e-Crime & Cybersecurity Mid-Year Summit

16th e-Crime & Cybersecurity Mid-Year Summit

October 17th, 2024, London

Simplifying cyber: is reducing complexity the key to better security?

Kubernetes, Containers, Cloud, OT/IT, BYOD, Defence-in-Depth, point solutions – how can CISOs make security manageable again?

https://akjassociates.com/event/midyear

AKJ Associates

If complexity is vulnerability, then how can CISOs simplify? What's the new paradigm?

We often ask why it is that so many of today's security problems were yesterday's and the day before's. One answer is that while security technology and processes have greatly improved, the problem has become vastly more difficult.

This is not simply because attackers have multiplied and become more sophisticated; it's not just because of AI or geopolitics or the expansion of the IoT and OT – although all of these have hugely increased attack surfaces and the scale of threats to them.

No, the underlying problem is more simply described as complexity. As one researcher says, "The simple combinatorial mathematics of the sheer increase in endpoints not only means a greater number of systems to manage but also much more complex network architectures and webs of connections underlying IT and technology infrastructure and systems."

For example, the rise of cloud computing, microservices, containers, IPv6, has created a vastly more complex endpoint infrastructure than existed before, even though that was comprised of billions of connected, physical devices. The default premise of cloud is to make services, APIs, storage, computing, and networking accessible – the default for a service is exposed to the world. Cloud storage is no longer segregated and sitting behind a server.

And at the same time as this increase in complexity and vulnerability, Cloud services (e.g. the IP blocks used by Amazon's S3 storage service) are increasingly easy to identify and attack.

The response of security teams to these paradigm shifts in technology, scale and complexity has often been to meet each challenge piecemeal as it occurs. So global firewalls have been supplemented with various technologies to cater for the fact that these firewalls must be. porous due to the growing number of APIs and services that must connect to the outside world.

Critical processes, services, and instances have been placed inside security groups, with access controls applied on a per-group basis, associated with identity providers and authentication systems.

At the same time, security teams put in place more defence technologies, often layering them to address specific threats or assets: data is protected one way, applications another, APIs are guarded by API gateways, Kubernetes clusters are guarded by specialized Web Application Firewalls and Ingress Controllers, SecDevOps teams mandate smaller, more lightweight firewalls in front of every public service or API and application security teams require that SAST and SCA scans be run on any code.

But what we end up with are security stacks too complex to fully understand or fully utilise. We create governance and assurance nightmares. We introduce insecurity because of the complexity and because of the additional third-party issues we create.

We need a new way to think about all this. But that would that look like?

The e-Crime & Cybersecurity Mid-Year Summit 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 Mid-Year Summit

Key Themes

Getting real about risk management

Until cybersecurity is truly seen as risk management, 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?**

AI for CISOs: the hype versus the reality

ChatGPT is hogging the headlines, but is it really relevant to CISOs still struggling with foundational cyber hygiene, preventing successful phishing attacks and avoiding DDoS and ransomware? **How is AI, in all its forms, being incorporated into security offerings and what should you ask providers about their products?**

Mobile device vulnerabilities and mitigations

Hybrid working isn't going away and for CISOs that means an ever-changing ecosystem of devices to secure, a non-existent perimeter and the threat of unknown connections and applications. Yes, zero trust is part of the solution but **what else should security teams watch out for in a mobile-centric world?**

Is it time to rethink your Cloud strategy?

Cloud was once seen as a business and security panacea. But hurried lift-and-shift, indiscriminate use of Cloud for all data storage and wholesale use of SaaS have caused problems from costs to misconfigurations and other security and business challenges. **Is the Cloud backlash justified? What should CISOs do now?**

Insuring the uninsurable?

Cyber-insurers need to understand the risks they are insuring if they are to set premiums at the right level. They need to know they are insuring risks clients have taken steps to mitigate properly: why insure those who leave their digital doors open. **So, what can and can't be insured?**

Securing the xIoT

The extended internet of things is a security headache. Connected cyber-physical systems were not originally designed to be connected to the internet and are riddled with vulnerabilities. And there are multiple challenges with cloud-based XIoT systems both via third-parties and via hacks to the host system. **Can you help secure these systems?**

Do you know your APIs?

Visibility is key in most areas of cybersecurity, but for APIs it could not be more critical. On average organisations employ around twice as many APIs as their security teams know about, and even those that are visible are rarely checked for quite straightforward vulnerabilities. **So, what should CISOs do about opaque API estates?**

Move to managed services?

If single point solutions and on-prem security are failing the business, what about the alternatives? What kinds of company need what kinds of third-party help? And where does that leave the in-house security team? **Do you have solutions that can help relieve the pressures on under-resourced CISOs?**

e-Crime & Cybersecurity Mid-Year Summit

Key Themes

Why regulation will drive better cybersecurity

Governments have ceded power to private sector organisations with more money, better agility and all the technology. But as governments belatedly recognize their dependence on private companies to deliver the modern state, they will remember their power to regulate, control and even nationalize. **What are they thinking today?**

Defeating ransomware and malicious malware

The NCSC still assesses that ransomware remains one of the greatest cyber threats to UK industry. In other words, the threat of malicious malware has still not been adequately confronted and the losses can be catastrophic. **So, forget about basic cyber hygiene and awareness, how do we protect the UK from this?**

The dangers of digitalisation – securing IoT and OT ecosystems

“There continues to be a heightened threat from state-aligned actors to operational technology (OT) operators. The NCSC urges all OT owners and operators, including UK essential service providers, to follow the recommended mitigation advice now to harden their defences.” **How can you help CNI-related companies harden their OT?**

Maximising the utility of threat intelligence

How can threat intelligence help defend and prepare against the emerging threat to organisations highlighted by the UK’s NCSC? As attack surfaces increases and geopolitics expands the range of threat actors and types, **how can organisations make the best use of threat intelligence to genuinely reduce their risk of breach?**

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?**

Evolving incident response: lessons from the past

All firms need well-rehearsed playbooks. They need Boards who have experienced realistic war games. They need to be battle-tested against sophisticated Red Teams. And they need to pay attention to the successful attacks of the past and present. **How can you help them develop and hone incident response procedures that work?**

Personal liability for CISOs? It’s here now.

CISOs and CIOs are in the dock in the US. They’ve been fined and banned in the UK. And the idea of driving corporate accountability through personal prosecution is now firmly embedded in regulatory and legislative thinking. **But CISOs cannot be held responsible for corporate failings, can they? We think they can.**

The answer really is zero trust, isn’t it? So how do we get there?

Look at the key security and resilience challenges. Ransomware, third-party, malicious insider, and the rest. None of them have been solved by better technology or better awareness or better security culture. And AI and OT insecurity will make things worse. **To take security seriously, zero trust is the only answer. So how to get there quickly?**

https://akjassociates.com/event/midyear

AKJ Associates

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

e-crime & cybersecurity MID-YEAR

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.

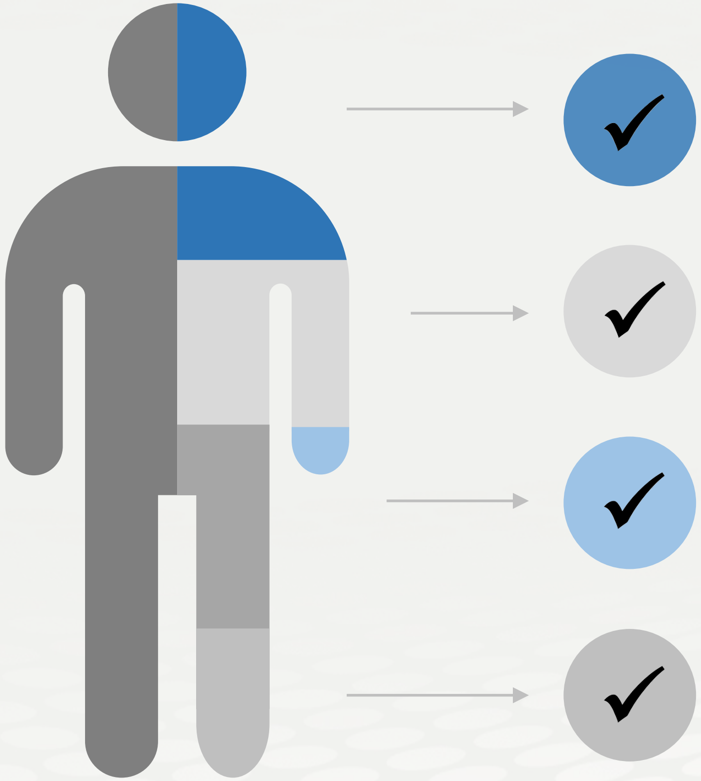
You will have access to the most senior buying audience in the cyber-security market.

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 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 Mid-Year Summit

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.

https://akjassociates.com/event/midyear

AKJ Associates

What our sponsors say about us

e-crime & cybersecurity MID-YEAR

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.

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.

✓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