



e-Crime & Cybersecurity **Retail Summit**

June 19th, 2025, **Online**

It's a steal: are hackers getting the better of the retail industry?

With complicated supply chains, third-party dependencies and digital sales channels, retailers need to spend more on security.

AKJ Associates

Cyberattacks on retail: A global threat that can't be ignored

The Blue Yonder attack is a case study in retail cybersecurity: The Arizona-based company, owned by Panasonic, **provides systems for fulfilment, delivery and returns for more than 3,000 major companies across 76 countries and was hit in November 2024**. It was also named as a victim of a separate attack via a zero-day vulnerability in a file-sharing program sold by Cleo.

The attack demonstrates the **dangers of ransomware, of advanced zero-day attacks, and of the complexity of third-party attacks: Morrisons and Sainsbury's**, two of Britain's largest supermarket groups, as well as many others globally, were affected by a third-party supplier of business-critical software. In turn, that supplier was also hit by an attack executed on a piece of its own third-party software.

So, it's **no surprise that cyber and data risks are what retailers are most concerned about** in the next 12 months, according to research by Barclays Corporate Banking and Retail Economics. Of the UK retailers surveyed, 34% said they see **cyber and data threats as the biggest risks**, with **70% saying they are one of their "top three risks"** over the next year.

However, many also view this as something they can feel confident about managing due to investment in technology to safeguard operations. Of those surveyed, **81% of retailers said the business is where it needs to be or ahead of the competition in terms of cybersecurity** issues such as ransomware, malware attacks, network security or fraudulent attacks.

Blue Yonder and other attacks like it show that **this complacency is misplaced**. And to prove it, another 2024 report revealed that 45% of retail businesses were hit by a ransomware attack last year, with more than half of those attacks succeeding in encrypting their data.

It's not just the big firms who get attacked either. Nearly half of all cyberattacks target businesses with 1,000 employees or less. Even physically small retail operations can have sizeable transaction flows and be attractive targets for hackers.

So, what should retailers be doing to heighten their security? Which technologies are best tailored to their particular needs? And can AI help in the fight against retail cybercrime?

This event will focus on multiple challenges including:

- **Implementing best-in-class endpoint device management**
- **Improve general technical controls including encryption, authentication, and authorization**
- **Third-party security and interoperability with other parts of the retail ecosystem**
- **Better risk assessment and business continuity plans**
- **Develop more coordinated incident response**
- **Secure a complex and rapidly evolving IT/OT environment**

The e-Crime & Cybersecurity Retail Summit will take place online and will look at how cybersecurity teams are tackling this new world. Join our real-life case studies and in-depth technical sessions from the security and privacy teams at a range of different providers and suppliers.

Key Themes

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, its connection and data flows and dependencies 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?**

Defending against the latest ransomware variants

Ransomware is effective precisely because it can exploit whatever weaknesses exist in your security architecture and processes. The threat and the actors are constantly evolving and that evolution is forcing the hands of government and causing havoc in the insurance market. **What can CISOs do to better defend against ransomware?**

OT and the regulations

DORA, NIS2 and other regulations put more responsibility for resilience on firms deemed important or critical. Many have focused on IT networks but the regulations include all resilience and so OT environments matter. **What does this new emphasis from regulators mean practically for OT security?**

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 keep up with sophisticated foes?**

Pen testing for OT / SCADA

Testing is key to identifying and fixing vulnerabilities before they're exploited. Regulations like NERC CIP require utilities to assess and mitigate risk. Testing checks OT security controls are functioning properly shows regulators an organization's commitment to security. **Can you help?**

Why AKJ Associates?



A History of Delivery

For more than 20 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 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.**

The challenge: end-user needs are rising, solution providers' too

Our end-user community of senior cybersecurity professionals is telling us that they face a host of new threats in the post-pandemic environment, to add to their existing challenges.

Remote working and an increased reliance on Cloud and SaaS products are all putting organisations across the world under even more strain. **They need cybersecurity products and services that can solve these issues.**

In addition, the post-COVID environment has created groups of cybersecurity professionals who are less willing or able to attend physical events, and yet these groups still demand the latest information on security technology and techniques.

At the time solution providers are finding it ever more difficult to build relationships in an increasingly competitive environment.

Economic and business drivers are making CISOs more selective and pushing them away from large security stacks and multiple point solutions.

To sell to this increasingly sophisticated community, vendors need multiple access points to engage security professionals, to build deeper relationships and maintain those relationships throughout the year.

To cater to all of the different sectors of the market, this means an increasingly varied palette of communications.

Therefore, **in response to many requests from our community** for us to continue to deliver best practice advice and to give them the up-to-date technical case studies and content they need to cope in the current environment, **we are adding to our traditional physical services.**

The e-Crime & Cybersecurity Congress Virtual Series will offer virtual versions of our key upcoming events and will deliver great **opportunities for lead generation and market engagement.**

Maintaining the ethos and quality of our physical events we will continue to offer **unrivalled partnership opportunities to cybersecurity vendors** looking to build strong, engaged relationships with high-level cybersecurity professionals.

Delegate Acquisition

- The e-Crime & Cybersecurity Congress has the **largest community of genuine cybersecurity stakeholders** to invite to our events.
- 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** will be the case for our online offering.
- **Each of our vendor partners will receive a delegate list at the end of 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 online plenary theatre: good content drives leads and engagement post event, as you showcase your company's expertise
- AKJ's in-house content / research team will complement the agenda with best practice from senior security professionals from the end-user community

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 online events keep the same ethos, limiting vendor numbers. We will keep our **online congresses exclusive and give you the best networking opportunities.**
- 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.

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.

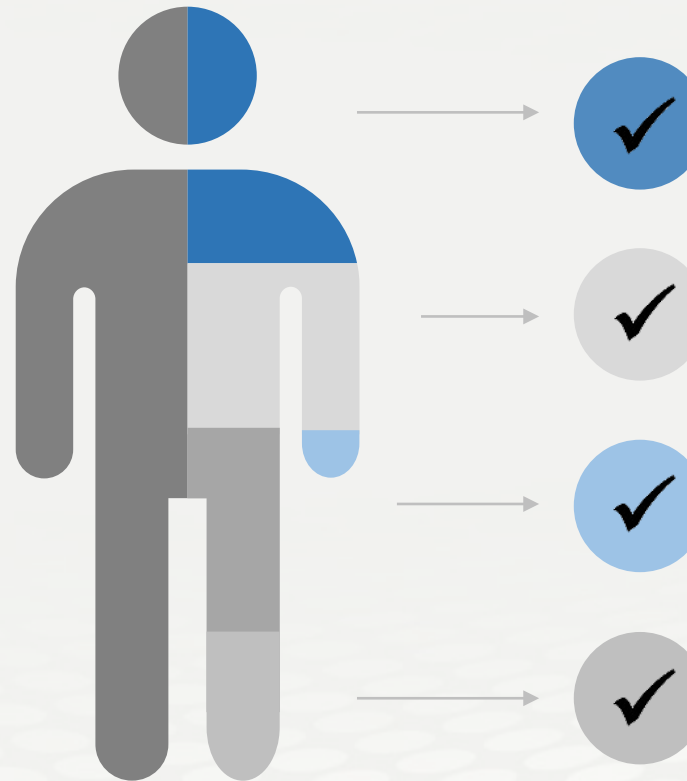
You will have access to the most senior buying audience in the cyber-security market.

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 an almost 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



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

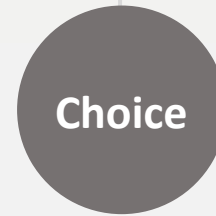
Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.



Leads

Boost sales

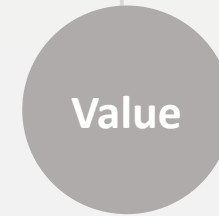
Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.



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.

What our sponsors say about us



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.



The level of engagement yesterday [at the Virtual Securing Financial Services Congress] was outstanding and we have already managed to book 2 meetings as a result, live on the day.



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