e-Crime & Cybersecurity Congress Online Series: Manufacturing

e-Crime & Cybersecurity Manufacturing Online

19th November 2026, Online

Manufacturing: cybersecurity's biggest unfinished job?

Manufacturing's exposure is structural, and it is getting worse as factories digitize. What are the economically viable solutions?

AKJ Associates

https://akjassociates.com/event/manufacturing

e-Crime & Cybersecurity Congress Online Series: Manufacturing

SECURING MANUFACTURING

Industry needs industrial-strength security

For the fourth consecutive year, manufacturing is the most attacked sector globally, responsible for around one In four of all recorded cyber Incidents Ransomware attacks against manufacturers surged by more than 60% in 2025 alone and things are arguab y getting worse. The last twelve months have supp ed the most damaging run of manufactur ng cyber incidents on record .

JLR's recovery from possib y the most damaging cyber inc dent in UK h story was still running well into this year. Then, in March 2026, the threat escalated in kind, not just degree. Stryker, one of the world's largest medical device manufacturers, was hit by a destructive wiper attack. More than 200,000 devices were destroyed across multiple continents, global manufacturing was halted, and hospitals cancelled surgeries. There was no ransom demand and no path to negotiation — the objective was destruction.

Weeks later, in May 2026, West Pharmaceutical was forced to take systems offline worldwide following a ransomware intrusion, while Foxconn confirmed an attack on its North American factories in which the N trogen group claimed to have stolen eight terabytes of data — reportedly including hardware schematics and network topologies belonging to its largest customers.

Four incidents, four different adversaries, four dif erent motives — extortion, geopolitics, data thef , supply-chain leverage. **One common victim profile: the modern connected manufacturer.**

And yet the sector's defences remain, by common consent of analysts, insurers and the manufacturers themselves, well behind those of best practice sectors such as banking.

So what do CISOs in this critical sector need to do:

Foundational — fix the unlocked doors first

- Build a complete O T asset inventory. You cannot defend what you cannot enumerate. Replace 'institutional' knowledge and spreadsheets with automated, OT-safe discovery of every controller, HMI and engineering workstation on the plant network — the prerequisite for every control that follows.
- Get identity right, everywhere. With roughly a quarter of sector losses traced to misconfigured MFA and nearly another tenth to its absence, hardening multi-factor authentication — including in shared-worksstation, shop-floor environments — is the single highes:-return investment available.
- Eliminate default and shared credentials. Factory passwords still live on controllers years after installation, and generic vendor accounts erase all accountability. Enforce unique, managed credentials across the OT estate as a matter of basic hygiene.

Structural — close the seams attackers actually use

- Replace standing vendor access with governed remote access. Trust-based, always-on V?N tunnels for equipment vendors are now a primary ransomware entry point. Move to role-based, time-limited, monitored sessions with full recording and privilege management — remembering that 65% of industrial sites still show insecure remote access conditions.
- Segment the network — properly. A phished office laptop should never sit on the same flat network as a safety-critical PLC. Implement zoning and conduits to ISA/IEC 62443, progressing toward zero-trust architectures adapted for deterministic industrial protocols.
- Contain what you cannot patch. Windows XP and 7 remain commonplace on production floors and can't run modern endpoint protection. Apply compensating controls — virtual patching, isolation, strict access mediation — around legacy systems, knowing breaches involving them take roughly half as long again to identify and contain.

Operational resilience — assume compromise, engineer for recovery

- Deploy OT-native threat detection and response. IT tooling is blind to attacks that manipulate legitimate industrial commands. Baseline normal process behaviour across indus:rial protocols and detect the subtle deviations — a changed setpoint, an anomalous command sequence — before physical consequences occur.
- Engineer recovery for wiper-class attacks. Immutable backups must extend beyond corporate data to PLC logic, robot configurations and historian data, with tested restoration measured in hours rather than weeks. JLR's £1.9 billion loss is the benchmark for what unpreparedness now costs.

Strategic — secure the extended and intelligent enterprise

- Extend assurance beyond the factory gate. With supply-chain-focused attacks doubling in 2025 and adversaries specialising in compromised third-party credentials, continuously monitor supplier security posture and treat every external connection as a potential breach path — JLR's loss began in someone else's software.
- Convert compliance into competitive advantage. Regulators, insurers and defence customers are making cyber maturity a condition of doing business through regimes such as NIS2 and CMMC. Build a continuously evidenced security programme rather than an annual audit scramble.
- Secure the smart factory by design. IT/OT convergence, cloud analytics on machine data and IIoT sensors are expanding the attack surface faster than teams can respond. Embed security into industry 4.0 architectures from the design stage, protecting data flows from sensor to cloud.

The e-Crime & Cybersecurity Manufacturing Summit will take place online and will look at how cybersecurity teams are tackling the latest challenges. Join our real-life case studies and in-depth technical sessions and help make manufacturing secure.

https://akjassociates.com/event/manufacturing

AKJ Associates

e-Crime & Cybersecurity Congress Online Series: Manufacturing

SECURING MANUFACTURING

Key Themes

Achieving visibility across OT/IT hybrid networks

Manufacturers struggle to maintain a unified, real-time view of assets spanning OT environments and IT infrastructure. Blind spots create exploitable gaps, while siloed monitoring tools generate fragmented intelligence. **Can vendors deliver a single pane of glass that discovers and monitors every connected asset without disrupting production?**

Held to ransom: is there a better way to build protection?

Ransomware groups target manufacturers, knowing that every hour of downtime costs millions. Traditional endpoint protection often can't run on industrial systems. **Are there detection, containment and recovery capabilities designed specifically for production environments, where restoring operations quickly matters as much as stopping the initial attack?**

Zero trust for the industrial environment

Zero trust principles were designed for IT, yet flat OT networks with implicit trust remain the norm on the plant floor. Retrofitting identity-based controls onto deterministic industrial protocols is complex and risky. **What's the roadmap for applying zero trust to OT without breaking production processes?**

Patching the patchwork

Production lines depend on decades-old PLCs, HMIs and control systems running unsupported operating systems that cannot be patched or taken offline. These assets represent the soft underbelly of the plant floor. **How can you provide compensating controls that protect unpatchable equipment without compromising uptime or safety?**

Securing Agentic AI

Agentic systems don't just generate content — they act. CISOs must address model manipulation, prompt injection, data poisoning, tool-chain abuse and privilege escalation within AI agents executing transactions. Governance must extend beyond ML pipelines into runtime controls, behavioural monitoring and kill-switch design

Securing critical remote access

Remote maintenance access has become essential, yet VPNs, jump servers and vendor-supplied remote tools create persistent attack pathways into control networks. Credential theft and session hijacking are rife. **Can you deliver secure, auditable, time-limited remote access that satisfies both operational urgency and security policy?**

AKJ Associates

e-Crime & Cybersecurity Congress Online Series: Manufacturing

SECURING MANUFACTURING

Key Themes

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?**

Navigating NIS2, IEC 62443 and converging compliance demands

Manufacturers face an expanding web of regulation — NIS2, IEC 62443, the Cyber Resilience Act — each demanding evidence of governance, risk management and technical controls. Compliance teams drown in overlapping frameworks and manual audits. How can vendors help turn this regulatory burden into a structured, continuous security programme?

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 IIoT, cloud and edge

Smart manufacturing initiatives are flooding plants with IIoT sensors, edge computing and cloud analytics platforms — each expanding the attack surface faster than security teams can respond. Digital transformation and security pull in opposite directions. **So, how to embed security into Industry 4.0 architectures from design onwards, protecting data flows from sensor to cloud?**

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?**

Securing the supplier

Manufacturers depend on hundreds of suppliers, integrators and maintenance contractors, many with privileged access to critical systems. A single compromised vendor can cascade through the entire supply chain. **But what can realistically be done? How can CISOs control third-party access, and detect malicious activity originating from trusted external connections before it reaches production?**

AKJ Associates

https://akjassociates.com/event/manufacturing

Why AKJ Associates?

SECURING MANUFACTURING

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.**

Why the e-Crime and Cybersecurity Online Series?

SECURING MANUFACTURING

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.

e-Crime & Cybersecurity Congress Online Series: Manufacturing

SECURING MANUFACTURING

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** is 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: 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 keep our **online congresses exclusive and give you the best networking opportunities**.
- This is an opportunity to **continue driving leads** in partnership with our outstanding 25-year reputation and the e-Crime & Cybersecurity Congress brand.

https://akjassociates.com/event/manufacturing

AKJ Associates

Delivering the most senior cybersecurity buyers

SECURING MANUFACTURING

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.

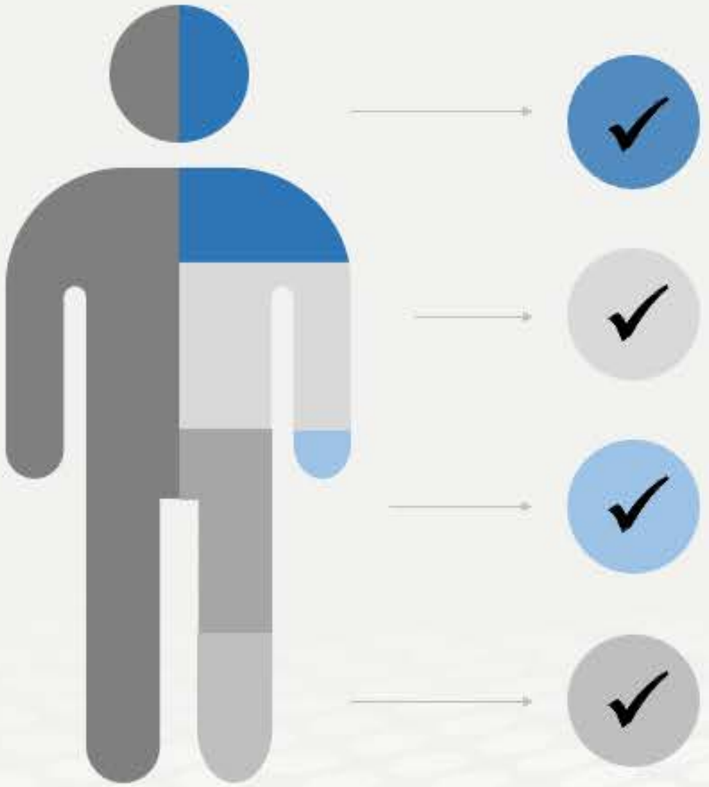
You will have access to the most senior buying audience in the cyber-security market.

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.



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.

e-Crime & Cybersecurity Congress Online Series: Manufacturing

SECURING MANUFACTURING

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 because they generate real business at our events every year. Our sponsor renewal rate is unrivalled in the market.

AKJ Associates

https://akjassociates.com/event/manufacturing