Securing the Law Firm

January 19th, London, UK

The perfect storm for legal cybersecurity?

Legal firms face an existential shift that some may not survive. Securing the new business model will be tough.

AKJ Associates

http://akjassociates.com/event/stlf

Is the legal sector becoming uninsurable? Time to get serious and spend

Over the past eighteen months the legal sector has become the most instructive case study in cybersecurity.

Luna Moth (also called Silent Ransom Group) has been extorting top-tier US firms with social engineering rather than malware: fake IT-support calls and, since 2025, people physically turning up at offices posing as IT contractors and plugging in storage devices. The FBI confirmed the physical-intrusion tactic in May 2026.

It's good business. Insurance-funded suppression payments, rational for each firm, have taught criminals that law firms pay fast and pay big. Weil Gotshal paid roughly $18–20 million in May 2026, allegedly within three days of the demand; WilmerHale at least $18 million (with insurer CNA covering the primary layer) and Goodwin Procter around $10 million, both disclosed in August 2026. Jones Day reportedly refused a $13 million demand in April 2026.

On 5 September 2026, three more unnamed US firms were reported hit.

In the mid-market the failure mode is different: INC Ransom, does use exploits, is getting in through known Citrix, Fortinet and RMM vulnerabilities and probably through a shared supplier. Between them, that's the sector's problem in one sentence: the top end fails on people and process, the middle fails on basics and suppliers.

In the UK, nearly three-quarters of the top 100 firms report being affected, regulators have begun fining for missing basics such as multi-factor authentication, and the Law Society has issued fresh guidance.

This should not be happening. The FBI described this playbook in mid-2025; the largest payments followed a year later.

The sector has not learned collectively, for structural reasons: partnerships that resent friction, a billable-hour culture that treats security as unbilled time, historically thin security budgets (estimated at a mere 0.3% of fee income), and a confidentiality reflex that settles incidents quietly so no one else benefits from shared knowledge.

AI sharpens the attacker's best weapon: voice cloning makes impersonating a partner or the IT director cheap and convincing. At the same time firms are moving privileged material into AI review platforms, widening the supplier exposure already being exploited, while UK legislation on ransom payments and resilience is reshaping what firms are permitted to do.

Regulators and clients add urgency. The SRA and the ICO expect effective controls; financial-services clients push DORA-style third-party obligations down their supply chain; outside-counsel guidelines are turning into security audits; and cyber insurers ask harder questions at every renewal.

The fixes are largely unglamorous: verified identity at the help desk and front desk, control of remote-access tools, alerts on bulk data movement, supplier assurance, and a pre-agreed governance position on payment before the demand arrives. None of this is exotic; all of it requires partners to treat security as governance rather than an IT cost.

Securing the Law Firm will focus on the practical security architecture behind client trust: identity-first controls, secure AI adoption, document and collaboration security, ransomware resilience, third-party risk, exposure management and recovery.

Through practical case studies and closed-door peer discussion, Securing The Law Firm Services will look at what the legal sector needs to do to

Key Themes

Agents at work: identity and access for AI acting on lawyers' behalf

CISOs must rethink core identity and governance frameworks, including the adoption of robust agent identity models (spanning machine, service, and workload identities), and clearly defined delegation structures that determine what authority an agent holds and who grants it. **What technologies can help them maintain visibility and control?**

The partner's voice: deepfakes, vishing and real-time verification

Voice cloning is now cheap and convincing, and a culture of urgency and deference to seniority makes law firms fertile ground. Payment instructions, file transfers and access requests all need a second factor that synthetic media cannot supply. **What technologies can help firms verify people and instructions in the moment?**

Integrity and the AI-enabled supply chain

AI-native operating models imply dependence on a complex supply chain of foundation models, internal systems, and external APIs and orchestration layers that collectively produce legal work. Imagine the consequences of hacking such a system. **So how do CISOs stop that happening?**

The 72-hour challenge

A breach now triggers ICO notification within 72 hours, a report to the SRA, as well as insurer engagement. Firms need a playbook that runs the legal, regulatory and communications tracks in parallel. When should they do what – including call their clients? **What tools and services help firms respond, report and rebuild trust under pressure?**

The power of automation

There's too much manual intervention in security. SOAR pulls data from SIEMs, EDRs, firewalls, cloud APIs, ticketing systems threat intelligence feeds, and even email servers and coordinates actions across tools via APIs and prebuilt integrations and intelligent playbooks. **Well, that's the theory. How does it work in the real world?**

Dealing with regulations

CISOs now must build a single coherent security program that simultaneously satisfies divergent regulatory demands; they must interpret vague legal standards into technical architectures, and they risk non-compliance if auditors, regulators, or courts interpret differently later; they face unrealistic expectations around incident reporting; and they face personal liability. **Can RegTech help?**

Key Themes

Shared platforms and the MSP as single point of failure

One ransomware group listed ten law firms on its leak site within 48 hours, most likely through a shared practice-management platform or MSP. Mid-tier firms outsource most of their IT and inherit their suppliers' weaknesses. **How can firms gain continuous assurance over the vendors and platforms that now hold their most sensitive matters?**

Watching the data leave: detecting exfiltration early

In the most damaging recent cases nothing was encrypted; attackers simply copied client files to cloud storage. Spotting unusual document and data movement and unapproved remote-access tools is critical. **What technologies give firms real-time visibility of data moving across DMS, email and cloud?**

Coping with compliance: the burden increases

Banks, insurers and corporates now impose their own security requirements on the firms that act for them, while the UK's Cyber Security and Resilience Bill pulls managed service providers into scope. **What technologies help firms evidence compliance continuously rather than scrambling at every request?**

Keeping cyber cover, proving security

Underwriters are responding to claims with tighter sub-limits, co-insurance on ransom payments, and hard requirements for MFA, endpoint detection and backups. Cover is becoming conditional on evidence, not assurances. **What technologies help firms demonstrate their controls continuously and stay insurable on acceptable terms?**

Post-quantum readiness – it's real

Wills, trusts, patents and settlement terms must stay confidential for decades, longer than today's encryption is expected to survive a capable quantum computer. The NCSC wants organisations to look at cryptographic dependencies now. **What technologies help firms inventory their cryptography and begin the migration without disrupting practice?**

AI solutions to lean legal teams

Law firm security teams are small, but cyber risks are not, and AI now promises to triage, investigate and even respond without adding headcount. The same tools can hallucinate, over-block or quietly widen access, and a partner will not accept "the model decided". **Which AI-enabled technologies deliver measurable capacity for a small team, and how should their decisions be supervised?**

AKJ Associates

Why AKJ Associates?

SECURING THE LAW FIRM

A History of Delivery

For more than 25 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 & Cyber Security 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, manufacturing, retail, healthcare, CNI.

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 25 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.**

Delivering your message direct to decision-makers

SECURING THE LAW FIRM

Plenary Speakers

The e-Crime & Cyber Security 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.

Delivering 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 25 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 lead generation and always increases profitable sales activity.

Cyber-security
We have a 25-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

AKJ Associates

http://akjassociates.com/event/stlf

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 25 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 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 25 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 25-year reputation and the e-Crime & Cybersecurity Congress brand.

What our sponsors say about us

SECURING THE LAW FIRM

OneSpan

"Firstly, a big thank you for yesterday — it was a fantastic event, and we really felt it was a great success. The quality of the attendees was excellent; people were genuinely engaged and very open to conversation. We had strong interest at the stand throughout the day, with many visitors eager to learn more about our solutions."

Sales Manager UK & I

Recorded Future®

"Thank you for your email. I attended the event yesterday and have to say it was very well organised.

We were very happy with the turnout for our afternoon session as well - all in all, it was a very successful event!

Senior Marketing Executive

Red Helix

"AKJ are a pleasure to work with.

A lot of work goes into making physical events a success, and with AKJ the team are there to support at each step.

They ensure the events are a great success for both suppliers and end users alike."

Senior Digital Marketing Manager

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 our work with them has delivered way beyond expectations."

Senior Marketing Manager

95% percent of our exhibitors and sponsors work with us on multiple events each year.

This is because they generate real business at our events every year. Our sponsor renewal rate is unrivalled in the market.