Securing Financial Services

SECURING FINANCIAL SERVICES

Securing Financial Services Summit

January 20th, 2026, London, UK

Securing the AI revolution in banking, insurance and asset management

Banks are at the forefront of AI experimentation and adoption, but how are they securing it and what are the pitfalls?

https://akjassociates.com/event/finserv

AKJ Associates

Securing Financial Services

The frontier challenge in cybersecurity

Artificial intelligence is no longer confined to proofs of concept or innovation labs. In financial institutions across the world, it is moving into production and being embedded in core processes from trading, to surveillance, to fraud and financial crime detection, to compliance. This breadth of deployment means the attack surface is no longer confined to a single system or department. AI is everywhere — and so are its risks.

Some of these systems are built in-house, but many are sourced from vendors or built on open-source frameworks. Some run in tightly controlled bank environments, while others rely on cloud infrastructure outside direct bank control. What unites them is a simple truth: every new AI initiative represents not only innovation, but also a fresh attack surface.

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?

Banks face a cluster of common issues when attempting to secure AI. The first is model integrity and supply chain risk. Many AI models are obtained from vendors or open-source communities. How can they be evaluated from a security perspective?

The second is data confidentiality. AI thrives on data, but that means client records, trading flows, internal communications, and sensitive HR files. Risks include prompt injection, model inversion attacks, and accidental leakage of confidential information. Even synthetic data can raise concerns about re-identification or inadvertent bias.

A third challenge is adversarial manipulation. Unlike traditional software, AI models can be tricked through carefully crafted inputs. Fraud engines can be nudged to misclassify transactions. Trade surveillance systems can be coaxed into ignoring abusive patterns. In practice, this means adversaries can attack not just the infrastructure around the model, but the model itself.

Finally, there is the question of resilience. If an AI system goes down, critical processes can halt: surveillance alerts are missed, payments are delayed, customer interactions fail. Banks must design fallback processes and "kill-switches" that allow continuity in the event of an outage or compromise.

Perhaps the most pressing new concern is the rise of agentic AI. Unlike traditional models, which generate outputs in response to inputs, agentic AI can act. It can call APIs, execute workflows, move money, approve trades, or reconfigure systems. In other words, it is not just making predictions — it is taking actions. Today, few banks have the sandboxing, kill-switches, or human-in-the-loop safeguards required to stop rogue agents instantly.

So, what do organisations need to do to integrate AI-driven processers into existing controls and governance frameworks?

How do IAM/PAM, threat detection, operational resilience and governance frameworks need to be adapted?

How can existing security stacks be configured to cope with the threats AI can introduce and what new tools may be necessary to augment traditional security and resilience solutions?

.

Securing Financial Services

SECURING FINANCIAL SERVICES

Key Themes

Securing the AI supply chain – a new 3rd party problem

Banks are sourcing AI from a mix of in-house teams, niche vendors, and global cloud providers. Each introduces new risks: unverified training data, hidden dependencies, and opaque contractual terms. The question is not if, but how, you can trust solutions providers whose technologies you don't fully control or understand. **How to deal with this?**

Protecting critical data in the age of AI

AI needs data and lots of it, but that includes customer records, trading data, and much besides. Securing against an AI-driven data leak or misuse issue is now part of securing the database itself. Compliance with GDPR, banking secrecy, and cross-border data laws raises the stakes further. **Can you help?**

AI everywhere: mapping the new attack surface

From trading desks to HR, AI is now embedded across the bank. Fraud detection, AML, chatbots, threat hunting — each new initiative is another attack surface. Security leaders must understand not just the technology, but the organisational sprawl of AI adoption. **What are the key issues?**

Adversarial threats and AI exploits

Unlike traditional systems, AI models can be manipulated through crafted inputs. Adversarial attacks may cause fraud engines to misclassify transactions or surveillance tools to ignore abusive patterns. Understanding and testing for these new exploits is critical. **So how can traditional security tools spot this – and model drift and other threats?**

Securing agentic AI

Agentic AI can call APIs, trigger workflows, and make sequential decisions. Attackers don't need to break into a system — they just need to trick the agent into acting against its intended purpose. In critical contexts like payments or surveillance, the consequences could be immediate and severe. **So how does agentic AI impact traditional tools? What's needed now?**

Embedding AI in the security stack

AI security events should feed into the bank's SIEM, SOAR, and SOC processes like any other risk. Model drift, adversarial anomalies, and data leakage must generate alerts alongside malware or phishing attempts. Existing IAM and PAM controls must evolve to cover AI agents and models to ensure that that they can't escalate privileges or bypass controls. **Can this be done withing traditional toolsets?**

Why AKJ Associates?

SECURING FINANCIAL SERVICES

A History of Delivery

For more than 20 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 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(I)SOs, 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 and gambling and gaming.

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 20 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.**

Securing Financial Services

SECURING FINANCIAL SERVICES

Plenary Speakers

The e-Crime 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.

Your team and your resources available in real-time

SECURING FINANCIAL SERVICES

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.

Delivering the most senior cybersecurity solution buyers

SECURING FINANCIAL SERVICES

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.

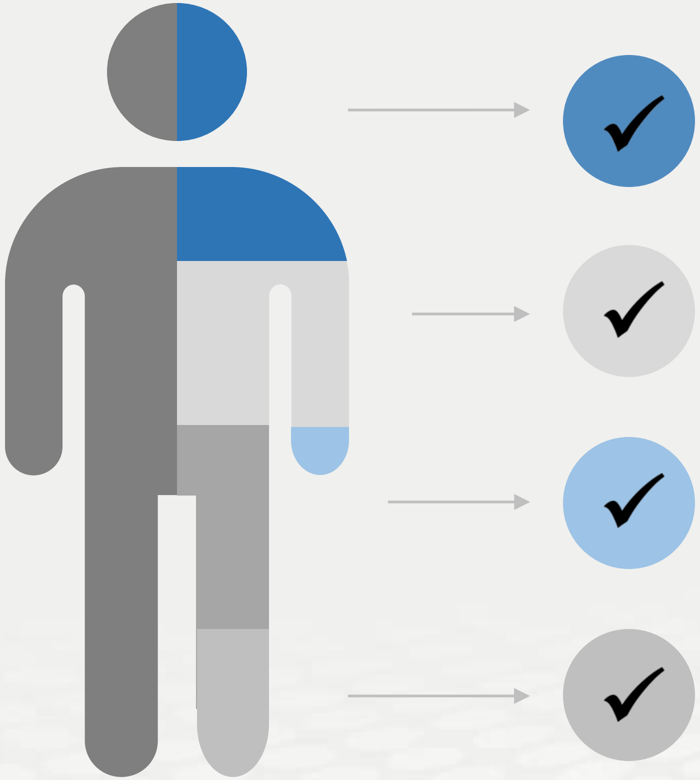
You will have access to the most senior buying audience in the cyber-security market.

AKJ Associates has been building relationships with senior information risk and security professionals for 20 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 the lead generation and always increases profitable sales activity.



Cyber-security
We have a 20-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

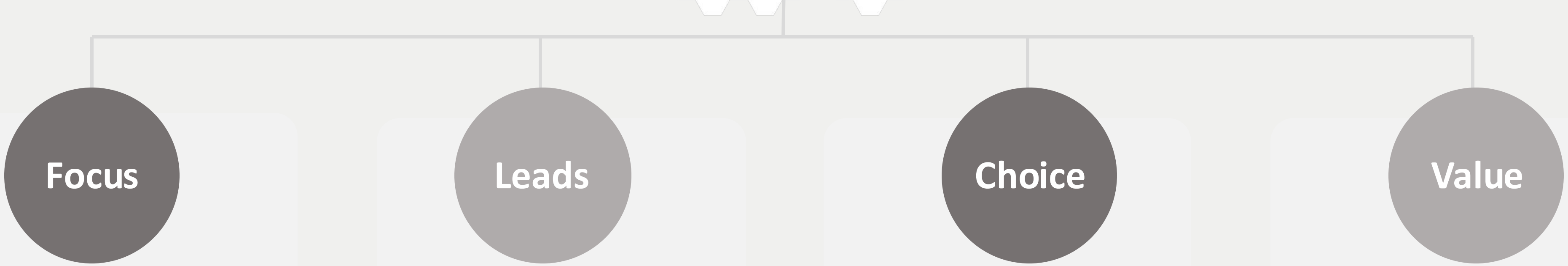
We deliver the most focused selling opportunity

SECURING FINANCIAL SERVICES

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

SECURING
FINANCIAL SERVICES

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



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.

Boost sales

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

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.

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.

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 20 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 virtual 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 20 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 20-year reputation and the e-Crime & Cybersecurity Congress brand.

Securing Financial Services

SECURING FINANCIAL SERVICES

PhishRod

It was indeed a great show. Despite the situation overall [COVID 19] the number of people that turned up, shows the trust people have of the e-Crime brand. Wish you all the best for the upcoming events and we shall surely be a part of them.

KASPERSKY lab

This is always a great event for 'taking the temperature' on security issues, to get a feel for people's impressions on current security challenges and to find out what organizations of all kinds are doing.

vmware Carbon Black

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 opportunities in the security sector, and our work with them has delivered way beyond expectations.

✓Ninety five percent of our exhibitors and sponsors work with us on multiple occasions each year

✓Our sponsor renewal rate is unrivalled in the marketplace

✓This is because our sponsors generate real business at our events every year

AKJ Associates

https://akjassociates.com/event/finserv