11th Annual e-Crime & Cybersecurity Congress in Dubai

March 19th, 2019, Dubai, UAE

Understanding the new rules of cybersecurity

How financial markets and new technology are changing the job of the CISO

AKJ Associates

https://akjassociates.com/event/dubai

Real life solutions for the virtual enterprise

"As data and operations become increasingly digitised in the UAE … cybersecurity has become even more paramount…and collaboration with global leaders in this area is one step forward to ensure a safe environment for everyone,"

His Excellency Omar bin Sultan Al Olama, Minister of State for Artificial Intelligence, UAE

Introduction

The first era of cybersecurity is over. It was an era of myths and half-truths. These obscured the business realities of providing and implementing cybersecurity and were driven partly by hype, and partly by confusion among end-users over the nature of cyber-risk and the appropriate risk management structures and staffing.

That era is being swept away by a new set of challenges. By 2030, more than 500 billion devices will be connected to the Internet and Smart Cities will be top targets for hackers. As the region's "most innovative city" and recently ranked by Mckinsey as top region for deployment of Smart applications, Dubai is forging ahead in the race for digital domination. But **this virtual landscape leaves a vast and exposed attack surface.**

Hyper-connectivity also means perimeters now extend outside the business. **The security of third parties is now as important as the security of your own organisation**: a lesson major local ride-hailing app Careem learnt the hard way when a breach compromised the data of over 14 million users held on external third-party servers. When 80% of data breaches originate from third parties, smart CISO's are looking for **trusted suppliers who understand the unique business challenges** this extended network brings.

At the same time, **breaches and regulatory non-compliance are now making the front pages**. Customers, investors and other stakeholders want to know that the companies they deal with or own are cybersecure. The current unwillingness to disclose breach and loss data and to detail cybersecurity precautions is untenable as stakeholders, customers and government demand this governance information and companies begin to use **cybersecurity as a competitive differentiator.**

This is **changing the way senior management view cybersecurity and the staff who they hire** to provide it. To them, cybersecurity is just another operational risk and needs to be managed like one. Cybersecurity is a business risk and so must be evaluated like any other business proposition. Everything cannot be protected equally. **Current CIOs and CISOs may not be the best people to make strategic cybersecurity calls – time to bring in the CFO?**

The $11.4 billion UAE cybersecurity market is expected to double in size by 2022. But end-users are putting their mouths where their money is. Peer testimonials and case studies are increasingly becoming the bedrock on which business leaders base their procurement decisions. **Never has the market been more competitive, and never has it been a better sales opportunity.**

As the UAE moves forward in its 4th Industrial Revolution, the e-Crime and Cybersecurity Congress returns for its 11th anniversary edition to cover the key themes and business risks faced by those charged with protecting key assets and sensitive data. We will be facing the truths the region needs to confront to succeed through this critical hyperconnected era.

Time to tear up the old cyber security playbook?

Introduction

- From bolt-on to built-in: industry and government need to stop thinking about cybersecurity and start thinking about cyber risk management: what is the difference and why does it matter so much?
- From techie to business partner: how can today's CISOs jump the gap from IT specialist to business risk manager? How do you implement holistic cybersecurity?
- It's all about the money: the financial impact of a breach on the bottom line has, up until now, been small enough that companies are prepared to chance it. But now investors and fund managers are taking an interest. Even without a breach, they're evaluating your cybersecurity. And if they don't like it, they can hit your company where it hurts: your share prices.
- The changing nature of the crown jewels: is today's obsession with data and breaches the right way to think about businesses' cyber dependencies? What are the real weak links and how to protect them?
- Building a best practice cybersecurity team: how, how much and who?
- How must CISOs adapt to a new environment of scrutiny? As cyber becomes part of corporate governance and social responsibility, what does this mean for the role?
- The UK's first cybersecurity class-action suits are coming, and more will follow as the use of NDAs to hide breaches becomes unacceptable. What happens when the true scale of cyber failure becomes clear to customers, citizens and employees?
- Cybersecurity as a competitive advantage: the myth that businesses are in this together will be exposed. Over time, companies with secure apps will beat those with insecure apps. Companies with better reputation for security will beat those with a worse reputation. Management knows this and will respond. What does this mean for the CISO?

Addressing the critical issues

Cybersecurity is now a top priority for businesses and governments. But they are no longer looking for short term fixes or silver bullets. Their solutions need to reflect the business realities they face and the concrete demands their clients are making today. So this edition of the e-Crime and Cybersecurity Congress in Dubai will focus on:

Key Themes

Cyber risk identification, measurement and management
- Translating security vulnerabilities into realistic operational loss scenarios
- Combining risk, cybersecurity and audit for the full picture
- Communicating cyber risk to the business

Securing specialised systems
- SAP and other ERP implementations are attractive targets: do CISOs get involved?
- What about treasury management, cash and risk management systems?
- Industrial, supply chain, logistics and manufacturing: identifying and securing embedded technologies.

The nature of nation state actors
- How can companies protect honest employees against increasingly sophisticated attacks?
- What are the most commonly used attack strategies and what are the best ways to defend against them?
- Is the state doing enough to provide secure national digital infrastructure?

Cost-effective compliance
- GDPR and other regulatory demands are expensive: how to reduce the cost?
- Cognitive, robotic process automation and AI solutions to compliance demands
- Outsourcing: from Cloud, to SaaS to virtual CISO – are off-premises solutions the answer?

AI: separating the hype from the reality
- AI attacks based on analysis of social media are the next threat. Solutions?
- What do vendors mean by “AI” and “machine learning” and what questions should CISOs be asking about these new products?
- AI for devops: finding the bugs before they escape

Getting the basics right
- The BA hack shows that without the fundamentals, no amount of money or innovative technology is the answer: why do firms still fail at the basics?
- Security in an outsourced IT environment: dealing with cost cutting and old-fashioned attitudes to IT
- The minimum viable cybersecurity process?

Demonstrate your solutions

Security professionals also need your help …

1 To find solutions that fit their needs

With so many providers, so little concrete information and so few metrics, choosing the right solutions is a real challenge. So how can security professionals choose from the provider ecosystem? **This is your opportunity to showcase yours.**

2 To deal with nation state actors and exploits

Just a couple of years ago, most firms were told they were not targets for nation states. How times have changed. Hostile state entities as well as 'escaped' state-developed exploits are a threat to all. **Can your products help?**

3 To comply with new regulations

Cyber-security is going mandatory. Voluntary commercial codes are not enough. Regulators want companies to demonstrate true cyber-security as well as basic compliance. **How can you help CISOs with this?**

4 To build more secure applications

In a world of rapid digitalization companies need constant product iteration and innovation to stay competitive. But rapid application development can compromise security and damage the business. **Do you have answers?**

5 To access the latest testing and simulation environments

The biggest firms now have access to state-of-the-art "cyber ranges" in which they can replicate their environments and safely experience real threats. But how can the rest of us test our system? **What solutions are available and affordable?**

6 To outsource what they cannot do in-house

Many organisations cannot afford in-house SOCs or security teams big enough to counter cyber threats effectively. So what can they outsource and does outsourcing really solve the underlying risk problem? **What can you offer?**

Demonstrate your expertise

They are looking for solutions to help with…

The exploding attack surface

Coping with a runaway threatscape

It's good to avoid FUD, but it also helps to confront reality: and the truth is that the Internet of Things, the nation-state and organised criminal focus on control and safety systems, and the wholesale migration to the Cloud by companies struggling to survive digitalisation means that the attack surface continues to grow far more quickly than defence capabilities or cybersecurity budgets. So what are the possible solutions?

Automation / AI / Blockchain

Smarter ways to guard the network

The adoption of identity analytics for identity governance and administration as well as authentication can reduce organizational risk and administrative efforts, while improving user experience. Products without analytics capabilities will over time increase administrative overhead and risk undiscovered security problems. What should CISOs look out for?

Safety and control systems

SCADA and the IoT move to centre stage

The resurgence of nation-state activity has renewed security professionals' focus on their vulnerable industrial safety and control systems. These are a prime target for sophisticated hackers and they are rarely developed with security in mind. In addition, the poor design of most consumer IoT devices is creating easy attack vectors into enterprise systems. SCADA is no longer an obscure niche: it's centre stage.

The data privacy problem

Dealing with data – cybersecurity becomes a governance issue

It's always been said that compliance and security are not the same thing. And that's true. But given the wave of new data privacy regulations companies are being forced to comply with, the boundary between the two has blurred. Securing private personal data is now a matter of law and good corporate governance. Stakeholders can put a number to the risks – even if it's just the GDPR fines regimen. So is there a cost effective way to kill two birds with one stone?

Where market-leading solution providers know they will find buyers

We deliver a focused selling opportunity

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

e-Crime Congress in Dubai

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.

https://akjassociates.com/event/dubai

Where the real decision-makers allocate budgets

Why do so many blue-chip vendors work with us? Real buyers ...

100%

The most senior cyber-security solution buyers

You will be surrounded by the most senior buying audience in the cyber-security market.

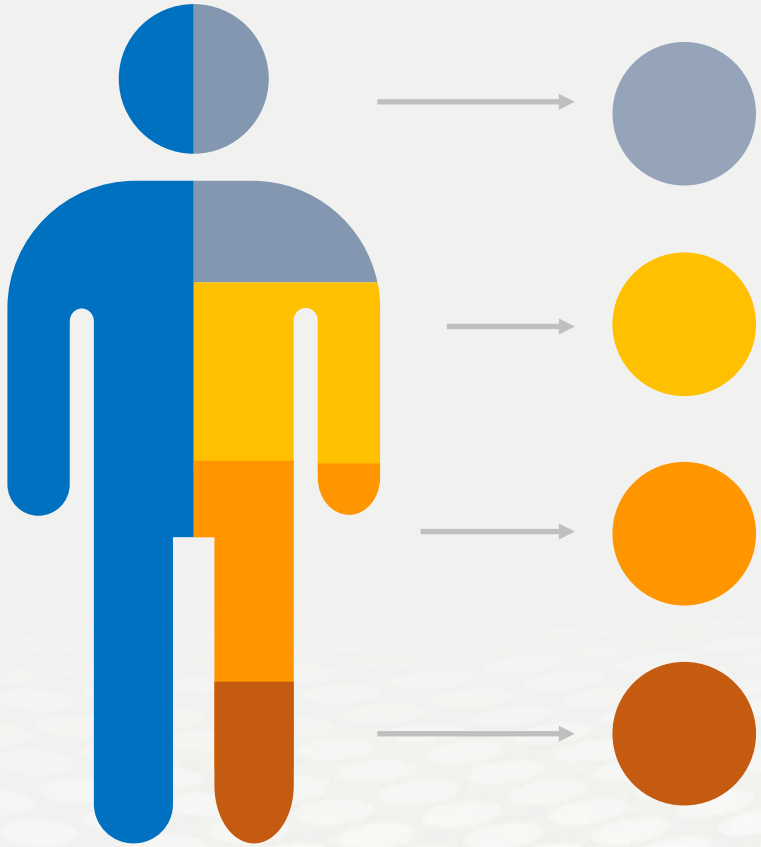
AKJ Associates has been building relationships with senior information risk and security professionals since 1999 and our cybersecurity community is the largest of its kind globally.

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 are attending e-Crime Congress Dubai.

We understand that every vendor needs to sell more. That is the bottom line.

Getting in front of the right people at the right time always increases lead generation and always increases profitable sales activity.



Cyber-security

We have been producing the events cybersecurity professionals take seriously for more than 15 years

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

https://akjassociates.com/event/dubai

Where the top solution vendors get their message across

Why do so many blue-chip vendors work with us? Real benefits...

Talk to customers

Face-to-face interaction with the right buyers works! Our vendors tell us it does and they renew year after year

Build relationships

Relationships built from a personal meeting are stronger than those initiated by solely digital conversations

Save time

Meet dozens or hundreds of selected buyers in a concentrated period – the value of a high quality event

Lead sourcing

We provide the best leads in the business. Each sponsor receives a delegate list.

Increase sales

All delegates are the right delegates. They have all been researched and confirmed as senior and with buying capacity

Get your message across

Delegates take all lunches and breaks in the exhibition area. So sponsors and exhibitors are always surrounded by qualified buyers

At AKJ we are always looking for ways to help our sponsors derive more value from our events. To reflect the evolution of contact channels, we are delighted to be able to confirm that we can offer lead scanners at our events. As sponsors seek to improve ROI and leverage post-event communication, we are committed to providing the latest technologies to help you drive your business forward.

https://akjassociates.com/event/dubai

Our testimonials speak for themselves: we have many more

What our sponsors say about us

proofpoint.

eCrime remains a critical event for security pros. Year after year, AKJ manage to stay on top of market trends and satisfy attendees' demand for topical expertise; we are delighted to be part of the e-Crime series.

KASPERSKY lab

AKJ events have yet to disappoint – from the massive number of attendees to our packed speaking sessions, this is one event we always look forward to!

COFENSE

We found the event very productive, it was good to meet potential customers and gives a chance for decision makers to meet us and understand what we do and how we can help them with their security.

Ninety five percent of our exhibitors and sponsors work with us on a number of 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.