Securing Financial Services

8th July, 2020, London

SECURING
FINANCIAL SERVICES

Secure the industry, protect the customer

How the convergence of fraud, KYC/AML, security and privacy makes cyber a manageable operational risk

https://akjassociates.com/event/finserv

AKJ Associates

The biggest threat to financial services?

Cybersecurity is a top investment priority for financial services (FS) firms globally, with the **big banks spending up to a billion dollars** a year on the problem.

FS firms are prime targets in cyberspace for the same reason that they have always been targets – the money. Smart criminals have long since abandoned guns and dynamite as their tools of choice and now see direct cyberattacks on financial infrastructure and **digital fraud on banks' retail, high-net worth and wholesale customers** as an attractive money maker.

In addition, disabling a prominent financial organization is a **high-profile way to embarrass a government**. Disrupting the data flow between institutions can cause volatility in key markets and unsettle the public.

And a full-scale attack on, say, an ATM system could cause panic and provoke uncontrolled bank runs. So **banks are also a CNI target for both organised crime and nation-states**.

Retail banks, and also asset managers and insurance companies, with their millions of dependent customers, are under threat as digital transformation is rolled out, as mobile becomes the key customer platform, as open banking and PSD2 create new risks around new Fintech players and APIs.

As one researcher points out: "Mobile malware authors have set their sights firmly on monetization… this is no doubt a response to the explosion in **mobile banking and financial applications** that we have seen during the last couple of years."

And of course **data privacy and GDPR, and payment standards such as PCI DSS**, are critical pieces of the FS compliance jigsaw.

Wealth management firms also see cybersecurity as a material threat to their business. Client PID is an absolute priority: the damage that would be done to a private bank if the details of its ultra-high net-worth individuals were leaked would be what one private banker calls a "disaster scenario".

SECURING
FINANCIAL SERVICES

Beyond banks: asset managers, fintechs & platforms

Introduction

Wholesale and investment banks are also vulnerable. They may not fear so much the DDoS or ransomware attacks that can hit retail institutions so hard, but in payments, FX, transaction banking, trade finance and capital markets, the need for more speed, better connectivity, mobile device access, a better user experience and better analytics has led banks to kick-start the development of digital versions of their products and digital delivery mechanisms.

Clients have continued to demand bank-agnostic platforms and have themselves connected to an increasing number of **new platforms and fintechs. This new ecosystem of wholesale financial technology is another area ripe for cyberattack**.

In payments, banks are joining global automated clearing-house (ACH) platforms such as PayCommerce and Earthport (now part of VISA), as well as self-described alternative to Swift (hacked in the Bangladesh Bank episode), Ripple.

The cybersecurity problem extends **to other areas of wholesale markets**. In trade finance, banks are digitizing the physical and financial supply chains as well as the information supply chain – while various fintech platforms are solving specific problems, such as supply-chain finance, for specific types of client.

And **Central Banks, from Bangladesh to the Netherlands** are now constantly bombarded with cyber attacks, threatening the stability of the global financial system.

Beyond banking, **the asset management industry** too is wrestling with problems of data, digital transformation and cybersecurity. Building resilience is now a top priority.

Securing Financial Services will cover these and other key subjects for its audience of professionals tasked with safeguarding digital assets and sensitive data. There will be real-life case studies, strategic talks and technical break-out sessions from security teams behind some of the world's most admired brands, who know, just like you, that security is now more important to business than ever.

SECURING
FINANCIAL SERVICES

Key themes

Key Themes

Is open banking open season for cyber attackers?

The increased attack surface creates new problems for both established and challenger banks, and also new fintechs and platforms.

- Cybersecurity and PSD2
- Securing the new ecosystem of banking APIs
- Securing new fintechs / PSPs / platforms and connections to them

Integrating Fraud, KYC/AML and cybersecurity

Banks must merge Fraud's identity and transaction knowledge, with Cybersecurity's system, IT and vulnerability expertise to build a holistic defence.

- Using cybersecurity data as a leading risk indicator to discover new frauds
- Using real-time fraud monitoring data to help detect and prevent cybersecurity vulnerabilities
- Building data models that blend cybersecurity and fraud indicators to signal possible threats and fraud events

Cybersecurity as risk management in the 3LOD model

Cybersecurity is not unique, it's just another piece of the operational risk management puzzle. Banks need to build the right control environment, based on sound risk management principles organised within the 3LOD model.

- Cyberrisk versus cybersecurity: taking an operational risk management approach
- Building a cyberrisk control environment
- Cybersecurity and the 3LOD model – where does it sit and how is it audited?

Securing bank technology

A study released in 2018 by Accenture examined the security posture of 30 major banking applications. Each of them had at least one known security risk, and a quarter of them were revealed to have at least one flaw that is considered "high-risk."

- Legacy systems are a huge problem. How can they be made secure?
- Cloud solutions may help with digital transformation but what about cybersecurity?
- As banking moves onto mobile platforms, how can customer data be protected?
- Securing the blockchain solutions in payments, trade finance and elsewhere

Governance and regulation

Cybersecurity is a stakeholder issue: lenders, bondholders, equity holders, ratings agencies, insurers, regulators and staff all need to know their bank's cybersecurity status. (Oh, and the press too.)

- Cyber ESG – what to tell whom?
- Satisfying the regulators: demonstrating good risk posture
- Measuring and reporting cybersecurity; third-party ratings: ensuring your best profile

Protecting employees in financial services

Because FS firms are such attractive targets, their staff are subject to far more attacks than most. Simply calling humans the weakest link isn't good enough. So how to protect employees from becoming unwitting tools of the cybercrminals?

- Stopping malware before it gets to the desktop
- Enterprise-scale phishing and BEC protection

SECURING
FINANCIAL SERVICES

Demonstrate your solutions

Financial firms need your help …

1 To maintain cutting-edge cybersecurity

The scale of risks faced by the financial services sector means that they must ensure absolute security best practice and implement the best security solutions. **Which solutions fit the bill and can be implemented inside complex firms?**

2 To build cyber resilience

Sustainability, resilience, mitigation and incident response are as important as security itself. Given the inevitability of attack and breach, recovery from attacks and business continuity are critical. **Show how your products can help achieve this.**

3 To build cross-border compliance

Cyber-security is going mandatory. Voluntary commercial codes are not enough. Regulators want companies to demonstrate true cyber-security as well as basic compliance. **Which solutions can generate metrics or otherwise help?**

4 To secure diffuse infrastructure at scale

FS firms are large, complex and cross-border. They have huge and complex supply chains. And they face multiple compliance regimes. Securing these kinds of enterprise and those who use them requires particular skills. **Are you up to the job?**

5 To train and retain key cyber staff

Everyone needs to buy-in to cybersecurity from the top down. They need training and education. Firms also need to prove that they value cyber-security staff and give them the responsibility they need. Otherwise they leave. **Can you help?**

6 To outsource what doesn't work in-house

Even large FS firms do not want their whole security and IT infrastructures in-house. So what should they outsource and what should remain on-premise? How does outsourcing help solve the underlying risk problem? **What can you offer?**

https://akjassociates.com/event/finserv

SECURING
FINANCIAL SERVICES

They are looking for solutions around …

Demonstrate your expertise

Digital transformation

Building security into all business processes

Too many companies find themselves with a muddle of consumer-grade security solutions when what they need is a robust, enterprise-grade solution stack that is scalable and can realistically be implemented across a global business. In addition, good security hygiene – the digital equivalent of health and safety – is required holistically. Which solutions reflect this underlying truth?

Fraud

How to join up fraud, security and privacy

It is still remarkable how often fraud and cybersecurity are in disconnected silos within their organisations. And yet fraud is the crime that results from poor security, and the flagging of potential fraud before it happens is one of the best defences against, and alerts for, data loss and data privacy issues. So why the disconnect and what does a joined-up fraud/security operation look like? And what technical solutions help build one?

Behavioural analysis

A different approach to the issue of us

A system designed to pick up unusual patterns of employee activity identifies a potential terrorist. Further investigation reveals that in fact the employee was considering suicide. The system was actually designed to alert companies to cybersecurity risks through behavioural analysis. This example shows that perhaps the best way to solve the core problems in cyber is to pay more attention to the things we do when we are simply getting on with the job.

AI – the state of play

Slow train coming: the wait for intelligent cybersecurity

Automation is linear and rules-based and automated cybersecurity solutions work that way –using signatures and/or other historical data to identify issues. Despite the claims made for artificial intelligence, current machine learning solutions are not too far from that methodology. Slightly smarter statistical analysis still generates too many alerts for most human teams. Are truly intelligent solutions in the pipeline?

Where market-leading solution providers know they will find buyers

SECURING
FINANCIAL SERVICES

We deliver a focused selling opportunity

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

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.

https://akjassociates.com/event/finserv

Where the real decision-makers allocate budgets

SECURING FINANCIAL SERVICES

Why do so many blue-chip vendors work with us? Real buyers ...

100%

The most senior cyber-security solution buyers

You will be surrounded by the most senior buying audience in the cyber-security market.

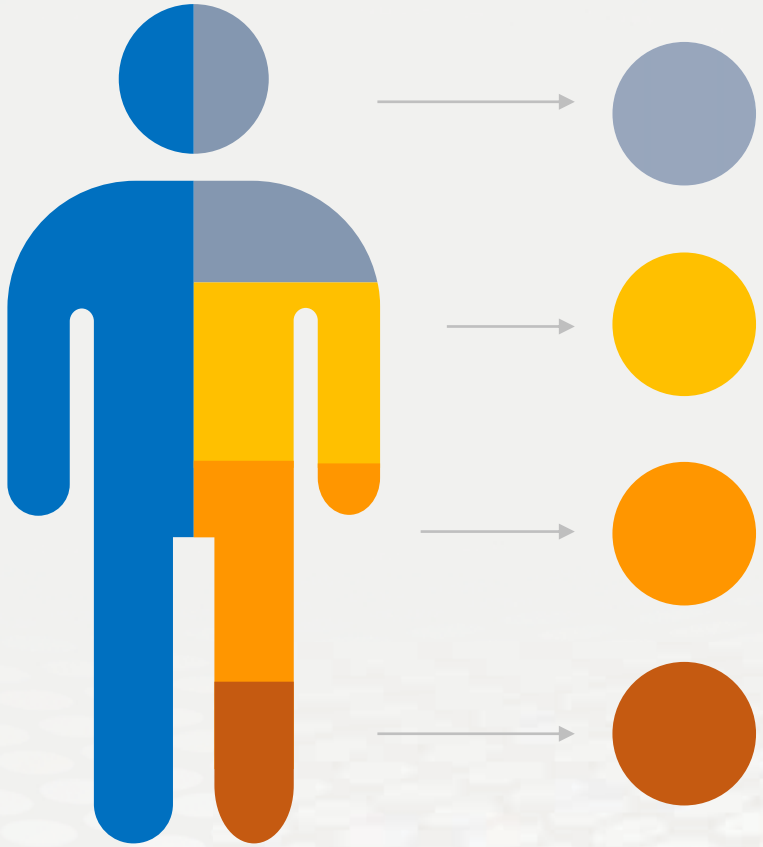
AKJ Associates has been building relationships with senior information risk and security professionals since 1999 and our cybersecurity community is the largest of its kind globally.

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 Securing Financial Services.

We understand that every vendor needs to sell more. That is the bottom line.

Getting in front of the right people at the right time always increases lead generation and always increases profitable sales activity



Cyber-security

We have been producing the events cybersecurity professionals take seriously for more than 15 years

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

https://akjassociates.com/event/finserv

Where the top solution vendors get their message across

SECURING
FINANCIAL SERVICES

Why do so many blue-chip vendors work with us?
Real benefits...

Talk to customers

Face-to-face interaction with the right buyers works! Our vendors tell us it does and they renew year after year

Build relationships

Relationships built from a personal meeting are stronger than those initiated by solely digital conversations

Save time

Meet dozens or hundreds of selected buyers in a concentrated period – the value of a high quality event

Lead sourcing

We provide the best leads in the business. Each sponsor receives a delegate list.

Increase sales

All delegates are the right delegates. They have all been researched and confirmed as senior and with buying capacity

Get your message across

Delegates take all lunches and breaks in the exhibition. So sponsors and exhibitors are always surrounded by qualified buyers

At AKJ we are always looking for ways to help our sponsors derive more value from our events. To reflect the evolution of contact channels, we are delighted to be able to confirm that we can offer lead scanners at our events. As sponsors seek to improve ROI and leverage post-event communication, we are committed to providing the latest technologies to help you drive your business forward.

https://akjassociates.com/event/finserv

Our testimonials speak for themselves: we have many more

SECURING
FINANCIAL SERVICES

What our sponsors say about us

proofpoint.

e-Crime remains a critical event for security pros. Year after year, AKJ manage to stay on top of market trends and satisfy attendees' demand for topical expertise; we are delighted to be part of the e-Crime series.

KASPERSKY lab

AKJ events have yet to disappoint – from the massive number of attendees to our packed speaking sessions, this is one event we always look forward to!

COFENSE

We found the event very productive, it was good to meet potential customers and gives a chance for decision makers to meet us and understand what we do and how we can help them with their security.

Ninety five percent of our exhibitors and sponsors work with us on a number of 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.

https://akjassociates.com/event/finserv