# e-Crime & Cybersecurity Congress Online Series: CNI

SECURING
CRITICAL NATIONAL
INFRASTRUCTURE


## e-Crime & Cybersecurity CNI Summit

**September 16th 2025, London, UK**

## CNI security and resilience are now a shared legal obligation. Time to invest.

**CISOs face more scrutiny, more firms in scope, broader duties, and a stronger regulatory environment. Organisations found wanting will be in trouble.**

**AKJ Associates**

http://akjassociates.com/event/cni

# e-Crime & Cybersecurity Congress Online Series: CNI

SECURING CRITICAL NATIONAL INFRASTRUCTURE

## More security investment is both compulsory and a strategic opportunity

The UK faces increasingly severe and frequent cyber threats from hostile states and cybercriminals. Recent incidents (e.g. ransomware attack on NHS suppliers) illustrate real-world impacts of cyber breaches. Supply chains are a major vulnerability, and current resilience is not improving fast enough.

**The case for change is obvious:** The current framework, based on the NIS Regulations 2018, is outdated and narrowly scoped. The next set of UK legislation aims to expand and modernise these regulations to match today's threat landscape. And it aligns with the EU's NIS2 directive while reflecting UK-specific needs. Of course, in the EU, and for anyone who wishes to do business there, things are moving even faster.

**CISOs face expanding regulatory scope and empowered regulators:**

- Managed Service Providers (MSPs) to be brought under regulation due to their critical IT roles.
- Supply chain security strengthened by allowing regulators to designate "Critical Suppliers" subject to new duties.
- Stronger technical standards and methodological requirements aligned with the NCSC Cyber Assessment Framework.
- Enhanced incident reporting (within 24–72 hours), including obligations for customer notifications.
- ICO granted proactive powers to collect data and act before incidents.
- Introduction of modern cost recovery mechanisms to make regulators financially self-sustaining.
- Delegated powers for the Secretary of State to swiftly update regulations without new primary legislation.

**So, what does this mean for CNI organisations and those who service them?**

- Businesses, especially MSPs and digital service providers, will face new compliance and reporting duties. Critical SMEs and other third parties may also come under regulation if they support essential services.
- Your organisation may now be in scope, especially if you offer or rely on managed services, data centres, or critical suppliers.
- Incidents affecting confidentiality, availability, or integrity must be reported within 24–72 hours – not just service disruptions.
- Regulators can now designate specific third parties as Critical Suppliers – you may be liable for their cyber failings.
- Expect proactive enforcement, more detailed technical standards (aligned with the NCSC CAF), and fee-based funding of oversight.
- The Secretary of State may direct your firm or regulator to take urgent action in response to national security threats.

**Increased regulation looks like a burden – and it certainly means more investment in security. But it is also a strategic opportunity.**

- Regulatory clarity means less ambiguity on cyber expectations.
- Proactive compliance and supply chain hygiene can become competitive advantages.
- This is a call to CNI security professionals to harden your risk posture before enforcement catches up.

**This is a national infrastructure priority and CISOs must lead the shift from compliance minimalism to strategic cyber resilience.**

AKJ Associates

# e-Crime & Cybersecurity Congress Online Series: CNI

SECURING CRITICAL NATIONAL INFRASTRUCTURE

## Key Themes

### Regulation – changing the game in cybersecurity?

Regulations are expanding the scope of who is included in CNI and the levels of accountability for firms and senior officers. So how does this new regulatory environment change the cybersecurity calculus? How do new reporting duties affect you? What happens if you are designated a critical third party? **What do firms need to do now?**

### A better approach to outsourcing cybersecurity

While outsourcing cybersecurity can improve security posture, organisations must retain key in-house cybersecurity expertise to oversee vendors, ensure clear contract terms and SLAs and regularly audit security providers to assess compliance and performance. **Can you help them adopt a hybrid model, where critical security functions remain in-house while external providers handle specific tasks?**

### Developing a risk-based approach to the Cloud

It's hard to square the need for national security with Cloud usage. Major defence contractors avoid it completely. So, what about critical sector such as healthcare or HMRC or nuclear energy or border control. **So, what does a balanced Cloud strategy look like – given the choice may be between crumbling legacy systems and Cloud? How can risks be reduced to acceptable levels?**

### Securing legacy technology

It isn't just the EOL of Windows 10 – though that is clearly a big deal. Public Sector organisations need to ensure legacy systems that cannot be replaced are isolated, monitored, and mitigated by compensating controls. **Can segmentation, virtual patching, data encryption, emulation, and secure API gateways help? What are your solutions?**

### The ultimate third-party problem

The public sector's dependency on third-parties is complete. Given that this is one of the great unsolved problems in general cybersecurity, how should the public sector go about managing the risk? What should it prioritise in both its own security practices and in its suppliers? **And what kinds of security architecture and solutions should these organisations look to implement asap?**

### Upskilling security teams

No organisation has an infinite budget. And most organisations are struggling to find sufficient security staff – the skills shortage is growing. This dynamic affects the type of on-prem security operation firms can employ and means that improving internal skillsets is critical to the security model. **So how can public sector CISOs continuously upskill their teams?**

## AKJ Associates

# e-Crime & Cybersecurity Congress Online Series: CNI

SECURING CRITICAL NATIONAL INFRASTRUCTURE

## Key Themes

### Ransomware – dealing with the new normal

The US Treasury reported that companies paid an estimated $5.2 billion in BitCoin transactions due to ransomware payments for companies in 2021, and only a quarter of ransomware attacks are reported. Ransomware is here to stay. **So how can CISOs stop it being a permanent tax on the business?**

### From cybercrime to cyberwar

Blurred lines between cyber-spies, cyber-criminals and cyber-armies have transformed the (in)security landscape, with nation-state exploits widely available. **How can the various elements of government work better with private sector solution providers and end-users to build security that can cope with not-quite-nation-state attackers?**

### Securing Arm's Length Bodies – a systemic issue

The neglect of cybersecurity in ALBs is a systemic issue driven by low budgets, weak oversight, outdated IT, and a lack of security culture. ALBs need help to impose cybersecurity standards (e.g., mandatory NCSC frameworks), help with security culture and training and help with incident response and other core security functions. **Can you help them with these challenges?**

### Cloud incident response

Recent Cloud outages have not simply disrupted low-level infrastructure, they have disabled cybersecurity solutions and, in turn, sometimes, shut down corporate access to critical network assets for significant amounts of time. Does CNI rely too much on Cloud? **As well as managing Cloud security, CISOs need good Cloud incident response. How are they going about it?**

### Managing insider threats at a time of crisis

When economies are under stress, employees too can find themselves in financial difficulty. When geopolitical tensions rise, people can take sides. Insider threats of various kinds become far more prevalent and dangerous at times like these. **So, how have security and other MIS tools matured to make detecting malicious insiders easier and more accurate?**

### Embracing risk management

Until cybersecurity is truly seen as risk management and not a whack-a-mole IT problem, the hackers will continue to evade outmoded control frameworks. Quantification is key but so is how it is used. Part of this is down to CISOs, part of it to Boards and part of it to solution providers. **The banks have done it. When will the rest of business catch up?**

## AKJ Associates

# Why AKJ Associates?

SECURING CRITICAL NATIONAL INFRASTRUCTURE

## 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.**

**AKJ Associates**

# Why the e-Crime and Cybersecurity Congress Online Series?

SECURING CRITICAL NATIONAL INFRASTRUCTURE

## 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: CNI

SECURING CRITICAL NATIONAL INFRASTRUCTURE

## 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.

# Delivering the most senior cybersecurity buyers

SECURING CRITICAL NATIONAL INFRASTRUCTURE

## 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.

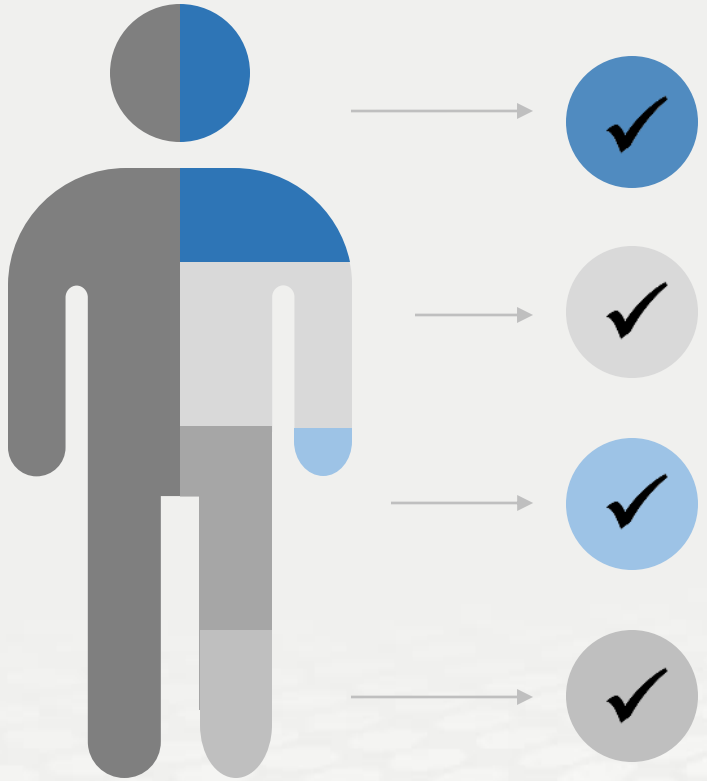
**You will have access to the most senior buying audience in the cyber-security market.**

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

AKJ Associates

# We deliver the most focused selling opportunity

SECURING CRITICAL NATIONAL INFRASTRUCTURE

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

SECURING CRITICAL NATIONAL INFRASTRUCTURE

**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 CRITICAL NATIONAL INFRASTRUCTURE

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.

KASPERSKY lab

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.

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**