e-Crime & Cybersecurity Congress Online Series: Healthcare

SECURING HEALTHCARE

e-Crime & Cybersecurity Healthcare Online

July 7th, 2026, Online

From data loss to care-delivery disruption

Cyber attacks in healthcare are no longer just 'data breaches'. They cause shut-downs and patient harm. What needs to be done?

AKJ Associates

https://akjassociates.com/event/health

e-Crime & Cybersecurity Congress Online Series: Healthcare

SECURING HEALTHCARE

Keeping healthcare safe

The Conduent data breach, discovered on January 13, 2025, has escalated into one of the largest third-party data incidents in U.S. history, with 25 million affected individuals. Attackers had unauthorized access to Conduent's systems from October 21, 2024, to January 13, 2025. The ransomware group SafePay (sometimes referred to as Safeway) claimed responsibility, alleging they exfiltrated 8.5 terabytes of data. The breach was traced back to compromised VPN credentials, which allowed hackers to encrypt internal systems.

Then there is Stryker, one of the world's largest medical technology companies with approximately 56,000 employees, $25.1 billion in revenue for 2025, and products that impact more than 150 million patients annually. Attackers used Microsoft Intune and a compromised admin account to remotely wipe 200,000 devices. The real-world impact was immediate. Maryland's emergency medical services reported that Stryker's Lifenet ECG transmission system, which paramedics use to send cardiac data to hospitals ahead of patient arrival, went offline.

These are just two of a series of really significant healthcare hacks that have occurred or been announced in just the first three months of 2026. Hackers are targeting primary care providers, third-party / back-office suppliers (like Conduent), managed care providers/claims management companies like Sedgwick – essentially the entire healthcare supply chain. CareCloud, Waterloo Regional Health Centre, IntraCare, the list goes on.

So, what are the lessons from these attacks and what should healthcare security leaders be focusing on right now? These are just some of the key takeways:

- **Stop living off the land:** organisations need much better systems for detecting bad actors once they have gained access and more sophisticated ways to find unusual activity. Aso, detection is not enough: detection must trigger policy-mandated actions.
- **Enforce phishing-resistant MFA:** Many admin accounts still lack proper Multi-Factor Authentication (MFA), providing an easy entry point.
- **MDM/UEM platforms are hacker's biggest prize: u**nified Endpoint Management (UEM) platforms like Intune have near-total control over endpoints. If compromised, they can be used to wipe machines, distribute fake data, or push malicious configurations at scale.
- **Bulk action controls:** implement controls that prevent or flag bulk actions (like wiping 200,000 devices).
- **Dual authorization:** require multi-admin approval for high-risk actions such as device wipes, retirements, or deletions.
- **Third-party risk is just risk:** your vendor risk is your risk. 98% of organizations globally have relationships with at least one breached third party. This breach confirms that attackers are actively targeting contractors to reach high-value targets. Organizations must view their security posture as inseparable from that of their vendors.
- **Isolation is not foolproof:** the incident showed that "isolated" network segments can still be compromised, meaning segmentation controls should be regularly tested and verified rather than assumed secure.
- **Data retention policies need review:** some breaches included data dating back to 2017–2019, emphasizing that holding outdated, sensitive data for too long increases risk.
- **Contextualize "low-risk" findings:** minor security findings can, when paired with factors like phishing or, as seen here, unauthorized access to a specific module, turn into critical breaches.
- **Encryption at rest and in transit is insufficient: a**ttackers are targeting data while it is in a "clear" state—being actively processed—meaning organizations must protect data during use.
- **Implement Zero Trust:** the incident reinforces the need for a "Zero Trust" approach, where no entity inside or outside the network is trusted, and continuous verification is required.
- **Prioritize resilience over trust:** In a 2026 landscape where breaches are common, firms must shift from hoping for stability to designing for failure.
- **Compliance is not enough:** the healthcare sector is a prime target for breaches because it handles high-value data. Organizations must move beyond mere compliance to proactive security strategies.

It's a long list, and it doesn't even include IT/OT, AI-enabled offence/defence, or the need to reduce security complexity and the need to create real visibility across the whole security technology stack to be able to detect and stop modern attacks that use legitimate credentials and standard network tools.

That's why we are running the e-Crime & Cybersecurity Healthcare Summit. To give you a chance to hear your peers in the industry talk about what they are doing now to improve their security posture, and what worries them most about the current threatscape.

Join us with your perspectives and help us make the healthcare sector a safer place for employees and patients.

The e-Crime & Cybersecurity Healthcare Summit will take place online and will look at how cybersecurity teams are tackling the latest challenges. Join our real-life case studies and in-depth technical sessions and help make manufacturing secure.

https://akjassociates.com/event/health

AKJ Associates

e-Crime & Cybersecurity Congress Online Series: Healthcare

SECURING HEALTHCARE

Key Themes

Achieving visibility across ecosystems

From exposed initial access points such as warehouse management systems to complex machine control software, simply understanding your device and application landscape is a huge challenge. **Can you help with asset tracking and endpoint visibility? And what about anomaly detection after that?**

Defending against the latest ransomware variants

Ransomware is effective precisely because it can exploit whatever weaknesses exist in your security architecture and processes. The threat and the actors are constantly evolving and that evolution is forcing the hands of government and causing havoc in the insurance market. **What can CISOs do to better defend against ransomware?**

Why zero trust, isolation and segmentation are key

Retail ecosystems now include logistics APIs, fintech integrations, marketplace sellers, social-commerce platforms and SaaS pricing engines. Each connection expands attack surface. **Continuous third-party risk scoring, API security testing, software bill of materials (SBOM) validation and zero-trust segmentation become foundational, not optional.**

Data integrity a critical priority

In AI-powered retail, corrupted data equals corrupted decisions. Pricing engines, demand forecasts and recommendation systems are only as trustworthy as their inputs. **CISOs must prioritise data lineage tracking, tamper detection, pipeline validation and cryptographic integrity controls across analytics and AI workflows**

Securing Agentic AI

Agentic systems don't just generate content — they act. CISOs must address model manipulation, prompt injection, data poisoning, tool-chain abuse and privilege escalation within AI agents executing transactions. Governance must extend beyond ML pipelines into runtime controls, behavioural monitoring and kill-switch design

From Analysts to AI Supervisors

Retail security teams cannot scale headcount at the pace of digital transformation. The future SOC blends automation engineers, detection scientists and AI risk specialists. **Peer collaboration, shared intelligence and trusted industry forums become force multipliers in defending fast-moving retail environments.**

AKJ Associates

e-Crime & Cybersecurity Congress Online Series: Healthcare

SECURING HEALTHCARE

Key Themes

Making the best use of threat intelligence

In a preemptive security model, timing is everything — success depends on detecting and neutralizing threats before they become active incidents. To do this, security operations can't just rely on internal telemetry (e.g., endpoint or network logs). They need external, real-time context about emerging threats — **where do they get it?**

Improving continuous attack surface discovery

You need to know what attackers can see and what they can actually attack – and you need it on a continuous basis, not in some static inventory. Ideally you also need assets ranked by risk priority and put into the current threat and vulnerability context. **Is this feasible and is it cost effective?**

Adversary simulation and behavioural analysis

Automated adversary simulation
Identifies telemetry blind spots. They provide prioritized remediation guidance and control effectiveness metrics. They track progress trends and validate security ROIs as well as providing board and audit reporting.
How well do they work in practice?

Security Posture Management

Traditional vulnerability scanners don't handle cloud native architectures well.
Today's cloud environments spin up thousands of ephemeral assets without a traditional OS, without an IP address for long. **So how do you adapt to that dynamic, API-driven reality? How can traditional tools connect the dots – not just generate tickets?**

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?**

AKJ Associates

Why AKJ Associates?

SECURING HEALTHCARE

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 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 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.**

https://akjassociates.com/event/health

AKJ Associates

Why the e-Crime and Cybersecurity Online Series?

SECURING HEALTHCARE

The challenge: end-user needs are rising, solution providers' too

Our end-user community of senior cybersecurity professionals is telling us that they face a host of new threats in the post-pandemic environment, to add to their existing challenges.

Remote working and an increased reliance on Cloud and SaaS products are all putting organisations across the world under even more strain. **They need cybersecurity products and services that can solve these issues**.

In addition, the post-COVID environment has created groups of cybersecurity professionals who are less willing or able to attend physical events, and yet these groups still demand the latest information on security technology and techniques.

At the time solution providers are finding it ever more difficult to build relationships in an increasingly competitive environment.

Economic and business drivers are making CISOs more selective and pushing them away from large security stacks and multiple point solutions.

To sell to this increasingly sophisticated community, vendors need multiple access points to engage security professionals, to build deeper relationships and maintain those relationships throughout the year.

To cater to all of the different sectors of the market, this means an increasingly varied palette of communications.

Therefore, **in response to many requests from our community** for us to continue to deliver best practice advice and to give them the up-to-date technical case studies and content they need to cope in the current environment, **we are adding to our traditional physical services.**

The e-Crime & Cybersecurity Congress Virtual Series will offer virtual versions of our key upcoming events and will deliver great **opportunities for lead generation and market engagement**.

Maintaining the ethos and quality of our physical events we will continue to offer **unrivalled partnership opportunities to cybersecurity vendors** looking to build strong, engaged relationships with high-level cybersecurity professionals.

e-Crime & Cybersecurity Congress Online Series: Healthcare

SECURING HEALTHCARE

Delegate Acquisition

- The e-Crime & Cybersecurity Congress has the **largest community of genuine cybersecurity stakeholders** to invite to our events.
- 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** is the case for our online offering.
- **Each of our vendor partners will receive a delegate list at the end of 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 online plenary theatre: good content drives leads and engagement post event: showcase your company's expertise
- AKJ's in-house content / research team will complement the agenda with best practice from senior security professionals from the end-user community

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 online events keep the same ethos, limiting vendor numbers. We keep our **online congresses exclusive and give you the best networking opportunities**.
- This is an opportunity to **continue driving leads** in partnership with our outstanding 25-year reputation and the e-Crime & Cybersecurity Congress brand.

Delivering the most senior cybersecurity buyers

SECURING HEALTHCARE

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.

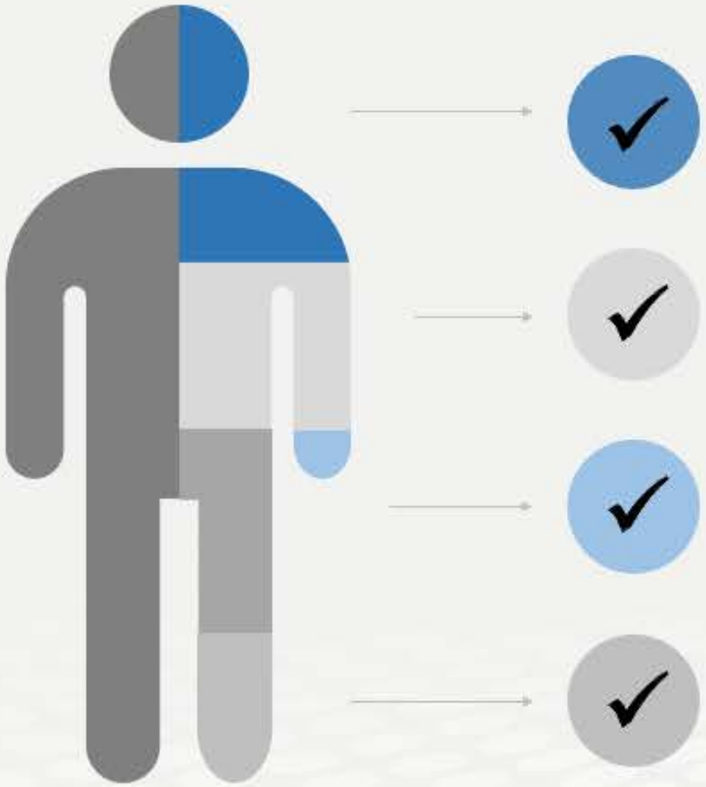
You will have access to the most senior buying audience in the cyber-security market.

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 the lead generation and always increases profitable sales activity.



Cyber-security
We have an almost 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

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.

What our sponsors say about us

SECURING HEALTHCARE

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

AKJ Associates