e-Crime & Cybersecurity Congress Germany

28th Annual e-Crime & Cybersecurity Congress GERMANY

January 21st, 2027, Frankfurt, Germany

Compliant on paper, exposed in practice?

Germany's industrial core is engineered for efficiency and regulated harder than ever. But is it secure, or just rarely breached? And does AI change the answer?

AKJ Associates

http://akjassociates.com/event/germany

e-Crime & Cybersecurity Congress Germany

Regulated, integrated — and exposed?

Germany's strengths are also its fault lines: deep integration between IT and OT, long supplier chains, an engineering culture that prizes stability over change, and a skills shortage that leaves security teams thin.

These teams are not only wrestling with security. They have a compliance problem too. The regulatory picture has changed more in twelve months than in the previous decade.

The NIS2 Implementation Act took effect in December 2025 with no transition period, taking the organisations supervised by the BSI from around 4,500 to almost 30,000 and making management personally accountable.

DORA governs finance and The EU Cyber Resilience Act's main obligations apply from 11 December 2027, making product security, vulnerability handling and supplier assurance immediate considerations for technology investment and procurement.

Yet when the registration window closed in March, only about four in ten in-scope organisations had registered and the BSI had to set a second deadline. The long tail of the Mittelstand — the family-owned exporters that hold much of Germany's most valuable intellectual property — was not ready.

Meanwhile the threat has become explicitly geopolitical. German industry, infrastructure and public bodies sit at the intersection of state-directed espionage and sabotage, criminal ransomware and hacktivism, at a moment when Europe is rearming and rail, energy, ports and defence supply chains are strategic targets.

This is the tipping point: cyber risk is moving from whether individual companies can prevent attacks to whether Europe's industrial core can sustain trust and operations under permanent pressure.

AI sharpens that challenge. Defenders must modernise detection, response and prioritisation just to keep pace — while securing their own use of AI agents.

Regulation adds urgency, but compliance is not resilience. NIS2 and DORA are a floor, not a strategy, and digital sovereignty — who runs the cloud, where the data sits, which suppliers can be trusted — is now a board-level security question rather than a procurement preference.

German firms may be well positioned by European standards, yet the strategic question is no longer whether they are "more mature than peers". It is whether their operating models are fit for the next phase of cyber risk.

CISOs therefore face an external challenge (a state-grade threatscape) and an internal problem: how to argue for preventive resourcing in a cost-conscious economy before attackers prove how damaging a breach can be.

Cyber incidents ranked as Germany's leading business risk in the **Allianz Risk Barometer 2026**, reflecting the close connection between digital security, operational continuity and corporate reputation.

So, where do German cyber leaders see genuine resilience, where is compliance masking hidden exposure, and what should organisations do before the storm becomes visible? If Germany is Europe's industrial core, is it also becoming one of its most exposed?

The e-Crime & Cybersecurity Congress Germany 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.

e-Crime & Cybersecurity Congress Germany

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?**

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?**

AI social engineering: the language barrier is gone

Flawless German phishing, cloned executive voices and "fake president" fraud are now cheap and scalable. Defence is shifting from static filtering to behavioural detection at scale, spotting manipulation cues and anomalies that rules miss, and from awareness training to real-time intervention. **Do you have solutions?**

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?**

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?**

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?**

AKJ Associates

e-Crime & Cybersecurity Congress Germany

Key Themes: Building Better Security

NIS2 in practice: from registration to resilience

Almost 30,000 German organisations are now supervised by the BSI, with personal liability for management, 24-hour reporting and evidence obligations to come. Registration was the easy part. **How do CISOs turn a compliance programme into measurable resilience — and prove it to auditors and the board?**

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 Cyber Resilience Act: security by design for producers

Germany makes the machines, components and connected products the CRA regulates. Reporting duties are here; full obligations follow. Manufacturers need vulnerability handling across product lifetimes measured in decades. **How do engineering-led companies get there?**

Ransomware and the Mittelstand

Extortion groups target the hidden champions precisely because they are rich in intellectual property and thin in security staff. Firms must go back to basics but also invest in immutable backups, tested recovery and early-stage infiltration detection. **What else can CISOs do to better defend against ransomware?**

Automation, MDR and the skills gap

The Fachkräftemangel means most German security teams cannot scale headcount. SOAR, AI-assisted triage and managed detection promise to pull data across SIEMs, EDRs, cloud APIs and ticketing systems and coordinate response through playbooks. Well, that's the theory. **How does it work in the real world?**

Digital sovereignty: cloud, data, control

Who runs the cloud, where data sits and which suppliers can be trusted have become board-level security questions. This is especially true around AI. EU providers, hyperscaler enclaves and an on-premise revival all compete for the same workloads. **But what does sovereignty mean in practice, and what does it cost in security terms?**

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(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.**

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.

Your team and your resources available in real time

e-Crime & cybersecurity GERMANY

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 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.

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

AKJ Associates

http://akjassociates.com/event/germany

Delivering 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.

e-Crime & Cybersecurity Congress Germany

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

e-Crime & cybersecurity GERMANY

OneSpan

"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

Recorded Future®

"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

Red Helix

"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

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 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