SECURING Manufacturing

e-Crime & Cybersecurity Manufacturing Summit

April 25th, 2024, Online

Securing OT and OT/IT dependencies in manufacturing and process industries

The most complicated challenge in cybersecurity? Probably. A regulatory timebomb? Definitely.

AKJ Associates

https://akjassociates.com/event/manufacturing

e-Crime & Cybersecurity Congress Online Series: Manufacturing

SECURING Manufacturing

A critical priority for companies and governments

Industrial organizations are at a turning point in their OT cybersecurity journeys. This includes discrete manufacturing operations that assemble many small parts into larger manufactured objects, such as automobiles or laptop computers, process industries that transform raw materials into a more useable form, such as mining or refining and also many types of critical infrastructure: Industrial operations that are essential for society to function such as transportation, power, and utilities.

According to McKinsey, more than 90% of manufacturing firms have had their production or energy supply hit by some form of cyberattack and 96%percent of business leaders indicate the need to invest in OT cybersecurity, and approximately 70 percent of those who have invested in it are facing implementation challenges.

In the US, CISA has highlighted dramatic increases in OT system cyberattacks, and in Europe ENISA's findings mirror this. The World Economic Forum has also just also put out a bulletin highlighting OT risks.

But OT risk is not a single issue. Attacks on (often legacy) ICS and SCADA systems are one thing. Attacks on broader industrial systems that cause physical consequences in the real world are another. And attacks on the IT systems upon which OT systems are increasingly reliant is another (IIoT insecurity is a big issue). Only a minority of attacks are "pure" OT compromises like the 2020 EKANS ransomware attacks against Honda and Enel and recent German wind turbine attack in 2022.

Increasingly, threats exploit the growing size and diversity of IT/OT attack surfaces. Attackers can rely on industrial control systems (ICS) being connected to corporate TCP/IP networks at least periodically giving access to them via standard business networks. For example, ransomware that encrypts data on IT networks is now a significant issue in OT security. And of course, attacks on IT/OT systems at third-party suppliers can then be weaponised against downstream IT/OT systems.

For example, in February 2022, Toyota shut down 14 manufacturing plants because of a cyber-attack on Kojima Industries, a key supplier. And when the company was hacked in February 2022, the world's top-selling carmaker had to halt operations at 14 factories at a cost of about $375 million.

The complexity of the IT/OT environment brings unique security challenges. For a start, normal tools do not work very well. In OT environments scanning-based solutions like endpoint detection and response (EDR) or endpoint protection platforms (EPPs) are not suitable. They rely on continual telemetry and cannot operate properly in an air-gapped situation.

These systems also fail to detect fileless and evasive attacks reliably as many threats don't create recognizable signatures EDR. The same applies to solutions that use similar technology in other parts of the IT environment, such as NDRs deployed to analyze network traffic. This is important because threats such as unauthorized firmware installed on OT systems or unknown, dynamic variants of malware normally found in traditional IT environments are becoming more common.

Even where traditional solutions do detect issues, because they struggle with, the diverse range of legacy OS, hardware, and applications that exist in a typical OT environment they often create huge numbers of false positives. These would bring manufacturing processes to a halt and downtime is the single biggest issue in critical industrial processes. Revenues are at risk as, sometimes, are human lives. Replacing compromised OT is extremely costly and time-consuming and so is remediation.

So, what are the solutions? Is Zero Trust the answer? What does layered security in an IT/OT environment look like? How do you deal with the issue of false positives? What kinds of solutions are not dependent on online updating? And how can firms stop advanced threats from cross-propagating business and OT systems. Industrial infrastructure is a prime target for well-funded attackers and complex attacks like zero-days, fileless worms, trojans and malware.

The e-Crime & Cybersecurity Manufacturing 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 behind some of the world's most admired brands.

https://akjassociates.com/event/manufacturing

AKJ Associates

e-Crime & Cybersecurity Congress Online Series: Manufacturing

SECURING Manufacturing

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?**

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?**

Why zero trust, isolation and segmentation are key

There has been a shift in recent attacks away form 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?**

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?**

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?**

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?**

AKJ Associates

Why AKJ Associates?

SECURING Manufacturing

A History of Delivery

For more than 20 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 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.**

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** 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 to your online booth, and showcases 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.

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.

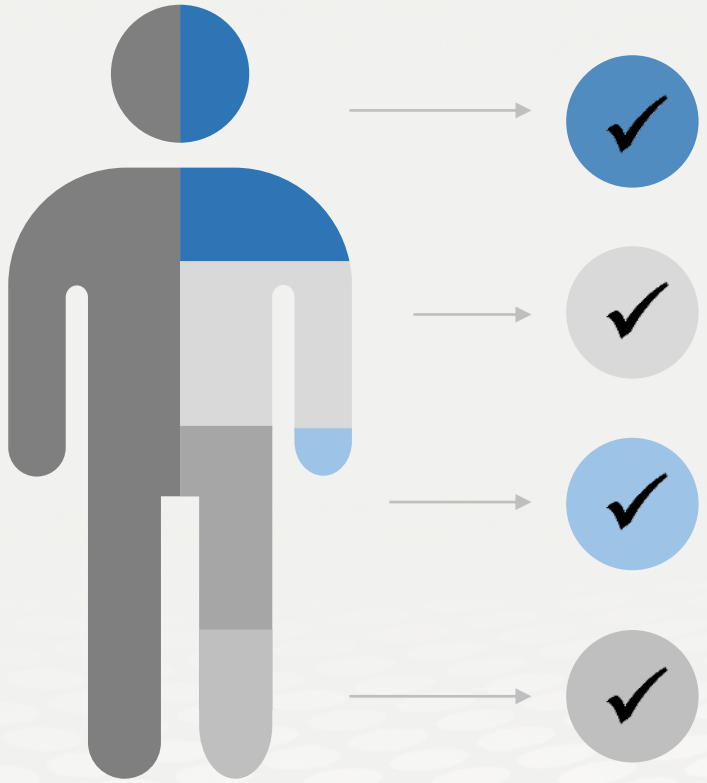
You will have access to the most senior buying audience in the cyber-security market.

AKJ Associates has been building relationships with senior information risk and security professionals for 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

SECURING Manufacturing

Specific, actionable and relevant information for time-constrained industry professionals

SECURING Manufacturing

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

SECURING Manufacturing

PhishRod

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.

VERACODE

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.

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 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