11th e-Crime & Cybersecurity Mid-Year Summit

17th October, 2019, London

Re-imagining the CISO

Is the current paradigm unsustainable? What must change and why?

https://akjassociates.com/event/midyear

AKJ Associates

21st Century CISO: mission intolerable?

Introduction

Digital transformation is the key to business success. Cybersecurity is the key to digitalisation. There is a huge shortage of skilled cybersecurity professionals. So there has never been a better time to be a CISO, right?

Maybe not. As companies claim to recognise the strategic importance of cybersecurity, they have been piling ever more responsibility onto CISOs and their teams, but rarely increasing resources commensurately. The CISO can now be any or all of: project manager, policy maker, compliance officer, designer of procedures, in-depth technologist and expert on everything from threat intelligence to DNS hacks, RFPer and POCer, incident response manager, SOC manager…the list goes on.

In addition, CISOs are increasingly expected to be able to interact with boards and provide assurance to clients, shareholders and other key stakeholders.

This is not a viable or reasonable job description and it goes some way to explaining why so many CISOs are leaving the business, for vendors, to become consultants or to get out completely. CISO burnout is now a trending conversation.

And it raises a fundamental question: if the job of the CISO has become an unwieldy, inadequately resourced aggregation of everything cyber, then not only is it impossible to do it well, but it reflects a much broader failure on the part of organisations to structure their information security, privacy and compliance efforts sensibly.

Does the ever-growing list of CISO responsibilities indicate that companies need to re-engineer both the role and the activities it oversees? How much cybersecurity can realistically be carried out on-premises and what does that imply for teams and technologies? And how can solution providers contribute to a better outcome?

The 11th e-Crime Congress Mid-Year Summit will look at the fundamental issues that underlie CISO overload. There will be real-life case studies, strategic talks and technical break-out sessions from the security and privacy teams behind some of the world's most forward thinking companies, with their solutions to the current problems in cybersecurity.

https://akjassociates.com/event/midyear

AKJ Associates

Key Themes

Making the CISO's job sustainable is not just about budget and board access. Digital transformation is rapidly overwhelming most companies' ability to deliver reasonable levels of security at an acceptable price. So is new technology and new outsourcing models the answer? Does cybersecurity itself need to transform?

Key Themes

Let's talk about CISO overload
- Why are security professionals under so much pressure – and does it matter?
- Is business really committed to good security?
- Is the fundamental security paradigm flawed?

Can technology really help?
- Is automated security the answer or is it just another set of solutions in the stack?
- What IS automated security?
- Can AI really deliver today?

Consolidating the security stack
- Integrated solutions versus best of breed
- CISOs and the procurement process
- Projects not products, reality not utopia
- Re-thinking the vendor/CISO relationship

Joining up fraud, security and privacy
- Fraud is the flipside of security and privacy but is often siloed away from them. Why?
- AI and behavioural analysis in fraud detection
- Solving key problems in fraud compliance

Cloud and the CASB
- Identifying Cloud usage and exposure
- Governing and monitoring Cloud access
- Is a CASB right for me?
- Choosing a provider: common pitfalls

SIEM versus SOAR
- Can you handle a SIEM?
- What is security automation and orchestration?
- The convergence of SOAR, SIRP and TIP: what's the endgame?

MSSP versus MDR
- Why use an MSSP / MDR?
- Implications for costs, staff and security
- Security management versus better cybersecurity
- MSSPs vs. MDRs, SIEMs, SOCs and the rest

Outsourcing individual services
- IP Intelligence and other network monitoring processes
- Endpoint monitoring and security
- AI and network traffic analysis
- Penetration testing and maintaining security

Or is it a people problem?
- Taking responsibility at the top
- Is there a talent gap and if so where is it?
- Is lack of diversity holding back security?
- Technologists versus operational risk specialists

Demonstrate your solutions

Senior security professionals need your help …

1 To design the right in-house security structure

Choosing the level and scope of an in-house cybersecurity capability is the foundation of any security strategy. But choosing the appropriate structure and stack is a complex balancing act. **This is your opportunity to show you can provide practical solutions.**

2 To build the right level of external security technology

Outsourcing is clearly a critical part of any cost-effective cybersecurity infrastructure. But this means CISOs need help evaluating Cloud IT, Cloud security, SIEM, MDR, SOAR and the rest of security as a service. **What can you offer?**

3 To understand what your solutions do and don't do

CISOs have a hard enough time without having to deal with the opacity of the vendor market. What exactly does your solution do? Is it enterprise scalable? How much does it cost? How well does it integrate? **Explain your products.**

4 To cope with digital transformation

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 pick the right emerging technologies

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 benefit from the new? **What solutions are available and affordable?**

6 To build realistic security processes

The physical world accepts human error, rejects the concept of absolute security and is only willing to give up a fraction of its wealth for greater safety. It treats cyberspace no differently. **How does taking a realistic view of security change things?**

https://akjassociates.com/event/midyear

Demonstrate your expertise

They are looking for solutions in …

Adaptive architectures

Building solutions to bite back

Passive, static systems are increasingly vulnerable in a world of adaptive malware and attackers developing AI-based threats. Global adaptive security architecture is one answer – using predictive modelling and threat intelligence to adapt to a changing threatscape. This may even mean solutions becoming available with the ability to go on the offensive.

Automated cybersecurity and AI

Let the machine take the strain

Regardless of where you stand on the need for better cybersecurity versus resilience, or on the idea that actually cybersecurity is the way it is right now because business and government are spending exactly what they think is the right amount given the risks relative to other exposures, it's clear that developments like digital transformation are increasing CISOs' workload. Is automation the solution to that and to building cost effective security?

Fraud

How to join up fraud, security and privacy

It is still remarkable how often fraud and cybersecurity are in disconnected silos within their organisations. And yet fraud is the crime that results from poor security, and the flagging of potential fraud before it happens is one of the best defences against, and alerts for, data loss and data privacy issues. So why the disconnect and what does a joined-up fraud/security operation look like? And what technical solutions help build one?

Outsourcing cyber

Is cybersecurity someone else's core competence?

In all the talk of cyber-security, threat intelligence, next generation solutions and artificial intelligence algorithms it is easy to lose sight of the fact that very few companies can possibly afford or manage solutions for network protection and monitoring, end point security, messaging security, web security, incident response, threat intelligence – the list goes on. Is the answer for most firms to outsource to a one-stop shop?

Securing digital transformation

Building security into all business processes

Too many companies find themselves with a muddle of consumer-grade security solutions when what they need is a robust, enterprise-grade solution stack that is scalable and can realistically be implemented across a global business. In addition, good security hygiene – the digital equivalent of health and safety – is required holistically. Which solutions reflect this underlying truth?

e-crime & cybersecurity SCOTLAND

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 Mid-Year 2019

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/midyear

Where the real decision-makers allocate budgets

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

100%

The most senior solution buyers

You will be surrounded by the most active buying audience in the cybersecurity and digitalisation marketplace.

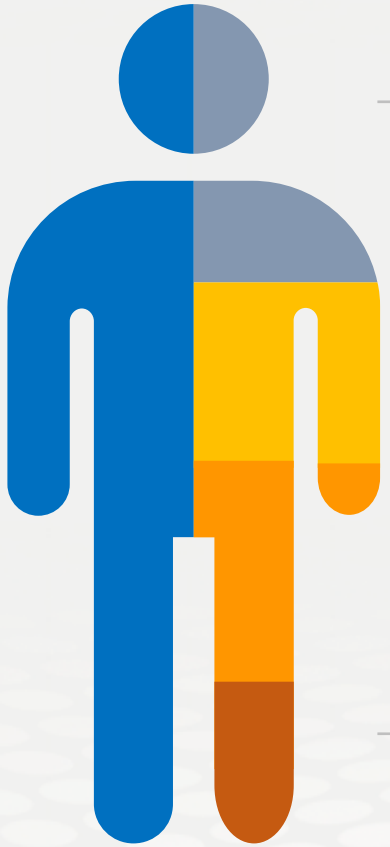
AKJ Associates has been building relationships with security and data privacy professionals since 1999 and our cybersecurity and payment security community is the largest of its kind globally.

We know the senior executives who drive strategy from the top, we know the enterprise architects who often control the largest budgets, we know the IT Security Leads and Engineers and we know the security and data specialists.

All of these job titles attend e-Crime Mid-Year Summit in 2019.

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 the lead generation and always increases profitable sales activity



Cybersecurity specialists

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

Digital transformation

We attract senior executives tasked with digital transformation and the associated need for new security solutions

Fraud, Audit, Compliance, Risk

We provide the go-to events for fraud prevention, digital risk managers 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 in privacy and GDPR

https://akjassociates.com/event/midyear

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 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. 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/midyear

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.

cigital

My team and I were impressed with the volume and caliber of the audience e-Crime Congress attracts. This event gave us the opportunity to expand our networks and learn more about our customers.

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.

https://akjassociates.com/event/midyear