13th e-Crime Germany

18th June, 2019, Munich

Ensuring digital autonomy

Securing business inside insecure states

e-crime & cybersecurity GERMANY

http://akjassociates.com/event/germany

AKJ Associates

Maintaining digital self-determination

"Illegal knowledge and technology transfer ... is a mass phenomenon," says Thomas Haldenweg, deputy president of the BfV domestic intelligence agency.

The ultimate aim of cybersecurity is to ensure that business and government maintain the ability to operate as they wish in the digital era.

For the private sector, digital autonomy means being able to rely upon the state for protected infrastructure and defence against state-to-state threats, and being able to trust that providers of digital products and services are themselves secure. This challenge is different in different sectors: securing e-Commerce for a retailer may mean a focus on mobile. Securing industrial control systems at an engineering firm or within critical infrastructure can mean a focus on peculiar legacy code and hardware.

For the public sector, security is largely a matter of ministerial-level recognition of the seriousness of the issue and the consequent levels of investment in people and infrastructure as well as a willingness to confront large technology providers over their cybersecurity stance.

Ensuring business continuity and autonomy through the transition to a digital economy is critical, and yet too often cybersecurity is viewed as a secondary consideration after "business" objectives: how often does the CFO mandate a move to the Cloud on the basis of cost-cutting, without costing the loss of control, autonomy and security such a move may entail?

The challenge, then, is the prevention of core operational losses and to defend the foundations on which companies are built. And this is where there has often been a disconnect between traditional, siloed cybersecurity operations and companies' business and financial centres. This disconnect is a two-way street, but it has not been helped by some of the key mantras of cybersecurity which can imply that failure is inevitable and that, no matter how much is spent, a crippling attack is certain: not the message other risk management functions routinely trumpet.

So how can companies build cybersecurity processes that focus on the most important business outcomes? How can cybersecurity integrate with existing risk management infrastructure and in what ways is it similar/different? And how can cyber professionals better understand the P&L impacts of key risks and mitigation techniques in order to better present tactical and strategic options to their boards and the leaders of their business units?

e-Crime Germany will cover these and other key subjects for its audience of professionals tasked with safeguarding digital assets and sensitive data. There will be real-life case studies, strategic talks and technical break-out sessions from security teams behind some of the world's most admired brands, who know, just like you, that security is now more important to business than ever.

Addressing the critical issues

Companies need cybersecurity advice and solutions tailored to their discrete circumstances. But this advice, and these solutions, also need to reflect the business realities they face and the concrete demands their clients are making today. So this edition of e-Crime Munich 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 profesionals 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 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 Congress Germany

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 buying audience in the cyber-security market.

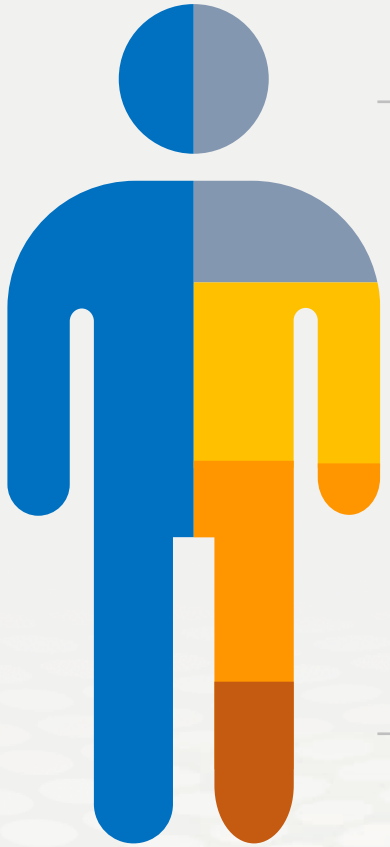
AKJ Associates has been building relationships with senior information risk and security professionals since 1999 and our cybersecurity community is the largest of its kind globally.

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 Germany.

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

http://akjassociates.com/event/germany

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.

http://akjassociates.com/event/germany

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.