. This **attention to quality over quantity** has been the hallmark of AKJ's events for 25 years.
- Each of our vendor partners will receive a delegate list at the end of the event.
- Through our targeted networking breaks built into our agendas you will have **unrivalled opportunities to network** with high-quality prospects with face-to-face networking at the event.

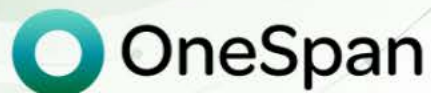
Get Your Message Across

- **Content is king**, which is why the e-Crime & Cybersecurity Congress prides itself on delivering informative and useful content, to attract senior audiences of decision-makers.
- Deliver an exclusive 20-min keynote presentation in the plenary theatre, or host a 30-min targeted workshop session: good content drives leads to your booth, and showcases your company's expertise
- AKJ's in-house content / research team will complement the agenda with best practice from leading experts and senior security professionals from the end-user community
- If you are not presenting, the exhibitor booth offers the opportunity to share white papers and other resources for delegates to takeaway

Exclusivity Delivered

- AKJ Associates has never done trade shows. We see most value in working with a **select number of the top vendor partners** and offering those companies the best access to leads.
- Our events keep the same ethos as when we first started 25 years ago, limiting vendor numbers. We will not be a hangar with hundreds of vendors competing for attention. We will keep our **events exclusive to give the best networking opportunities**.
- All booths offer the same opportunities with the same capacity and functionality regardless of the vendor company.
- This is an opportunity to **continue building pipeline and driving leads** in partnership with our outstanding 25-year reputation and the e-Crime & Cybersecurity Congress brand.

SECURING FINANCIAL SERVICES



"Firstly, a big thank you for yesterday — it was a fantastic event, and we really felt it was a great success. The quality of the attendees was excellent; people were genuinely engaged and very open to conversation. We had strong interest at the stand throughout the day, with many visitors eager to learn more about our solutions."

Sales Manager UK & I



"Thank you for your email. I attended the event yesterday and have to say it was very well organised.

We were very happy with the turnout for our afternoon session as well - all in all, it was a very successful event!

Senior Marketing Executive



"AKJ are a pleasure to work with.

A lot of work goes into making physical events a success, and with AKJ the team are there to support at each step.

They ensure the events are a great success for both suppliers and end users alike."

Senior Digital Marketing Manager



"AKJ has been a valuable partner for us for a few years now, enabling us to build relationships and engage with the CISO community in a number of key territories across Europe. The events they hold are a great vehicle for discussing the latest challenges and our work with them has delivered way beyond expectations."

Senior Marketing Manager

95% percent of our exhibitors and sponsors work with us on multiple events each year.

This is because they generate real business at our events every year. Our sponsor renewal rate is unrivalled in the market.

AKJ Associates