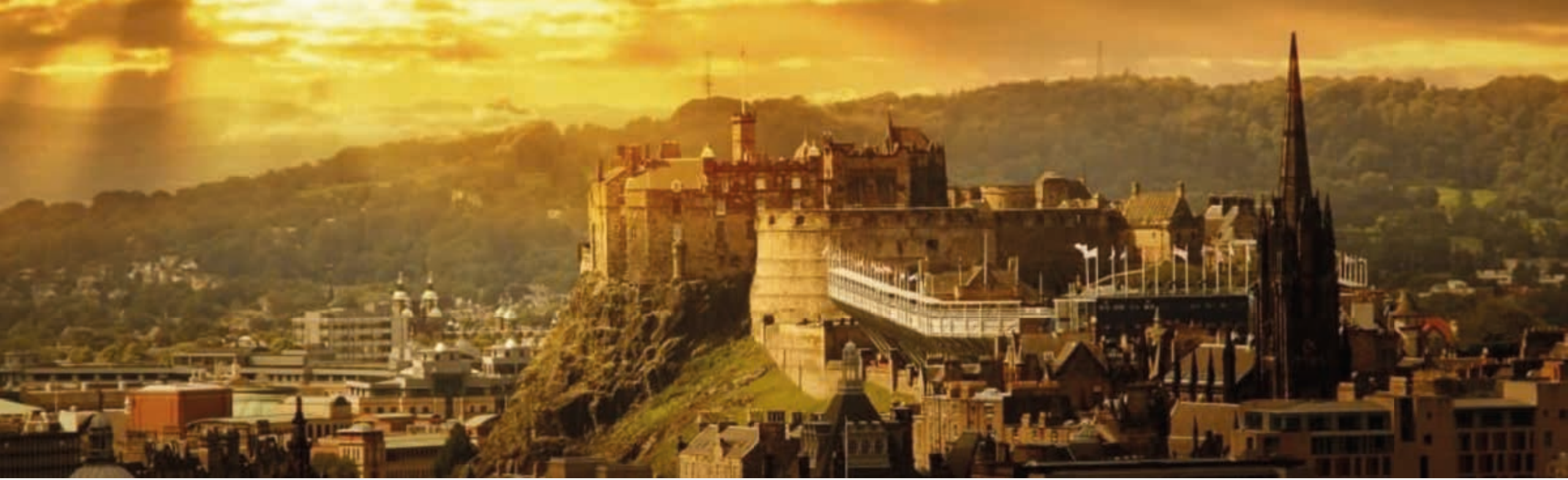


2nd e-Crime & Cybersecurity Congress Scotland

6th November, 2019, Edinburgh

Protection versus privacy: getting data right

As GDPR fines start to bite, does privacy trump protection? And is the CISO in the loop?

AKJ Associates

GDPR fines changing the game

e-Crime & Cybersecurity Scotland 2019
building holistic security and privacy

"A really wonderfully organised event with a great turnout and great programme," *Scottish Police*

Is security more or less important than early fraud detection? More or less important than making the consumer recovery process from fraud and data breaches easier? More or less important than keeping data safe from authorised access rather than unauthorised?

Cybersecurity professionals, and the senior managers who decide security budgets, have wrestled with these questions over the past 20 years, and, if the current state of cybersecurity is evidence, the answer is that security concerns have indeed been largely subservient to processes that ensure public, consumer-oriented losses are rectified. If the public does not lose money, everyone seems to accept current levels of data loss and cyber-insecurity.

The latest, largest GDPR fines change this calculus. The regulators at least have determined that the authorised misuse of data is worthy of a fine in the tens of millions of euros and that the inadvertent loss of data can cost those who lost it seven figure sums.

These fines, finally, give the business world what it needed: a way to calculate the materiality of data protection and data privacy and to suggest the levels of budgeting appropriate to the newly measurable risk.

But where should any new money be spent? GDPR is notionally focused on data privacy, and security professionals have long distinguished between data protection (securing data against unauthorized access) and data privacy (managing authorized access — who has it and who defines it). This has led to the assertion that data protection is essentially a technical issue, data privacy a legal one.

The GDPR fines render this distinction philosophical rather than practical: data privacy is compromised both by technical failures in data protection and by failures in data management ethics or processes. Regulators are therefore penalising both. The common denominators are data management in the broadest sense and the consumer. **So who is responsible for what? And what should end-users do now?**

GDPR's super-fines change the cybersecurity calculus. This year's e-Crime and Cybersecurity Congress Scotland will convene to discuss the latest problems and solutions.

https://akjassociates.com/event /scotland

AKJ Associates

Demonstrate your solutions

End-users need your help …

1 To solve the basic issues around data breaches

The fines make it official: the core technical issues cybersecurity professionals have known about for years must now be fixed. What are the critical problems? What are the priorities? **This is your opportunity to showcase your answers.**

2 To prevent known vulnerabilities leading to breach

Most data breaches are the result of vulnerabilities identified long ago and usually patched. Yes, the patching process can be complex and interrupt business so **show how your products can help users do this.**

3 To properly manage privileged user accounts

Data privacy and data security both rely upon the proper management of privileged accounts. How do the different requirements of privacy and security affect this? And **how can you help CISOs here?**

4 To secure Cloud and SaaS infrastructure

Who is accountable for the Cloud? As companies move applications and data into the Cloud, cybersecurity increasingly means ensuring the integrity of those Cloud-based operations. **How do standalone security solutions help with this?**

5 To manage data privacy issues proactively

Data privacy can now potentially result in larger fines than any other form of security incident. But managing privacy is more complex than putting technology in place against hackers. **Which solutions are available, scalable and easy to implement?**

6 To build more secure applications

So far the perceived benefits of insecure applications seem to outweigh the perceived downsides. With digital transformation, AI, and the IoT, insecurity's effects become more profound and potentially dangerous. **What can you offer?**

Demonstrate your expertise

They are looking for solutions in …

Fraud

Getting rid of silos

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?

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?

Artificial intelligence

Much ado about nothing or the only solution?

True artificial intelligence – in its guises of machine learning, deep learning, neural networks and so on – is extraordinarily complex and difficult. It is a work in progress and tends to be the preserve of those with the deepest pockets – governments or a handful of tech giants, such as Google and Facebook. So are the statistical models at cybersecurity vendors AI? More importantly, what is the proof they identify and nullify threats better than the alternatives?

Behavioural analysis

A different approach to the issue of us

A system designed to pick up unusual patterns of employee activity identifies a potential terrorist. Further investigation reveals that in fact the employee was considering suicide. The system was actually designed to alert companies to cybersecurity risks through behavioural analysis. This example shows that perhaps the best way to solve the core problems in cyber is to pay more attention to the things we do when we are simply getting on with the job.

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 Scotland

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.

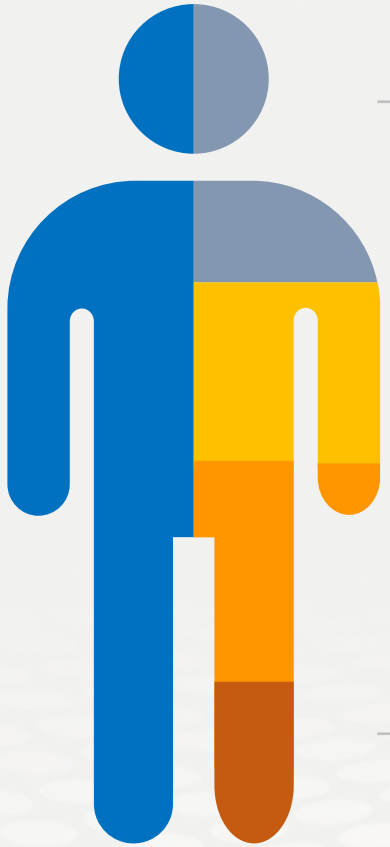
AKJ Associates has been building relationships with senior information risk and security professionals since 1999 and our cybersecurity community is the largest of its kind globally.

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 attend the e-Crime & Cybersecurity Congress Scotland.

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 a 15-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 /scotland

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 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

Our testimonials speak for themselves

What our sponsors say about us

Voltage security

e-Crime Congress continues to be the place for us to meet high caliber delegates and our security peers. We will be back!

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.

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.

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