

e-Crime & Cybersecurity Congress Benelux



15th Annual e-Crime & Cybersecurity Congress BENELUX

November 25th, 2025, Amsterdam, The Netherlands

Benelux's Digital Ambitions Undermined Without Robust Cyber Defences

Cybersecurity continues to be the missing pillar of many countries' digital ambitions. What needs to be done?

A troubling pattern of vulnerabilities

In July 2025, a serious cybersecurity incident struck the Dutch Public Prosecution Service (Openbaar Ministerie, OM), revealing the fragility of even the most critical national institutions.

As a result of a suspected breach, the OM remains disconnected from the internet indefinitely — a measure taken to contain and investigate the intrusion. Prosecutors are unable to send or receive emails, log in remotely, or even edit or print legal documents. Court proceedings are expected to face delays, and public confidence is under pressure.

This incident is not isolated. It forms part of a broader wave of cyberattacks affecting the Benelux region in 2025.

Luxair (Luxembourg, April 2025): the national airline suffered a ransomware attack that grounded flights for nearly two days. Attackers exploited a misconfigured VPN appliance.

Belgian Ministry of the Interior (May 2025): hackers accessed sensitive documents by exploiting an unpatched vulnerability in the Ministry's document management system.

Port of Rotterdam (June 2025): a supply chain attack disrupted port logistics when malware was introduced via a customs broker's software update.

Together, these events demonstrate not only growing attacker sophistication but also serious vulnerabilities in public and private digital infrastructure. For CISOs, the implications are urgent and strategic.

- Incident response plans must cover prolonged disconnection scenarios — not just recovery and restoration.
- Visibility into endpoint and third-party environments is vital, especially for government agencies that may be targets of nation-state actors or politically motivated hackers.
- Legacy systems and exposed remote access points remain key attack vectors. Regular configuration audits are critical.
- Patch management failures offer easy wins to attackers. CISOs must implement faster update cycles and use attack surface monitoring tools.
- Cyber supply chain risk is a huge challenge. Trust boundaries must be re-evaluated, and vendors continuously assessed.
- Critical operations should be decoupled from external systems wherever possible.
- Slow detection & response are still a problem. CISOs must improve real-time threat detection and internal threat hunting capabilities. The Dutch NCSC discovered the OM breach before internal teams did.
- Crisis management readiness: the OM is still offline weeks later/ Incident response and resilience must go beyond disaster recovery and into sustained continuity planning.

In the Benelux region, governments pride themselves on high levels of digital public service delivery. Corporations also have committed to high levels of digitalisation. But these levels of digitalisation must be backed up by solid security. Without this, public trust in institutions and companies will be eroded, and the benefits of digitalisation will be damaged by the costs of repeated clean-ups.

The e-Crime & Cybersecurity Congress Benelux will look at how cybersecurity professionals can stay ahead of a rapidly evolving attack environment. Join our real-life case studies and in-depth technical sessions from the most sophisticated teams in the market.

e-Crime & Cybersecurity Congress Benelux

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?**

Security Posture Management

Traditional vulnerability scanners don't handle cloud native architectures well. Today's cloud environments spin up thousands of ephemeral assets without a traditional OS, without an IP address for long. **So how do you adapt to that dynamic, API-driven reality?** **How can traditional tools connect the dots – not just generate tickets?**

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 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?**

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?**

Dealing with regulations

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?**

e-Crime & Cybersecurity Congress Benelux

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 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**.

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

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.

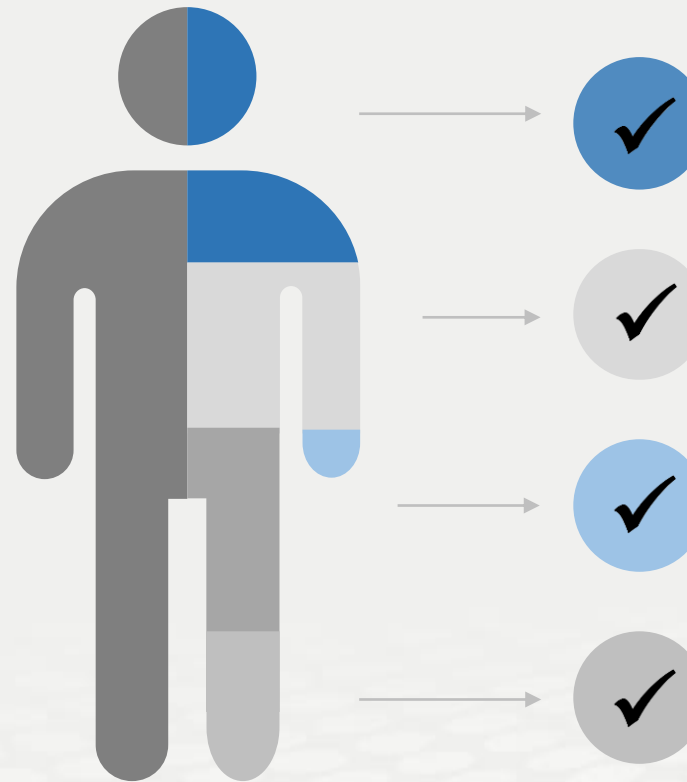
You will have access to the most senior buying audience in the cyber-security market.

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

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 20 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 20 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 20-year reputation and the e-Crime & Cybersecurity Congress brand.

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.



This is always a great event for 'taking the temperature' on security issues, to get a feel for people's impressions on current security challenges and to find out what organizations of all kinds are doing.



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