SECURING THE LAW FIRM

July 3rd, 2024, London, UK

Legal sector vulnerability gets expensive

It should now be crystal clear to law firms that paying for better security makes good business sense

SECURING THE LAW FIRM

The costs of insecurity are rising fast – is it time to invest more in people and tech?

The number of reported cyber attacks on UK law firms has increased 36 per cent over the past year.

According to data by speciality reinsurance group Chaucer, there were 166 reported cyber breaches in 2021/22, this number jumped to 226 for 2022/23 (as of 30 September).

The National Cyber Security Centre (NCSC) cyber threat report 2023 also noted that nearly-three quarters of UK's Top 100 law firms have been impacted by cyber-attacks.

Chaucer says that the large number of attacks against law firms has been driven by a belief amongst hackers that law firms are particularly vulnerable to ransomware attacks and threats from the hackers to publish information stolen online.

This is not just down to the extremely sensitive data that law firms hold on behalf of their clients, it's the hackers' near certainty that law firms will pay them to either unlock data they encrypt in ransomware attacks or pay "blackmail" in exchange for the hackers not publishing the law firm's stolen data online.

In one recent Magic Circle attack, the firm involved will not say whether it paid the ransom – but its data was not leaked by Lockbit.

The financial costs (and reputational and legal issues) associated with paying ransoms are just the tip of the iceberg when it comes to the costs of serious incidents.

As well as all the internal remediation costs, depending on the types of information lost, organisations will now probably have to endure regulatory inspections and fines, as well as class action lawsuits from damaged clients and other third-parties.

U.S. law firm Orrick, Herrington & Sutcliffe has just had to update the number of affected parties to its data breach last year. The pool of victims quadrupled between its July and December disclosures to more than 630,000. These victims lost data including personally identifiable information such as names, addresses, email addresses, dates of birth, Social Security numbers, driver's license numbers, passport numbers, financial account information, credit or debit card numbers and tax ID numbers. Health information was also stolen, including medical treatment or diagnosis information, claims information, health insurance ID numbers, healthcare providers, medical record numbers and account credentials.

The breach led to four consolidated lawsuits brought on behalf of hundreds of thousands of alleged victims of the breach and the firm has just announced that it has come to an undisclosed agreement to settle these suits. Clearly the cost will be extremely significant.

Orrick did not say how the threat actor gained access to its system or if it was extorted for a ransom. Lack of transparency is still a hallmark of the industry as few firms are listed.

So, what are the key challenges that Law Firms still struggle with? Are they more difficult to defend than other organisations? And does the scale and sensitivity of the data they hold mean they need to consider security measures unnecessary in other sectors?

Securing the Law Firm will look at the latest thinking around legal cybersecurity. As well as presentations from some of the world's largest firms we will also be asking how small and medium-sized organisations can keep up with cybersecurity best practice in the sector.

SECURING THE LAW FIRM

Key Themes

Re-thinking email and messaging: is there a better way?

From secure web gateways to clever tools designed to let employees flag suspicious emails, technologists have tried to solve the problem of email and message-delivered malware. And they've failed. This is still the number one vector for the cyber attacks that cause real damage. **Is there another way?**

Streamlining tools and information: focus on insight

No wonder cybersecurity teams are overwhelmed. To solve their problems they are told to add ever more tools to their stacks, ingest ever more internal and external data, and somehow aggregate all of that complexity to detect cyberattacks, determine risk metrics and all the rest of it. **So how to change the paradigm?**

Re-engineering the SOC: the problem of alert overload

One specific example of staff overload is the SOC: there are debates over the value of network traffic analysis and other data, but meanwhile SOC teams are flooded with false positives and even 'smart' solutions do not alter this calculus very much**. Is the answer to outsource or evolve?**

Fixing Cloud configuration

Cloud security is a multi-dimensional problem, but underneath all the technology and complexity, once again it is human error that is likely to cause the most material losses. For large firms with complex hybrid and multi-cloud environments, this problem is compounded. **So, what are the most common errors and how can they be avoided?**

Solutions for CISO burnout

CISO churn is astonishing. The number of security professionals on LinkedIn who've left without another job to go to is strange given the shortage of cyber-talent. So, what is going on? Are CISOs being fired for breaches? Are they quitting companies who've lied about their commitment to security? Or are they just getting out of the sector? **How can firms solve this problem?**

From awareness to behaviour

There's too much talk of awareness in cybersecurity and not enough talk about actually changing behaviour. There's too little talk of personal accountability and disciplinary enforcement of security policies. These are controversial statements but should they be? **Isn't part of the paradigm shift we need a fundamental change in employee responsibility?**

AKJ Associates

SECURING THE LAW FIRM

Key Themes

Ransomware – dealing with the new normal

The US Treasury reported that companies paid an estimated $5.2 billion in BitCoin transactions due to ransomware payments for companies in 2021, and only a quarter of ransomware attacks are reported. Ransomware is here to stay. **So how can CISOs stop it being a permanent tax on the business?**

From cybercrime to cyberwar

Blurred lines between cyber-spies, cyber-criminals and cyber-armies have transformed the (in)security landscape, with nation-state exploits widely available. **How can the various elements of government work better with private sector solution providers and end-users to build security that can cope with not-quite-nation-state attackers?**

NIS2 – changing the game in cybersecurity?

NIS2 expands the scope of who is included. It adds more regulations and divides the world into two tiers, each with different requirements. And it increases the personal liability of senior officers around cybersecurity failings. So how does this new regulatory environment change the cybersecurity calculus? **What do firms need to do now?**

Cloud incident response

Recent Cloud outtages have not simply disrupted low-level infrastructure, they have disabled cybersecurity solutions and, in turn, sometimes, shut down corporate access to critical network assets for significant amounts of time. **As well as managing Cloud security, CISOs need good Cloud incident response. How are they going about it?**

Managing insider threats at a time of crisis

When economies are under stress, employees too can find themselves in financial difficulty. When geopolitical tensions rise, people can take sides. Insider threats of various kinds become far more prevalent and dangerous at times like these. **So, how have security and other MIS tools matured to make detecting malicious insiders easier and more accurate?**

Embracing risk management

Until cybersecurity is truly seen as risk management and not a whack-a-mole IT problem, the hackers will continue to evade outmoded control frameworks. Quantification is key but so is how it is used. Part of this is down to CISOs, part of it to Boards and part of it to solution providers. **The banks have done it. When will the rest of business catch up?**

AKJ Associates

We deliver your message direct to decision-makers

SECURING THE LAW FIRM

Plenary Speakers

The e-Crime Congress Series events offer sponsors the opportunity to deliver content in a number of different ways.

Plenary speakers **deliver their presentations on the day of the event from a fully featured AV stage to a face-to-face audience**.

Their presentations can contain slides, video and audio and speakers can deliver their speeches from the podium or from any point on the stage.

Plenary presentations are 20 minutes long and take place in the main event auditorium guaranteeing access to the largest possible audience of cybersecurity professionals on the day.

Presentations are generally designed to be informative, topical and actionable, with the use of case studies and up-to-the-minute references to current developments.

Double-handed talks with clients are also welcomed.

Education Seminars

At pre-defined points in the day, attendees will be notified that the main plenary sessions are making way for a series of in-depth technical break-outs.

These sessions of up to 30 attendees are held in break-out rooms and delivered live to attendees.

They are an opportunity for vendors to deep-dive into a topical problem, technology or solution in front of a group of cybersecurity professionals who have self-selected as being interested in the topic being discussed.

They are also the ideal venue for solution providers to go into technical detail about their own products and services.

These Seminars run simultaneously, and attendees choose which session to attend.

At the end of the Seminar, attendees are notified that Networking time is now available before the next Plenary session.

Your team and your resources available in real-time

SECURING THE LAW FIRM

Exhibition Booths

Sponsor packages that contain an Exhibition Booth give sponsors the opportunity to be present in the main networking area of the event.

At these booths, sponsor representatives can interact with delegates face-to-face, deliver messaging and technical information via video presentations, demo products using their own BYOD technology and to distribute printed marketing and product information.

Sponsors may wish to consider different ways to drive footfall to their booths.

For example, sponsors who have presented in Plenary or in an Education Seminar can close their presentations by directing the audience to their booths.

And there are additional gamification elements available, including sponsor-supplied prizes, that can effectively drive traffic to booths.

Why AKJ Associates?

SECURING THE LAW FIRM

A History of Delivery

For more than 20 years, AKJ Associates has been running been the world's most sophisticated closed-door meeting places for senior cyber-security professionals from government, law enforcement, intelligence and business.

For example, our annual London-based e-Crime Congress is still **the largest invitation-only, Chatham House rules,** gathering of the most senior information risk and security professionals from business and government in the world.

The UK Home Office sponsored the public sector delegation from 40 countries in 2002 and we are delighted to say they still do today.

Global Engagement

We have run hundreds of events in the **UK, across Europe, the Middle East and Asia**, attracting **tens of thousands of delegates** in cybersecurity, data security and privacy.

These delegates range from C-suite CIOs, CTOs, CROs and C(I)SOs, to heads of enterprise architecture, desktop and network. They encompass all the senior professionals whose input drives security and privacy solution purchase decisions.

And as well as cross-sector events for both private and public sector, we also design and deliver sector-specific conferences for high-value, high-sophistication sectors including the legal sector, financial services and gambling and gaming.

Unrivalled Relationships

Events like this have enabled us to build relationships of trust with **the most influential decision-makers** at the full spectrum of public and private sector organisations in the UK, Europe, Asia and the Middle East.

By providing this audience with valuable insights and business intelligence over the past 20 years, we have built up **the world's most significant community of professionals in cybersecurity.**

We use this to develop new events; to conduct research to understand what cybersecurity professionals are doing, thinking and buying; and to market our conferences and other services.

Smart Lead Generation

We have also developed and trained one of the **most effective marketing and telemarketing operations** in the cybersecurity space.

Our in-depth knowledge of the marketplace allows us to design marketing outreach that **consistently delivers the best audiences** for the providers of critical cybersecurity infrastructure and solutions.

We connect vendors directly with B2B decision-makers. By combining unrivalled reach, deep knowledge of specialist markets and sophisticated marketing we **engage buyers to deliver real results.**

AKJ Associates

http://akjassociates.com/event/stlf

We deliver the most senior cybersecurity solution buyers

SECURING THE LAW FIRM

Our USP? We put buyers and sellers together

We understand that every vendor needs to sell more. That is the bottom line. This is even more necessary in the present situation.

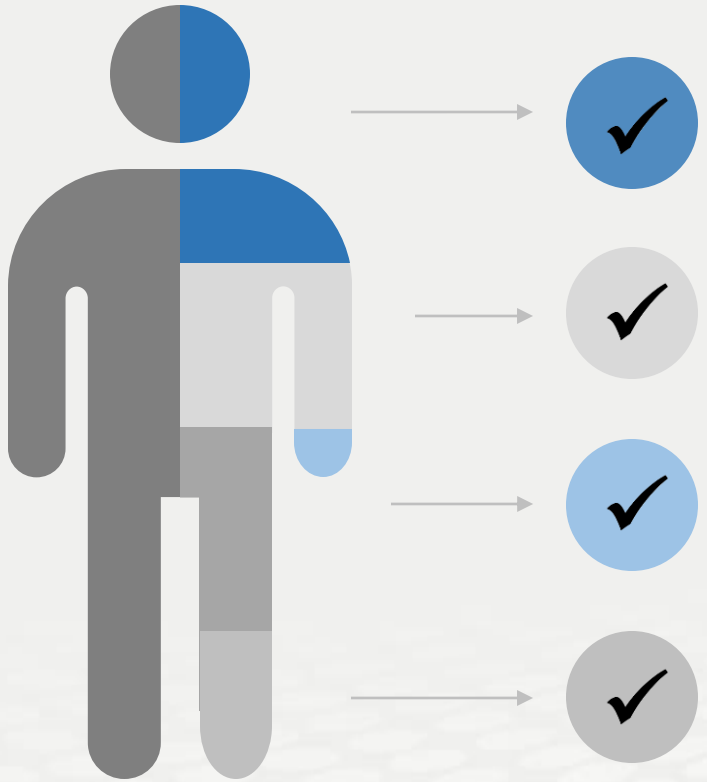
You will have access to the most senior buying audience in the cyber-security market.

AKJ Associates has been building relationships with senior information risk and security professionals for 20 years 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 e-Crime & Cybersecurity Congress events.

Getting access to the right people at the right time always increases the lead generation and always increases profitable sales activity.



Cyber-security
We have a 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

We deliver the most focused selling opportunity

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

SECURING THE LAW FIRM

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.

SECURING THE LAW FIRM

Delegate Acquisition

- The e-Crime & Cybersecurity Congress has the **largest community of genuine cybersecurity stakeholders** to invite to our events.
- Our reputation for hosting **exceptional events with informative content, excellent networking opportunities and the best vendor partners** means delegates know they are attending a quality event, and are willing to give up the time to attend.
- Our delegates are **invited by an in-house delegate liaison team** who call senior security and privacy professionals at public and private sector companies with a personal invitation to attend
- We **follow up all registrations** with further calls, emails on logistics requirements and reminders to **ensure the best possible attendance**.

Lead Sourcing

- The e-Crime & Cybersecurity Congress prides itself on **putting the key cybersecurity buyers and sellers together**
- To offer you the best prospects to network with, **we don't invite academics, job seekers, consultants,** non-sponsoring vendors or marketing service providers to this closed-door event. This **attention to quality over quantity** has been the hallmark of AKJ's events for 20 years.
- Each of our vendor partners will receive a delegate list at the end of the event.
- Through our targeted networking breaks built into our agendas you will have **unrivalled opportunities to network** with high-quality prospects with face-to-face networking at the event.

Get Your Message Across

- **Content is king,** which is why the e-Crime & Cybersecurity Congress prides itself on delivering informative and useful content, to attract senior audiences of decision-makers.
- Deliver an exclusive 20-min keynote presentation in the virtual plenary theatre, or host a 30-min targeted workshop session: good content drives leads to your booth, and showcases your company's expertise
- AKJ's in-house content / research team will complement the agenda with best practice from leading experts and senior security professionals from the end-user community
- If you are not presenting, the exhibitor booth offers the opportunity to share white papers and other resources for delegates to takeaway

Exclusivity Delivered

- AKJ Associates has never done trade shows. We see most value in working with **a select number of the top vendor partners**, and offering those companies the best access to leads.
- Our events keep the same ethos as when we first started 20 years ago, limiting vendor numbers. We will not be a hangar with hundreds of vendors competing for attention. We will keep our **events exclusive to give the best networking opportunities**.
- All booths offer the same opportunities with the same capacity and functionality regardless of the vendor company.
- This is an opportunity to **continue building pipeline and driving leads** in partnership with our outstanding 20-year reputation and the e-Crime & Cybersecurity Congress brand.

What our sponsors say about us

SECURING THE LAW FIRM

PhishRod

It was indeed a great show. Despite the situation overall [COVID 19] the number of people that turned up, shows the trust people have of the e-Crime brand. Wish you all the best for the upcoming events and we shall surely be a part of them.

KASPERSKY lab

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.

vmware Carbon Black

AKJ has been a valuable partner for us for a few years now, enabling us to build relationships and engage with the CISO community in a number of key territories across Europe. The events they hold are a great vehicle for discussing the latest challenges and opportunities in the security sector, and our work with them has delivered way beyond expectations.

✓**Ninety five percent of our exhibitors and sponsors work with us on multiple 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**

AKJ Associates