

e-Crime & Cybersecurity Congress Switzerland



5th Annual e-Crime & Cybersecurity Congress Switzerland

September 17th, Zurich, Switzerland

A new security operating model for a new security era

Switzerland's unique corporate and geographical role is amplifying the challenges of AI, quantum, digital sovereignty and resilience. Is it time to focus on what works – and time for the business to back off?

AKJ Associates

Time to focus on the practical

Swisscom's latest cybersecurity threat radar headlines geopolitics and AI as critical accelerants of cybercrime and says the situation is far worse than in 2025. Their view is that cybersecurity is no longer primarily an IT security problem. It is becoming a systemic business, geopolitical and operational resilience problem.

From this perspective, the Swiss threat environment has materially worsened because several forces are converging simultaneously: AI, geopolitical instability, cloud/platform dependency, software supply-chain fragility and IT/OT convergence

And these trends amplify one another rather than existing independently.

It certainly seems, from talking to security leaders, that organisations are under pressure to deploy AI tools far faster than security teams are comfortable with. Software suppliers are incorporating AI into their products faster than CISOs can evaluate the impact.

But that is far from the only near impossible challenge on Swiss security teams. How about digital dependency? Organisations face Cloud concentration risk, dependence on US hyperscalers, dependence on foreign security vendors, issues of data sovereignty, concentration risk in identity providers...the list goes on.

If organisations must now think strategically about who controls their infrastructure, which jurisdictions suppliers fall under and where dependencies create hidden exposure then security just became a much bigger problem.

So firms need to accelerate their current BAU security programmes whilst adding additional AI- and other risk-related initiatives:

- **Replace network-centric security with identity security because the former failed:** identity lifecycle management & privileged-access hardening; unifying IAM, PAM, CIEM, and SSO into a coherent identity fabric; conditional access with continuous risk scoring; identity threat detection (ITDR); MFA hardening + phishing-resistant methods (FIDO2, passkeys).
- **Replace prevention with resilience because prevention doesn't work and doesn't scale:** so go 'unglamorous' – focus on the practical and operational: immutable backup architecture, isolated recovery environments, recovery testing, segmentation of critical functions, blast-radius reduction.
- **Reduce complexity:** attack tool sprawl, privilege sprawl, architecture sprawl.
- **Modernise detection and response modernisation:** XDR + AI-augmented SOC; automated incident response and playbooks; adversary-simulation tooling to tune detections.
- **Third-party and SaaS risk:** Continuous external attack-surface monitoring of vendors; Automated evidence collection & assurance workflows; contract-level visibility of data access, and attack/threat data.
- **Data security and data governance** (especially in AI-driven environments): data discovery; DSPM (Data Security Posture Management); guardrails for LLM/AI usage: data leakage prevention, policy enforcement.

The e-Crime & Cybersecurity Congress Switzerland will look at how at how security teams and the business must respond to a new era in cybersecurity. Join our real-life case studies and in-depth technical sessions from the most sophisticated teams in the market.

Key Themes: AI and Quantum

Identity, authority, and control for non-human actors

CISOs must rethink core identity and governance frameworks, including the adoption of robust agent identity models (spanning machine, service, and workload identities), and clearly defined delegation structures that determine what authority an agent holds and who grants it. **What technologies can help them maintain visibility and control?**

Data protection and leakage risks

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?**

AI anti-phishing and social engineering defences

AI is shifting defence from static filtering to behavioural detection at scale, flagging anomalies that rules / signatures miss. It can also enable pre-emptive defence against social engineering, identifying manipulation cues. The result is a move from reactive blocking to adaptive defence reducing both successful attacks and analyst workload. **Can you help?**

Who needs to be quantum-ready?

Anyone responsible for long-lived sensitive data or critical infrastructure has a quantum problem. That means banks, governments, telecoms, energy, healthcare whose datasets need to last decades. If your encryption protects value over time, you need crypto-agility and a migration path now, not when quantum arrives. **How does this work in the real world?**

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?**

Intelligent Threat Detection

CISOs now must build a single coherent security program that simultaneously satisfies divergent regulatory demands; they must interpret vague legal standards into technical architectures, and they risk non-compliance if auditors, regulators, or courts interpret differently later; they face unrealistic expectations around incident reporting; and they face personal liability. **Can RegTech help?**

Key Themes: Building Better Security

Making the best use of threat intelligence

In a preemptive security model, timing is everything — success depends on detecting and neutralizing threats before they become active incidents. To do this, security operations can't just rely on internal telemetry (e.g., endpoint or network logs). They need external, real-time context about emerging threats — **where do they get it?**

Security Posture Management

Traditional vulnerability scanners don't handle cloud native architectures well. Today's cloud environments spin up thousands of ephemeral assets without a traditional OS, without an IP address for long. **So how do you adapt to that dynamic, API-driven reality? How can traditional tools connect the dots — not just generate tickets?**

Improving continuous attack surface discovery

You need to know what attackers can see and what they can actually attack — and you need it on a continuous basis, not in some static inventory. Ideally you also need assets ranked by risk priority and put into the current threat and vulnerability context. **Is this feasible and is it cost effective?**

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?**

Adversary simulation and behavioural analysis

Automated adversary simulation Identifies telemetry blind spots. They provide prioritized remediation guidance and control effectiveness metrics. They track progress trends and validate security ROIs as well as providing board and audit reporting. **How well do they work in practice?**

Securing the Cloud: still a problem

The Cloud may be secure but misconfiguration, API proliferation, federated identity challenges, third-party compromise and a misplaced trust in shared responsibility all make Cloud environments extremely complex to understand and secure. **So is the answer CSPM/CIEM tooling? What about CNAPP/CWPP? How to push your controls into SaaS providers and MSSPs? Can vendors help?**

Key Themes: Best Practice Fundamentals

Achieving visibility across ecosystems

From exposed initial access points such as warehouse management systems to complex machine control software, simply understanding your device and application landscape is a huge challenge. Can you help with asset tracking and endpoint visibility? And what about anomaly detection after that?

Transitioning OT to the Cloud?

OT traditionally was localized in particular sites and air-gapped from IT systems. But connectivity with broader corporate networks and the need to manage technology more centrally (especially during COVID) has seen companies looking at managed services in the Cloud for OT. **Is this a way forward? Or does the Cloud just create more problems?**

Defending against the latest ransomware variants

Ransomware evolution is forcing the hands of government and causing havoc in the insurance market. So firms must go back to basics (see below) but also invest in immutable back-ups and real resilience. Detecting early-stage infiltration is also critical. **What else can CISOs do to better defend against ransomware?**

Securing the basics

The endpoint and email are still a critical cybersecurity battleground. So, organisations still need EDR/XDR everywhere; they need advanced email security; they need more aggressive patching of internet-facing anything. They need to move from awareness training to behavioural conditioning. **What does that mean practically for CISOs?**

Why zero trust, isolation and segmentation are key

There has been a shift in recent attacks away from the theft of data – now threat actors are concerned with interrupting all operation activity. It is now critical that business functions are separated, and that internet access to OT networks is limited. **Can security teams still keep up with sophisticated foes? Should they upgrade their capabilities?**

Dealing with regulations

CISOs now must simultaneously satisfy divergent regulatory demands; they must interpret often vague legal standards into technical architectures, and they risk non-compliance if auditors, regulators, or courts interpret those regulations differently later; they face unrealistic expectations around incident reporting; and they face personal liability. **Can RegTech help?**

Why AKJ Associates?



A History of Delivery

For more than 25 years, AKJ Associates has been running 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(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, 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**.

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.



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.



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.



Cyber-security

We have a 25-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

Delivering the most focused selling opportunity



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.

What our sponsors say about us



"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