

# e-Crime & Cybersecurity Congress in Abu Dhabi



## 12<sup>th</sup> Annual e-Crime in Abu Dhabi

21<sup>st</sup> September, 2022, Abu Dhabi

### Securing future tech

Crypto, quantum, DLT, AR/VR and the Metaverse – they are all here and all insecure. And what about web3?



# e-Crime & Cybersecurity Congress in Abu Dhabi

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.

That may sound an exaggeration but is it? JP Morgan has opened a lounge in the popular blockchain-based world, Decentraland with a suite of permissioned Ethereum-based services. CaixaBank is running advanced POCs in quantum banking.

Investing in crypto and NFTs is now routine for everyday citizens and so is exposure to the cybersecurity issues: in October 2021, attackers used phishing emails to rob cryptocurrency from 6,000 customer accounts at Coinbase by exploiting a flaw in its two-factor SMS system. Another malicious example of this kind of theft was seen in February, when \$1.7 million in non-fungible tokens (NFTs) were stolen in a phishing attack on OpenSea users. Over 250 tokens were stolen by an attack that exploited a hole in the Wyvern Protocol, which is the standard that underlies most NFTs. Millions have 'played-to-earn' in Axie Infinity – a game that has just been hacked to the tune of \$625 million.

As truly pervasive new technologies develop – web3 and DLT, AI and automation, and quantum computing to name just three – 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.

That commitment to cybersecurity will not just be driven by technology change. Strategic cybersecurity planning is already becoming a key part of reducing your organizations' potential for negative societal impact: cybersecurity is now part of ESG compliance.

And global regulators are increasingly interested in cybersecurity itself and not just data privacy. Just recently, the U.S. Securities and Exchange Commission (SEC) signalled a significant change in how it thinks about what constitutes a threat to companies: It now considers cyber vulnerabilities to be an existential business risk. This was evident in fines levied against two companies over inadequate disclosures of cybersecurity issues — British publishing company Pearson PLC and First American Financial Corp. These fines signal a major shift, and one that could profoundly change the way companies think about cybersecurity threats, communicate internally about these threats, and disclose breaches.

**The e-Crime & Cybersecurity Congress in Abu Dhabi will look at how we all need cybersecurity. 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.**

## Key Themes

### Getting real about automation, AI and the rest

The next 20 years will see an ecosystem of small single-issue vendors slim down to a far less complex set of larger platforms able to invest in continuous development and offering to cover all or large chunks of organisations' security needs. **But will the winners in this evolution be those at today's cutting edge?**

### 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 the technologies of the future

Quantum computers, web3, multiple types of distributed ledger technology, augmented and virtual reality, the Metaverse, AI-driven applications and even organisations, automation as a service – the list goes on. These technologies are happening now and they all have security implications. **Who is thinking about how to secure future tech?**

### All aboard the Cloud

Applications have become increasingly complex with users demanding more and more. They expect rapid responsiveness, innovative features, and zero downtime. Performance problems are no longer acceptable. They'll easily move to your competitor. **Should you go Cloud Native? What does this mean for security in practice?**

### The perimeter is dead – that is not just hype

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. The problem is what to do next. **What business and public sector bodies need is practical help with implementation.**

### 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?**

## Key Themes

### 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?**

### Keeping citizens safe

The COVID era demands unprecedented levels of citizen engagement. Compromises are inevitable to ensure the safety of all. But the systems required to provide safety also create a huge data security and privacy challenge for both governments and employers alike. **Can solution providers help?**

### 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?**

### 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 organisations ensure security when they rely on vendors who are vulnerable but above leverage with even their biggest clients? **Time for governments to step in?**

### 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?**

### Securing digital currencies and DLT

The move towards non-cash payment methods during the crisis has been extreme and looks irreversible. In addition, many more governments are now looking at developing their own digital currencies. **So how do we go about securing a world in which most, perhaps all, payments are digital? And what about the blockchain?**

# Why AKJ Associates?



**For more than 20 years**, AKJ Associates has been running 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.

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.

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.

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.



# 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.



# Increased impact through On Demand availability



## On Demand

### How does it work?

We film our physical e-Crime Congress events – keynote speeches and Education Seminars – and we make every one of these sessions available to view on our online platform for seven days.

Each session can be viewed by itself and registrants to this online, on demand version of the event will be able to view (but not download) any part of the event as many times as they wish over that week.

After seven days, the content will become inaccessible.

### Who can attend?

Everyone who attended the physical event has access to the On Demand event.

In addition, we carry out additional marketing and only registrants vetted by our team will be permitted to access the platform, exactly as we vet registrants to our digital and physical events already.

Unlike simultaneous, streamed hybrid events, On Demand events do not force delegates to choose between attending in person and attending virtually.



## Benefits of On Demand

### Delegate Benefits

- All those who access the On Demand content will be eligible for CPE points, making attendance of as many sessions as possible highly beneficial
- Delegates who wish to watch particular sessions again can do so
- Delegates can only attend one physical Education Seminar per session; they can now watch all of the Education Seminars
- Delegates unable to travel to the event for work, health or geographical reasons can now watch all the event sessions
- New delegates who did not register for the physical event or who prefer digital events can attend all the event sessions
- Organisations who are only able to send one or two team members to physical events can now allow their whole teams and related functions to view the content

### Sponsor Benefits

- All of the above create greatly enhanced traffic to all event sessions and so significant additional lead generation opportunities
- The On Demand event creates an additional branding and marketing opportunity post-physical event to supplement pre- and during-event efforts
- Sponsors benefit from an extensive marketing campaign by AKJ Associates to promote the On Demand version of the event



# 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.

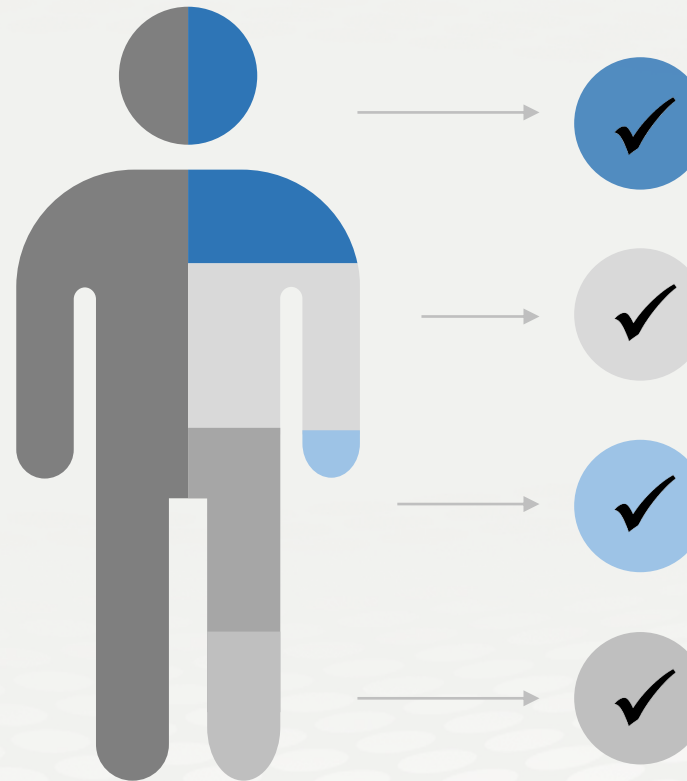
**You will have access to the most senior buying audience in the cyber-security market.**

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

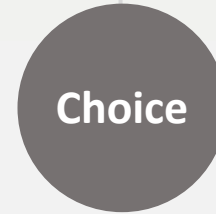
Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.



**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 in Abu Dhabi

## 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**