18th Annual e-Crime & Cybersecurity Congress
March 3rd & 4th 2020, London

The Age of Convergence: can CISOs adapt?
How digital transformation is merging cybersecurity, privacy, compliance and fraud

AKJ Associates
Digital transformation (DX) is upending companies’ treatment of IT, security and information risk.

Most companies still treat IT as they did when it was new: as a toolset external to the business, limited to providing low-value services. Data is almost then just a waste product of that service provision.

In this model, cybersecurity is the defence of specific pieces of technology (networks or endpoints or perimeters) or specific ‘crown jewel data’.

To judge from budgeting and seniority, it is still not viewed as a strategic imperative, a way of protecting the entire company, or a way to see off an existential threat. And it has proved largely true that traditional operating and business risks are indeed far more important than cybersecurity risk, as well as being more quantifiable. Brexit, the US-China trade war and, for Boeing, the Max 737 crashes, are all higher up the risk priority list than data loss, DDoS and ransomware.

But that is starting to change. Post-DX, a company is interacting with its customers and supply chain digitally; its e-Commerce channels may have outstripped its physical channels and so its payments systems may also be fully digital; it may be developing new applications in-house; it may be gathering vast amounts of customer data and metadata to drive sales strategy, new product development, inventory management and credit control.

And it is likely in the B2C realm that it has been driven to a seamless omnichannel approach to business which requires centralised data and data management to deliver a consistent customer journey.

In that post-DX business, technology and data are no longer discrete tools useful to, but separate from, the business, they are the way the business delivers. Without them, there is no business.

At that point, cybersecurity is not just an IT operations matter; it’s not just about a loss of data, a blip in customer confidence, share price and reputation; it has finally become the real business risk that CISOs and vendors have claimed it was all along.

DX turns cybersecurity into a real business risk. So what next?

AKJ Associates

https://akjassociates.com/event/congress
e-Crime Congress 2020: Cybersecurity Re-booted

In this new environment, old models of security, privacy, fraud and data integrity are a real problem.

While cybersecurity was a matter of network security, firewalls, maybe a SOC and a bit of SecDevOps, left largely to techies, the idea of the security stack was allowed to prosper and cybersecurity became a piecemeal activity in which particular pieces of tech are protected in particular ways.

Intimately related activities such as fraud detection and prevention, data management, PCI DSS and data privacy are often still siloed, with professionals in each discipline admitting they rarely interact with each other.

And security professionals either explicitly rejected or simply did not understand the idea that cybersecurity was just another form of operational risk management, to be prioritised, analysed and managed like other, often more significant, risks.

All this must change.

First, cybersecurity must lose its exceptionalist mindset. Cyberthreats are generally not existential. Losses are survivable. Risk does not have to be reduced to zero.

Second, cybersecurity needs to be integrated into normal operational risk management and business continuity planning and it needs to operate according to standard risk management practices.

Third, cybersecurity must enable and secure the data centralisation, analytics and visibility required to deliver truly digital services.

And last but not least, in digital companies, cybersecurity must be integrated into the anti-fraud effort where previously both organisation and corporate culture have meant that these efforts often rarely collaborate.

In short, a new level of business orientation and rigour is needed to shape a new era of cybersecurity. The effects on CISOs, their staff and the entire function will be profound.

The end of cyber-exceptionalism, the start of cyber-transformation

AKJ Associates
In this era of DX & Convergence end-users need your help ...

1. To move data and security off-prem

Most companies cannot afford the time or staff to develop complex on-prem IT and security. Those who can would rather not – the costs and difficulty of keeping up with technology change are too high. This is your opportunity to show how you can help.

2. To connect security, fraud and data management silos

Most fraud these days is digitally-enabled. So why do fraud and cybersecurity departments regard themselves as separate? Can holistic solutions help to change this? Use the e-Crime Congress to showcase your solutions.

3. To create true cyber risk management

Boards understand that cybersecurity is just another enterprise risk to be managed. They want it run like other risks by people who understand the business not just narrow technology risks. Are you in the risk management business?

4. To secure partner ecosystems

Digital companies increasingly rely on complex webs of suppliers and partners, exchanging ever larger amounts of sensitive data. The third-party security problem is getting bigger. How do standalone security solutions help with this?

5. To secure increasing IT automation

Companies are automating everything from FX trading to cash management and procurement. As RPA replaces people, what are the security implications? Has the cybersecurity marketplace come up with solutions for this new paradigm?

6. To reduce the costs of cybersecurity

Many organisations cannot afford in-house SOCs or security teams big enough to guarantee continuous compliance let alone security. So do they outsource accountability and is automation one answer? What can you offer?

https://akjassociates.com/event/congress
They are looking for solutions in ...

Adapting to the changing threatscape
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. Which endpoint protection platform (EPP) vendors can do all this?

Defining data, dealing with data
Ask most companies what their core problem is in the digitalization era and it is not security, it is data. What do they have? What is its value? Can they reduce their data footprint to reduce risk? Can they aggregate, analyse and secure what is left? And can they reduce organizational risk exposure to the General Data Protection Regulation (GDPR) and other privacy regulations?

Solving the problem of privileged access
It should be a basic security requirement: applying the appropriate controls to privileged accounts is a critical defence against a key hacker vector. The difficulty is ensuring this across on-premises, hybrid and cloud environments without disrupting those who need that access. The best solutions allow a dynamic and risk-based approach to access.

Next generation threat and vulnerability management
It’s easy for security teams to be overwhelmed by threat intelligence. And even if they can digest the threatscape they cannot immediately patch every single single vulnerability. So they need solutions that allow them to isolate the risks that pertain most to them, and to remediate those, rather than trying to pursue a fix-everything policy that will disrupt the business and prove unsustainable from a cost perspective.
March 3\textsuperscript{rd} 2020
Key themes

Session 1: Digital transformation

- What does digital transformation mean for data, for silos and for cybersecurity?
- Does securing the digital enterprise imply the transformation of cybersecurity?
- Once boards wake up they want answers, metrics and the personnel they trust to deliver. Can they get them?

Session 2: Convergence

- Why is cybersecurity so siloed? As it becomes more integrated into operational risk management what does it mean for CISOs?
- How can fraud and cybersecurity be integrated to provide a better defence against the attacks that cost the most?
- Compliance failure and data loss is now a material P&L hit. What does this mean for security/compliance convergence?

Session 3: Cloud

- Cloud: customer error causes most Cloud breaches. How can using CASB / CSPM help?
- The more providers, the more breaches. Why would anyone go multi-cloud?
- The top five problems with hybrid cloud: why are we making the same old mistakes?

Session 4: The Internet of Things

- Digital enterprises’ attack surfaces will increase dramatically with the IoT. Is this the tipping point?
- 24/7 and always on, IoT devices are a security headache. What are the best approaches to securing them?
- Whose job is it to secure the IoT? Governments? Platform and system providers? Cloud providers?
March 4th 2020
Key Themes

Session 1: Talent, people and pay
- If cybersecurity is the place to be, why are so many CISOs moving on? Why do cyber recruiters and make so little money? Why do vendors struggle for clients?
- Will accountability change the role of the CISO – or make it redundant?

Session 2: Solving the vendor conundrum
- Making sense of the vendor ecosystem: the right-hand quadrant is not a panacea.
- Who and how to choose: the perfect RFP, the six-month POC and still it’s anyone’s guess. Tips from the customers.
- How do you know they are secure: since most solutions are black boxes, customers don’t know how they work, let alone if they are safe.

Session 3: The technology tsunami
- Automation, virtualisation, deception technologies, micro-segmentation, machine learning – dozens of ‘new technologies’ all with their own unique claims. What do CISOs need to know?
- True AI is the preserve of tech titans with deep pockets. If it’s the future of cybersecurity, should we just wait for Google?

Session 4: Securing the digital nation
- Nation-state attacks are no longer a rarity. But who is equipped to defend against them?
- The IoT – an $11 trillion opportunity or a disaster waiting to happen? What are the public and private sector imperatives?
- Securing digital transformation, Fintech and the payments revolution
Why AKJ Associates? Why the e-Crime Congress?

For 18 years, the e-Crime & Cybersecurity Congress in London has been the most sophisticated, closed-door 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 the National Hi-Tech Crime Unit (NHTCU).
- 18 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 a must-attend event for senior information risk and security professionals from business and government in the world.
We deliver a focused selling opportunity

**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.

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

The perfect platform for solution providers to deliver tailored advice to the right audience

https://akjassociates.com/event/congress
Why do so many blue-chip vendors work with us? Real 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 attend the e-Crime & Cybersecurity 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 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

https://akjassociates.com/event/congress
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 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 at the end of the meeting

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

https://akjassociates.com/event/congress
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.

What our sponsors say about us

<table>
<thead>
<tr>
<th>Voltage security</th>
<th>Kaspersky</th>
<th>cigital</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-Crime Congress continues to be the place for us to meet high caliber delegates and our security peers. We will be back!</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>