17th Annual e-Crime & Cybersecurity Congress

5th & 6th March, 2019, London

The cybersecurity reboot: time to start over?

The new thinking, technologies and people needed to stay digitally fit

AKJ Associates

In the age of the stakeholder, the old rules don't apply

"People have had enough of experts," said UK minister Michael Gove in 2016, explaining the Brexit 'yes' vote. And he was right. Experts told us that structured mortgage debt was safe and the financial system was fine. The writers that asked questions were fools who didn't understand the system well enough. And experts respond in a similar fashion across industries as diverse as food, automotive, Big Pharma and cybersecurity when things look problematic: the average Joe doesn't know enough to ask questions and the odd problem is just something that happens. Keep the problems out of sight, and that's good enough.

But it's not. Early adopters may have been happy to accept the idea that the occasional loss of services or money is the price of having a credit card, a bank account or using e-Commerce and other websites. After all, these are the guys who put up with beta software and buggy first gen hardware. But as **digitalisation becomes the norm, then normal customers, normal citizens, and their expectations drive what business and government have to deliver**. And they will not be told by some expert that the complexity of cybersecurity means that they risk everything every time they go online. Nor will they be happy to learn that serious data breaches are more common than they imagine, but **covered up by NDAs and spurious excuses to avoid transparency**.

They've already started to push back: **the first class-action suits are coming, courtesy of security and PCI DSS compliance failures that demonstrate basic failings at even the biggest, most technology-dependent companies.** More will follow and **the C-suite will listen to stakeholders' demands,** not the security team's statistical arguments about the nature of cybersecurity, the need for customers to get used to losses and for everyone to be scared to go online.

The regulators are backing them up too. GDPR is a citizens' charter, forcing companies to disclose the true extent of the current failure of their systems and processes.

This edition of the e-Crime and Cybersecurity Congress will look at the unspoken truths of cybersecurity, the things we all know and say in private, those truths that normally stay hidden but which must be confronted if the industry is to meet the challenges of this new era.

Time to tear up the cybersecurity playbook?

What's the point of cybersecurity? It may seem an odd question, but if you listen to security professionals, you'd conclude that it was to stop ransomware losses, data exfiltration or GDPR non-compliance. In fact, **cybersecurity is a risk management function** whose job it is to ensure that organizations can operate in the way that management and stakeholders want. In the case of the private sector, this means ensuring that customer demands, products and services can be fulfilled within an increasingly digital environment. In the case of government, it means the same issues of digital transformation along with the additional problems posed by connected CNI, smart cities and securing citizens more broadly.

From cars to buildings, the inanimate is becoming smart, connected to smart devices, controlling smart machines. Data drives just-in-time supply chains and on-demand manufacturing. In government, smart cities mean autonomous traffic systems controlling flows, smart surveillance systems can react to everything from crime to the weather, with CNI like power and water able to anticipate demand.

And for both all of this means a convergence of previously separate networks, devices and assets, with huge amounts of data having to flow seamlessly across a multitude of what once were silos. To say that the attack surface is growing is a profound understatement. It is more accurate to say that **everything is part of the attack surface.**

But current models of cybersecurity – and indeed of IT and broader management – were **not designed for this**. Organisations still treat different pieces of infrastructure separately; they identify critical assets infrequently and discretely; they identify specific problems and implement solutions without a holistic approach; and **they staff and manage IT and cybersecurity as a bolt-on**. **This has to change.**

The e-Crime and Cybersecurity Congress will focus on the new tools, technologies and risk management thinking needed not just to secure digital transformation and the IoT, but simply to deliver the basic levels of security business and government need to operate.

e-Crime & Cybersecurity Congress 2019

Day One: the unspoken truths of cybersecurity

Session 1: the true state of the cyber-nation

- If a national airline can't even stay PCI compliant, what is the true state of cybersecurity (and corporate commitment) today?
- If the true level of data breaches has been hidden by NDAs and compliant regulators and markets, what will we see now that those defences are crumbling?
- If there is a huge skills gap, what does that say about the current ability of firms and governments to defend?

Session 2: cyber-financialisation is a gamechanger

- Regulators from the FTC to the EC are making data loss a big deal: compliance failure is now a material P&L hit.
- Institutional investors have been slow to the game but they are all in now. Get security wrong and they will hurt you. The cleverest are shorting you already.
- The perception of bad cybersecurity hurts enterprise value as much as an actual hack. Do firms understand what this means?

Session 3: show me the money

- Outside banking cybersecurity budgets are pitiful relative to the risk. This has to change.
- Are you paying enough? CISO and other security packages look too low. Why?
- How much funding has your vendor had? Is it hoping to be flipped? The small can't build an enterprise solution.

Session 4: how scrutiny changes everything

- Old-school cyber experts poo-poo transparency and the press; they're out of time. Customers and their lawyers will rule.
- Boards are realising that cybersecurity is governance and that governance is public
- Proper operational risk management techniques will replace IT- and compliance-based processes.

Cybersecurity is governance and governance is public. The big picture of stakeholders, scrutiny, financial markets and customer action is taking over. Companies skimping on IT outsourcing or PCI/GDPR compliance will be found out. 'Can do' not 'can't do' CISOs will come out on top.

e-Crime & Cybersecurity Congress 2019

Day Two: revolution not evolution

Session 1: Securing Digital Transformation

- If business survival depends on going digital, then it depends on cybersecurity. Can the industry deliver?
- Boards get it – and now they want answers, metrics and the right personnel. Can they get them?
- As B2C and B2B interactions migrate online, the payments revolution accelerates. What are the latest developments?

Session 2: Time to tear up your security playbook?

- Digital transformation, the prevalence of organised and skilled adversaries – cybersecurity was difficult before; what needs to change going forward?
- Choosing solution providers is critical: what's your process? Are you picking the right partners?
- Are the current NIST and other frameworks actually sensible ways to think about and manage cyber operational risk?

Session 3: Securing hyper-connectivity

- The IoT – an $11 trillion opportunity or a disaster waiting to happen? How do vendors, private firms and governments fix this?
- Government, under pressure from citizens and consumers, will also demand more. But how can we secure those public digital spaces?
- Nation-state attacks are no longer a rarity. But who is equipped to defend against them?

Session 4: From cybersecurity to risk management

- If cybersecurity controls don't work, they don't reduce risk. But how many CISOs operate to reduce real-world business risk?
- Where does cyber sit in your firm's overall risk management framework? Why? Should that change?
- Do CISOs genuinely understand how to align their own function with the businesses that ultimately fund them?

The digital world requires systemic digital security. The piecemeal approach is not scalable or effective. So how does that change the vendor ecosystem? What does it means for CISOs/CSOs? And how does it change cybersecurity priorities for the CFOs who ultimately have to fund them?

e-Crime & Cybersecurity Congress 2019

Private sector end-users need your help with …

Cybersecurity: a core risk management discipline

- Prove your cybersecurity wish-list is appropriate to the business
- Making cyber part of existing operational risk processes
- Getting buy-in from the CFO

Making cybersecurity affordable

- Who is the on-premises enterprise security stack really for?
- Building the minimum viable cybersecurity infrastructure
- The wider IT implications of cyber: does *anything* stay on-premises?
- The role of automation in creating affordable cybersecurity

Ensuring enterprise scalability

- How to build a scalable technology and team
- Long-tail, Big Data – solving the core cyber scale problem
- Do your solutions and stack scale to enterprise and threat?

Cybersecurity for the SME

- Even large SMEs cannot resource large in-house IT/security. Solutions?
- Cost versus risk: proving the value of cyber for the SME
- Cloud solutions for 'normal' companies – what makes sense?

Taking third-party security seriously

- Going beyond questionnaires – real solutions to the problem
- Technology versus people versus process
- Third-party security as a governance issue: helping your supply chain

Cyber-physical security: a holistic approach

- Why physical security and cybersecurity must be managed together
- The implications for the CISO and the security teams
- Which solutions recognise the combined nature of next generation cyber-physical risks?

Intelligence-based cybersecurity

- The importance of threat intel in budgeting for cyber risk
- Matching threat intel with vulnerability assessment
- Getting solution providers to work together

Prepare for transparency now

- Stakeholders are demanding information today
- Cybersecurity attitude is untenable from a business perspective
- Cybersecurity is governance and governance is public

e-Crime & Cybersecurity Congress 2019

Public sector end-users need your help with …

Getting the basics in place
- From the health service to local councils, government is way behind
- Implementation of core cybersecurity processes and technology
- Outsourcing, the Cloud, choosing the right IT partner

Protecting the country and the citizen
- Defending CNI against nation-state and criminal attack
- Ensuring the digital security of online citizens of all ages
- Third-party security as a governance issue: helping your supply chain

Providing a secure foundation for the digital economy
- Providing world-class, secure connectivity
- Delivering public services through secure, modern IT
- Helping industry with digital transformation

Improving lives through smart communities and cities
- Building secure technology and communications infrastructure
- Being the core connector and protector of the IoT
- Developing strategy and oversight of hyperconnectivity

Solving the cyber skills gap
- Designing and building education to provide real-world cyber skills
- Collaborating with private sector training companies to boost skills
- Creating initiatives at all levels to boost cybersecurity awareness

Providing intelligence
- Providing daily cyber threat and incident data
- Sharing information on vulnerabilities
- Distributing best practice and awareness for threat intelligence program.

Driving innovation
- Helping with automation, AI and blockchain solutions
- Promoting innovation at all levels
- Getting solution providers to work together

Building better regulations
- Working with vendors and end users to develop real-world regulations
- Moving away from a tick-box compliance approach
- Trying to build a workable global framework through harmonisation

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

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.

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

Where the real decision-makers allocate budgets

100%

The most senior cyber-security solution buyers

You will be surrounded by the **most senior buying audience** in the cybersecurity market.

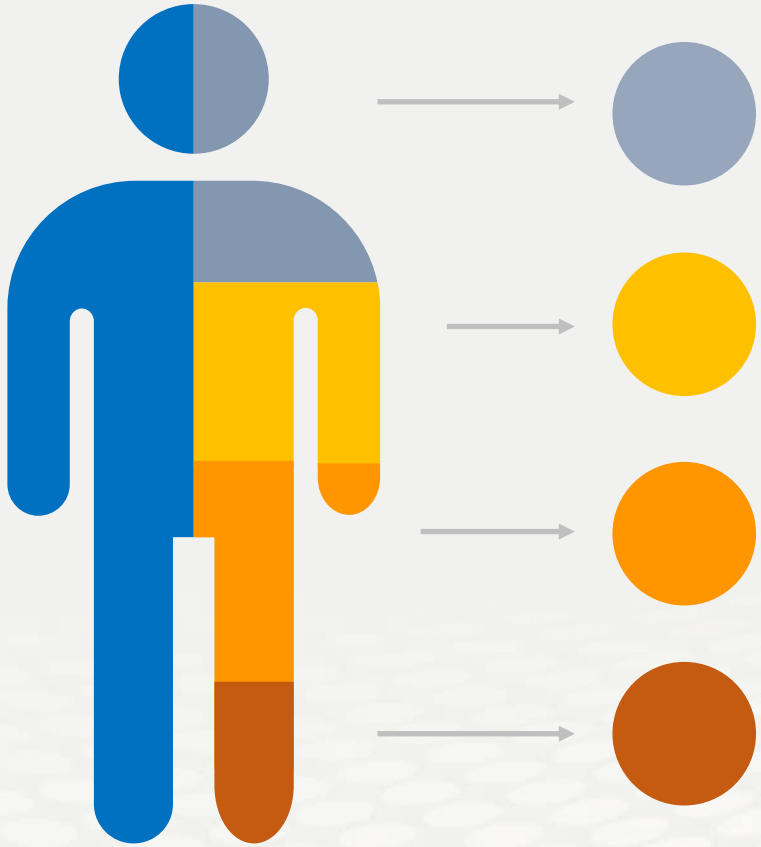
AKJ Associates has been building relationships with senior information risk and security professionals since 1999 and our **cybersecurity community is the largest of its kind** globally.

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, Enterprise Architects and Engineers **who so often dictate the purchase process**.

All of these job titles attend the e-Crime & Cyberscurity Congress.

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

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 personal meetings are stronger than those initiated by solely digital conversations

Save time

Meet dozens or hundreds of selected buyers in just one or two days – the value of a high quality event

Lead sourcing

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

Increase sales

All delegates are the right delegates. They have all been 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.

Unparalleled commitment and experience in digital security

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

Back in 2002 it was clear that there was a need for 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). **Sixteen 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 the largest gathering of the most senior information risk and security professionals from business and government in the world. The Home Office sponsored the public sector delegation from 40 countries in 2002 and we are delighted to say they still do today.
AKJ continues to ensure the highest level of private sector delegation attends.

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 eCrime 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.