From Security to Resilience – Rethinking the Impossible

24th e-Crime & Cybersecurity Congress

March 11th & 12th 2026, London

100% security is impossible. So, security alone doesn't keep organisations running, security+resilience does. Recognising this requires a fundamental shift at every organisation – in people, process, and technology

Secure everything? Or survive anything?

"Cybercriminals pose a seismic and increasingly sophisticated threat to businesses and national security. Yet Britain seems remarkably ill-prepared," The Guardian October 2025

Cybersecurity professionals may take issue with the last words, but they surely understand that that's what it looks like to politicians, shareholders, customers and the public in general. 'What are ministers going to do about this?' is an increasingly common question in the press. All of which means that at last the true significance of cybersecurity is being realised. Finally, then, will organisations spend the right money on the right things?

Preventing a Digital Breakdown

Airports grounded. Automakers stalled. Retailers offline. Breweries silenced. The economy runs on tech no one can fully secure. Technology implementation has been so fast and fragmented that organisations no longer understand what they have or who/what they depend on. Security has never been more important.

The Accountability Reckoning

Boards no longer accept 'too hard to quantify.' CISOs must speak the language of risk — or be replaced. If we can model credit default and hurricane exposure, and allocate capital against it, why pretend cyber risk is immeasurable? Security is operational risk. It should be measured and managed as such.

Regulators Have Already Decided

Their question isn't if you'll be breached. It's how fast you recover. DORA, NIS2, the UK Resilience Framework and the rest are much less interested in your security stack and much more interested in how you've identified critical dependencies, business services and processes and how you can keep them running.

From Defence to Design for Failure

If security can't guarantee safety, resilience must become the organising principle. A truly resilient enterprise could survive without security. Security becomes an efficiency function — not a guarantee.

The ROI Reset

CISOs started off talking about data crown jewels and GDPR – but data losses are not existential, it's data encryption and attacks on IoT systems that are. So, is uptime the only relevant metric?

Enabling continuity

Defence tools must prove they enable continuity. Cybersecurity done well should be seen as foundational to resilience. The key is to be able to link specific security goals to business risks.

Next generation tools and models: the rise of AI

Resilience and security need many of the same things: visibility across technology and processes; accurate inventory mapping; data integrity and availability; risk-based prioritization. So how will AI help with these?

The future of the cybersecurity stack

The stack of the future is a resilience architecture: dynamic, AI-assisted, and impact-aware. Its goal is not to prevent every breach, but to ensure that when compromise happens, the organisation stays in business.

CISO or Cyber Resilience Chief – A New Power Base?

Resilience is the new seat at the table. If resilience not security is the endgame, what does that mean for hierarchies, budgets and responsibilities? Will The next generation of CISOs defend walls or rebuild faster?

How vendors can respond to the new resilience paradigm

Turning security into resilience – re-thinking your security toolset

Defence tools must prove they enable risk measurement and management, as well as continuity.

Detection as Resilience
Speed is resilience. The vendors who thrive will be those who turn detection and response into minutes, not days. It's no longer about catching every attacker — it's about shortening dwell time, preserving core processes, and containing the blast radius before business impact sets in.

Incident Response Becomes Recovery Engineering
New generation incident response it starts when operations must be restored. The leading IR providers are expanding into "recovery engineering" — building predefined restoration playbooks, secure failover architectures, and post-incident dependency analytics that prove to boards and regulators that recovery times are predictable and tested.

Resilience is a Data Problem
You can't recover what you don't understand. The best cybersecurity tools are now the ones that see across dependencies — mapping which processes, identities, and suppliers matter most. Visibility isn't just security analytics anymore; it's the foundation of adaptive recovery.

Zero Trust Re-Defined as Graceful Degradation
Zero Trust has been sold as "trust nothing." The resilience version is "trust what's left." The most forward-looking vendors are designing architectures where services degrade gracefully rather than fail catastrophically — so the business can operate in a partial trust mode while recovering full capacity. An impractical utopia becomes realizable.

Vulnerability Management vs Exposure Prioritisation
Scanning every CVE means nothing without knowing which asset underpins which process. Resilience-aligned vulnerability vendors will fuse exposure data with business criticality scoring — helping risk leaders prove that the systems most vital to operations are also the most defended.

From Endpoint Protection to Endpoint Continuity
Endpoints aren't just entry points; they're business enablers. In a resilience model, the endpoint provider that wins is the one that helps the organisation keep working even when devices are compromised. Automated isolation, local restore capabilities, and identity-based reauthentication make endpoint agents part of the continuity fabric, not just the perimeter.

"The fusion of security and resilience will demand new architectures, new mindsets, and perhaps new leadership titles — but also more investment. Organisations can no longer just talk the talk."

AKJ Associates

How vendors can respond to the new resilience paradigm

Turning security into resilience – re-thinking your security toolset

Defence tools must prove they enable risk measurement and management, as well as continuity.

Threat Intelligence is Business Impact Intelligence
Threat data has become abundant; what's scarce is relevance. The next generation of threat-intel vendors map adversary campaigns to the organisation's critical process dependencies — turning technical IOCs into operational risk insights. The winners are those who can brief not just SOC analysts, but resilience committees and risk officers in business-impact language.

Threat Hunting For Continuous Assurance
The best hunters are becoming *resilience auditors*. Instead of chasing every trace of intrusion, they prioritise hunts by business criticality — proving that vital functions remain uncompromised. Continuous threat hunting becomes a living control assurance mechanism: a test of whether resilience assumptions hold in practice.

From I(D)AM to Identity Resilience
Identity systems are now single points of systemic failure. IAM vendors must pivot from "locking down" to "failing safe" — ensuring that recovery identity stores, delegated trust models, and just-in-time credentials can keep essential services running when the primary directory collapses. The new IAM pitch: you can still operate when your IdP goes dark.

Cloud Security is Cloud Recovery Architecture
Cloud controls can't just prevent misconfiguration — they must guarantee recoverability. Cloud-security vendors that integrate configuration management, snapshot integrity checks, and cross-region failover orchestration are no longer security add-ons; they are resilience engines that assure continuity in hybrid and multi-cloud ecosystems.

Network Security Means Dependency Mapping
Firewalls and segmentation are necessary but insufficient. The real value for network vendors now lies in visibility of interdependence — knowing which flows matter most for critical processes. By mapping and tagging business-critical pathways, network vendors can position themselves as resilience cartographers, not just traffic police.

SIEM & XDR Are Situational Awareness Platforms
In a resilience-driven enterprise, telemetry is only useful if it supports real-time decision-making under duress. SIEM and XDR vendors can position themselves as command-centre backbones, feeding incident command, risk, and business continuity teams with shared situational awareness — not just an undigestible tsunami of alerts.

"The good news for vendors is that organisations are being reminded daily that their operations can be taken offline for weeks, even months, by a straightforward ransomware attack. They need to invest now."

AKJ Associates

How vendors can respond to the new resilience paradigm

Security and Resilience through AI (while Securing AI…)

AI in cybersecurity is well-funded but poorly explained. How does it work, what will it deliver and is it secure?

From Static Rules to Self-Learning Defences
Traditional SIEM, EDR, and XDR platforms are evolving from rule-based systems into self-learning ecosystems. Advanced ML models and transformer-based architectures allow systems to identify novel attack patterns without prior signatures. However, these models can be poisoned by adversarial data or manipulated through prompt injection and model inversion — creating new surfaces of compromise.

Threat Intelligence and Adversary Simulation
Generative AI is transforming how analysts synthesize and communicate intelligence. LLMs can draft attacker playbooks, simulate phishing lures, and summarize multi-source threat feeds, dramatically reducing the time between detection and action. But the same capability can be exploited by attackers at scale — forcing defenders to authenticate not just identities, but language patterns and context.

Predict, Prioritise, Patch
By integrating NLP and predictive analytics, AI can mine vulnerability databases, code repositories, and telemetry to predict which CVEs are most likely to be exploited in a given environment. This enables CISOs to move from reactive patching to pre-emptive mitigation. But attackers can use similar models to target unpatched systems faster than ever, creating an AI-accelerated race between discovery and exploitation.

Always-On Defence, Continuous Response
Agentic AI architectures — where semi-autonomous software entities patrol networks, triage incidents, and even patch systems — promise 24/7 protection without human fatigue. These agents can coordinate across silos (endpoint, cloud, identity) to contain threats in seconds. Yet the delegation of operational authority raises governance questions: how do CISOs ensure explainability, ethical boundaries, and control if an agent acts on incomplete or corrupted data?

Data Correlation and Anomaly Detection
AI's ability to unify disparate telemetry — from IoT sensors to SaaS APIs to industrial controllers — gives security teams unprecedented visibility across the enterprise. Cross-domain embeddings and graph AI reveal hidden dependencies and behaviours that human analysts would miss. Yet increased reliance on centralized AI pipelines introduces systemic risk: if data integrity or model logic is compromised, every downstream decision may be corrupted.

Model Integrity, Governance, and Supply-Chain Risk As organizations embed AI into every layer of their stack, "AI security" becomes a new domain of cybersecurity. Models must be version-controlled, auditable, and protected from theft, inversion, or malicious fine-tuning. Governance frameworks must extend beyond data privacy to include model provenance and policy enforcement. CISOs now need to protect not just networks and data — but the AI decision systems that will increasingly run both.

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 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 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 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

http://akjassociates.com/event/congress

Your team and your resources available 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.

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.

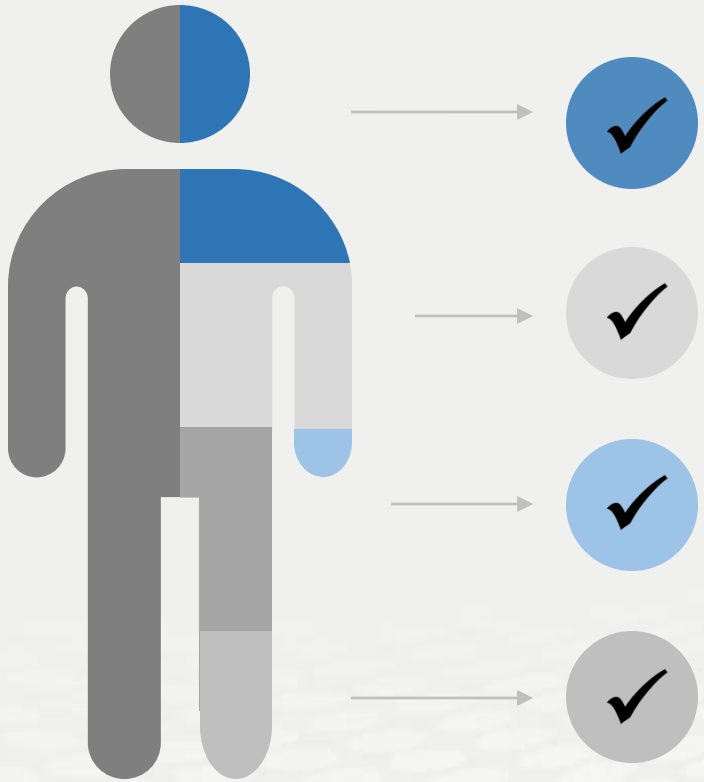
You will have access to the most senior buying audience in the cyber-security market.

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 the lead generation and always increases profitable sales activity.



Cybersecurity
We have a 25-year track record of producing the events cyber-security professionals take seriously

Risk Management & Resilience
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

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.

Results

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

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 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 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

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, **Red Helix Ltd**

proofpoint.

e-Crime remains a critical event for security professionals. Year after year, AKJ have managed to stay on top of market trends and deliver on the demand for topical expertise from its attendees and we are delighted to be part of the e-Crime series.
VP, Products, Proofpoint

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 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