8th Annual e-Crime & Cybersecurity Benelux

6th December, 2018, Amsterdam

Transparency plus transformation: the cybersecurity rubicon

As security finally makes it to the top table of business risks, what now for CISOs?

e-crime & cybersecurity BENELUX

www.akjassociates.com/event/europe

AKJ Associates

e-Crime & Cybersecurity Benelux 2018: introduction

As business moves increasingly to digital channels across Europe, fraud attempts and other cyber-enabled economic crime are rising sharply. And recent research has shown that as well as increasing volumes, there has been an evolution from short, isolated peaks of fraud attacks to more sustained, high-volume attacks across a number of days or even weeks.

Of particular concern is the rise in identity spoofing, the result of the easy availability of stolen personal data now available on the Dark Web.

In addition, digital transformation is moving increasingly to mobile, rather than desktop online, channels. In Europe, 58% of all transactions now come from mobile devices and growth is accelerating.

These trends pose a huge challenge for business and for cybersecurity professionals. Businesses need to go digital and to make digital channels as seamless as possible for their customers. But they also need to keep those transactions, and their customers' personal data, secure. Cybersecurity is therefore a strategic business imperative.

As well as the need to dramatically strengthen cybersecurity to support digital transformation, businesses also need to respond to the post-GDPR environment of mandatory breach notification.

One of the unspoken truths of cybersecurity has been that businesses have been able to avoid most of the negative consequences of data breaches and loss, and therefore most of the need to invest in better security, because they have been able to simply hide their problems.

The huge volumes of personal data available on the Dark Web are a testament to those failures as are the increasing number of announcements relating to historical data losses.

This secrecy, and the resulting lack of consequences, is now gone. Business leaders will be confronted with the full reputational and business effects of any cybersecurity lapses and as we have seen with the recent Ticketmaster breach, security is also becoming a matter of competitive advantage: in an ecosystem of business relationships, the first to notify may actually gain reputation, while those who delay increase the damage they do to themselves.

It has been a long time coming, but these two core business drivers mean that cybersecurity will finally begin to be treated as a serious business risk management problem. As the costs of consumer and stakeholder reaction become clearer, and as smart businesses begin to compete directly or indirectly on security, budgets will rise.

e-Crime & Cybersecurity Benelux 2018 will look at these key developments. Do they mean CSOs and not CISOs are the new risk masters? Does digital transformation make IDAM the critical competence? And what about AI and blockchain?

e-Crime & Cybersecurity Benelux 2018: key themes

Key Themes

Cybersecurity as operational risk management
- Making cyber part of existing operational risk processes
- Getting buy-in from the CFO
- CISO versus CSO? Governance versus security?

Is acceptable 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

Cybersecurity solutions: a problem of 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 'normal company'
- 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?

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

The merger of physical and cybersecurity
- 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?

Why threat intelligence is the key to real security
- The importance of threat intel in budgeting for cyber risk
- Matching threat intel with vulnerability assessment
- Getting solution providers to work together

Does anyone take 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

Demonstrate your solutions

End-users and security professionals 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 the alert tsunami

SIEM systems are smart, but they're expensive, noisy, they require highly-skilled staff and alerts without context are not that useful. They can be hard to set up and reporting can be inflexible. **Can your products help?**

3 To innovate in identity management

Low friction transactions are critical but so is fighting fraud. New ways to use consumer data and behaviour to build identity and AI look like the way forward. **How can you help CISOs with IDAM and anti-fraud?**

4 To better utilise threat intelligence

Cybersecurity spending should be tailored to the threats and vulnerabilities specific to a particular organization. Smarter threat intelligence allows CISOs to map the threatscape to their specific vulnerabilities and invest appropriately. **Can you help?**

5 To build better faster SOCs

Speed of detection and remediation is the biggest single driver of risk (and loss) reduction in cybersecurity. So how can CISOs improve the speed of their SOC or other security processes. **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 around …

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 implement, 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 Benelux

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.

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 and most sophisticated buying audience in the cybersecurity market.

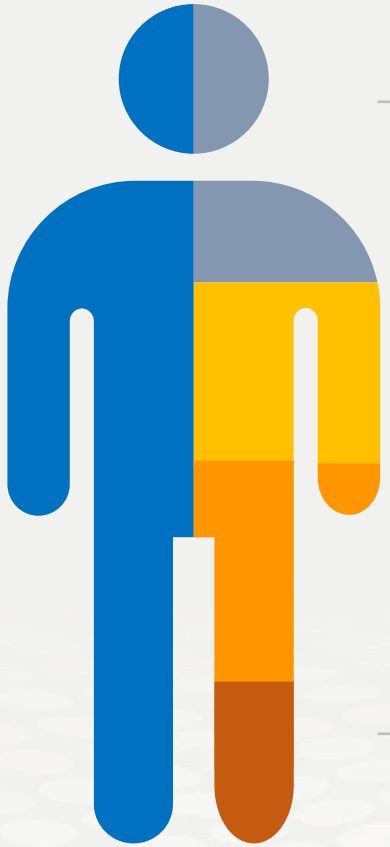
AKJ Associates has been building relationships with senior information risk and security professionals since 1999 and our cybersecurity community is the largest of its kind globally.

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 and Engineers who so often dictate the purchase process.

All of these job titles attend the e-Crime Benelux event.

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

We have a 15-year track record of producing the events cybersecurity 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

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 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 are senior within their organization and have procurement authority

Get your message across

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

Our testimonials speak for themselves: we have many more

What our sponsors say about us

TESSIAN

An impeccably organised event with all the right people, genuinely interested in learning about new solutions. AKJ events definitely give you the opportunity to leave a mark on your attendees.

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!

eset

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