e-Crime & Cybersecurity Congress

March 1st and 2nd, 2023, London

From cybercrime to cyberwar – the implications of a new era

As cyberspace becomes the arena for a new cold war, are traditional concepts of cybersecurity redundant?

e-Crime & Cybersecurity Congress

All change or no change?

Not that long ago cybersecurity was the art and science of stopping economically motivated actors exploiting vulnerabilities in traditional IT networks to commit a fairly narrow range of frauds, disruptions and data thefts. It was the counterpoint to cybercrime, which was seen as being carried out almost exclusively by non-state actors. Yes, some nation-states used cybercrime to make money and yes, governments' use of cyberattacks for economic and political espionage is not new.

However, it's become increasingly clear that a new global cyberwar has started that looks very much like the cold war of the 1950s to 1980s. Predictions of a transformation in the nature of warfare seem to have come true. And, as one commentator puts it, instead of stockpiles of nuclear weapons, "the threat of cyberwar, by contrast, has more to do with a global stockpile of vulnerabilities, amassed by accident as a by-product of continued innovations in connectivity. In the end, the sensation is the same: a foreboding feeling of pervasive, imminent risk. Cyberwar is real."

The question is, does this change anything for cybersecurity professionals? Does a cyber-cold war create a different set of risks for individual organisations?

It does. The potential for huge rises in the scale and sophistication of attacks, and the likelihood that infrastructure disruption and destruction will become more prevalent objectives changes the security calculus.

- **71% of CIOs and CISOs in a sample of almost 7,000 cybersecurity professionals believe cyberwarfare is a threat to their organization, and yet 27% admit to not having a strategy in place to mitigate this risk.**
- **51% of CISOs/CIOs, believe that businesses will need a specific strategy in place to protect against cyberwarfare in the next 12-18 months.**
- **The C-suite is increasingly concerned about loss of IP and R&D secrets, revenues and operational resilience.**
- **Governments are concerned about the potential for attacks on CNI and also for exploitation of poorly-understood linkages in financial systems, energy infrastructure and supply chains.**

NCSC CEO Lindy Cameron has said cybersecurity should be viewed with the same importance to CEOs as finance, legal or any other vital day-to-day part of the enterprise.

"Cybersecurity is still not taken as seriously as it should be, and simply is not embedded into the UK's boardroom thinking," she said during a speech at Queen's University, Belfast. "The pace of change is no excuse – in boardrooms, digital literacy is as non-negotiable as financial or legal literacy. Our CEOs should be as close to their CISO as their finance director and general counsel."

This year's e-Crime & Cybersecurity Congress will look at how we all need a new kind of security. Join our real-life case studies and in-depth technical sessions from the security and privacy teams at some of the world's most admired brands.

e-Crime & Cybersecurity Congress

Law enforcement resourcing, and indeed the resourcing of cybersecurity in the public health, education and council systems is laughable. It's time for government to put its money and power where its mouth is – and not just at the glamorous, GCHQ, offensive cyber, end of the spectrum.

And the model needs to change elsewhere. With increased dependencies on a handful of large telco and IT providers, governments need to grasp the nettle of regulating these providers too.

The fragmented and confusing security solutions market needs a shakeout: should a globally significant threat to public health and safety and business viability be left in the hands of hundreds of small start-ups almost all of which are no use to the SMEs who make up most of the economy?

And the NCSC and government need to take responsibility for the slow pace of cybersecurity literacy and effectiveness. The digital portfolio passes from minister to minister like an unwanted relay baton. Initiatives on fraud – the largest single crime area in the UK today – have been almost farcical. Recent revelations of ministerial security lapses are shocking.

We desperately need:

- More investment in cybersecurity defences both from government and the private sector
- A better understanding of the threat landscape at all levels
- Better intel from national security and law enforcement fed back to the private sector
- A higher rate of outsourcing security services by most organisations
- A revolution in IoT security
- More regulation and more joined up global regulation
- To move away from a CISO culture of risk aversion, checklists and specific systems towards a holistic, risk-based view of security

The next 20 years will be an increasingly asymmetric fight between a powerful, sophisticated and well-resourced set of attackers, and the rest of us. We now live in a hybrid metaverse, in which our digital lives, at work and at home, are as significant as the physical, and in which we require as much protection and regulation as in the physical world. Creating a safe digital space in which we can work, transact, and communicate securely, and which delivers critical components of public services, will require a completely different level of commitment to cybersecurity than that shown in the previous 20. And governments may need to take the lead to solve the most intractable problems of nation-state activity and dependency on unregulated BigTech monopolies.

e-Crime & Cybersecurity Congress

Key Themes: public sector

Where's the government when you need it?

Actions speak louder than words – especially if there aren't many words. Some governments have come late to the realization that they need to provide a much greater degree of protection for public services and citizens than they have done so far. **To do this they will need a huge amount of help. Are you part of the solution?**

The rise and rise of effective cybersecurity regulation

Data privacy is only a small part of the picture. Regulators are looking at operational resilience in key sectors like finance – securing the wholesale payments market is a priority and others will follow. They are looking at disclosure and fining the miscreants. **Can you help businesses comply with new regimes?**

Boosting bang for buck in law enforcement

Cybercrime, and particularly fraud, have overwhelmed global law enforcement. It will not be possible simply to staff up to beat the hackers, smarter, data-driven, AI-driven solutions are needed. **So, what does a modern cyber police force need and which advisors and solution providers will kit it out?**

Public-private partnership

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?**

Reining in BigTech

Resilience and security increasingly come down to key dependencies outside the organization. With on prem tech the past and Cloud and external IT the future, how do public and private sector organisations ensure security when they rely on vendors who are vulnerable but aloof and above leverage with even their biggest clients? **Time for governments to step in?**

Cyber versus crypto

Digital currencies are here to stay. Bitcoin and the rest may remain exotic assets, but central bank digital currencies look a certainty in the next 20 years and, in any case, digital payments are already consigning cash and cards to the same history book in which cheques live on. **What are the cyber implications of all this and who secures what?**

e-Crime & Cybersecurity Congress

Key Themes: private sector

Developing the next generation of security leaders

If cybersecurity is to change to meet the evolution of our digital world, then so must those who implement it. CISOs cannot cling to an IT paradigm and companies must move away from hiring on false pretences (on budget and commitment) and firing at the first breach. **What does a next-gen CISO look like and are you one of them?**

From smart machines to smart cities – securing the IoT

How long will it be before every significant device and location is part of an ecosystem of sensors connected to public and private networks? Driving apps tell insurers what premiums to charge. Packaging machines report their own breakdowns. **But are these devices visible on your network and how are you securing them?**

Mapping resources and controls to material business risks

How can CISOs understand which threats represent real business risks? It's easy to say 'talk to the business' – but how does that conversation work? If it does then CISOs can create a framework for prioritizing security, resilience, incident response and BCP spend. **So, what does this means and what does it look like in practice?**

The perimeter is dead - really

ZTNA and SASE may be tricky to implement; they may involve hard decisions about legacy tech; but they are also one of the few ways to deal with the death of the perimeter and new challenges like software supply chain attacks. **What business and public sector bodies need is practical help with implementation.**

From Cloud security to Cloud IR

Recent Cloud outtages have not simply disrupted low-level infrastructure, they have disabled cybersecurity solutions and, in turn, sometimes, shut down corporate access to critical network assets. **As well as managing Cloud security, CISOs need good Cloud incident response. How do they do that?**

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. 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?**

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 that they continue to support us 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 & Cybersecurity Congress?

For 20 years, the e-Crime & Cybersecurity Congress in London has been the most sophisticated, closed-door meeting place for senior cybersecurity professionals from government, law enforcement, intelligence and the private sector.

- Twenty years ago, it was clear that there was a need for a highly select assembly that brought together business, government, law enforcement and intelligence agencies in order to learn, share and work to combat cyber-crime of all kinds.
- So, in that year, AKJ Associates founded the e-Crime Congress after an approach by the Home Office, The National Crime Squad, The National Criminal Intelligence Service and the then recently founded National Hi-Tech Crime Unit (NHTCU).
- 20 years later we still work in partnership with the latest incarnation of the NHTCU – the National Crime Agency (NCA) – as well as the governments and intelligence agencies of many leading countries.
- We started a number of large and renowned closed-door events including: The European Public Private Partnership Forum, Combatting Global Counterfeiting Congress and Tackling Organised Crime in Partnership. The last of these led to the formation of SOCA – now the NCA.
- At a local level, we are very proud to say that we were invited into the very first discussions and activities when the UK Government was considering starting national entities such as Get Safe Online and CEOP (Child Exploitation and Online Protection Centre).

Today the e-Crime Congress is still a must-attend event for senior information risk and security professionals from business and government all over the world.

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.

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.

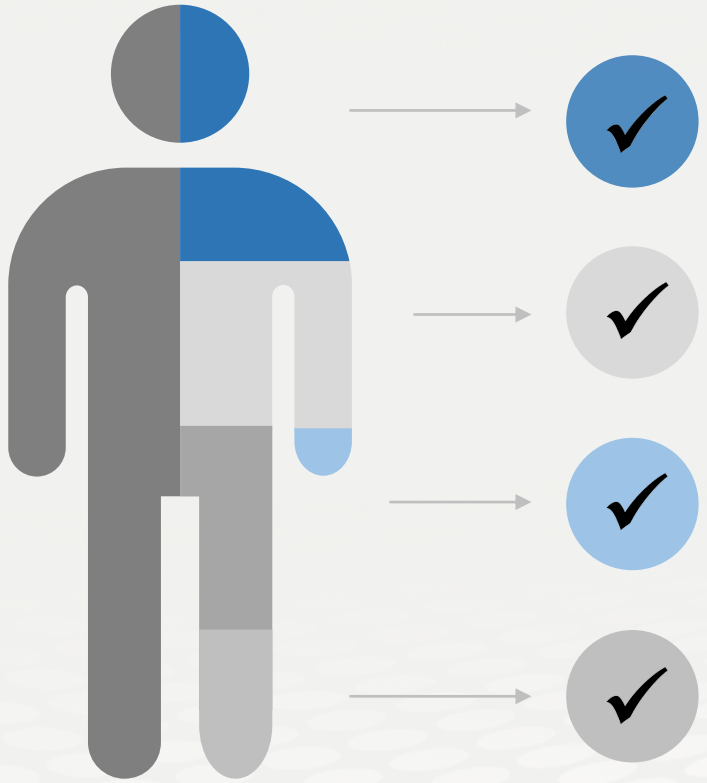
You will have access to the most senior buying audience in the cyber-security market.

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

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 visits 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, marketing documentation 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