Securing the Education Sector

e-Crime & Cybersecurity Education Summit

20th November, 2024, Online

Protecting pupils, payments, personal data and intellectual property

The education sector is large, complex and connected. How can security professionals deliver defence while maintaining BAU?

https://akjassociates.com/event/education

AKJ Associates

e-Crime & Cybersecurity Congress Online Series: Education

SECURING EDUCATION

Protecting pupils, payments, and IP

In February this year, the universities of Cambridge, Manchester, and Wolverhampton have been hit by cyber-attacks in what appears to be a targeted campaign by the Anonymous Sudan hacker group.

In a post on X, the University of Cambridge's Clinical School Computing Service said that 'multiple universities' were experiencing a Distributed Denial of Service (DDoS) attack and warned that internet access was intermittent.

This attack highlighted the vulnerability of organisations in the sector as well as their attractiveness as a target not simply to economically motivated hackers, but to hacktivist and nation-state actors.

And it's not just universities. In June, Billericay School in School Road wrote to parents saying that the school had fallen victim to a "significant cyber malware attack", which shut down their IT network. The school was totally closed to students in years seven, eight, nine and 12 except for examinations and revision classes.

And in May, Embrace Multi-Academy Trust CEO Sharon Mullins said her schools were still feeling the effects of a cyber-attack, which happened just before Easter.

The government recognizes the issue and has released data quantifying it. For example:

- Primary schools are relatively close to the typical business in terms of how many identify breaches or attacks - 52% identified a breach or attack in the past year.
- All other types of education institutions are more likely to have identified cyber security breaches or attacks in the last 12 months than the average UK business.
- 71% of secondary schools identified a breach or attack in the past year.
- Further education and higher education institutions are more likely to experience breaches and attacks than schools, and to experience a wider range of attack types, such as impersonation, viruses or other malware, and unauthorised access of files or networks by outsiders.
- 86% of further education colleges identified a breach or attack in the past year.
- Higher education institutions are more likely to be affected by cyber-attacks - 97% identified a breach or attack in the past year. Just under six in ten of the higher education institutions identified that they had been negatively impacted by a breach.

So how can organisations harden security and build resilience as threats multiply?

The e-Crime & Cybersecurity Education Summit will look at how we all need a new kind of security for our educational establishments. Join our real-life case studies and in-depth technical sessions from the security and privacy teams in the sector.

e-Crime & Cybersecurity Congress Online Series: Education

SECURING EDUCATION

Key Themes

Defeating ransomware and malicious malware

The NCSC still assesses that ransomware remains one of the greatest cyber threats to UK CNI sectors. In other words, the threat of malicious malware has still not been adequately confronted and in the context of CNI the losses can be catastrophic. **So, forget about basic cyber hygiene and awareness, how do we protect the UK from this?**

From security to resilience

If security cannot be guaranteed, and attackers will eventually succeed, then you need to decide what that success looks like. Resilience is being able to maintain at least the minimum viable organization and in CNI it means maintaining the level of service required to keep the country running. **How can you help with critical resilience?**

Maximising the utility of threat intelligence

How can threat intelligence help defend and prepare against the emerging threat to CNI highlighted by the UK's NCSC? As attack surfaces increases and geopolitics expands the range of threat actors and types, **how can organisations make the best use of threat intelligence to genuinely reduce their risk of breach?**

The answer really is zero trust, isn't it?

Look at the key security and resilience challenges. Ransomware, third-party, malicious insider, and the rest. None of them have been solved by better technology or better awareness or better security culture. And AI and OT insecurity will make things worse in CNI. Unless we decide to abandon the public internet, and take security seriously, then zero trust is the only answer. So how to get there quickly?

Evolving incident response: lessons from the past

CNI organisations need well-rehearsed playbooks. They need Boards who have experienced realistic war games. They need to be battle-tested against sophisticated Red Teams. And they need to pay attention to the successful attacks of the past and present. **How can you help them develop and hone incident response procedures that work?**

Upskilling security teams

No organisation has an infinite budget. And most organisations are struggling to find sufficient security staff – the skills shortage is growing. This dynamic affects the type of on-prem security operation firms can employ and means that improving internal skillsets is critical to the security model. **So how can CISOs continuously upskill their teams?**

e-Crime & Cybersecurity Congress Online Series: Education

SECURING EDUCATION

Key Themes

Why regulation will drive CNI security

Governments have ceded power to private sector organisations with more money, better agility and all the technology. But as governments belatedly recognize their dependence on private companies to deliver the modern state, they will remember their power to regulate, control and even nationalize. **What are they thinking today?**

Reducing your attack surface

Initially, digitalization was touted as a panacea for productivity, innovation, flexibility and agility. It turns out that the rapid adoption of new technology and connectivity comes with new and complex costs. So, should operators of CNI retreat: **when the delivery of a critical service is paramount, how do we re-engineer digital systems to prioritize availability and not privacy or 'security'?**

The dangers of digitalisation – securing IoT and OT ecosystems

"There continues to be a heightened threat from state-aligned actors to operational technology (OT) operators. The NCSC urges all OT owners and operators, including UK essential service providers, to follow the recommended mitigation advice now to harden their defences." **How can you help CNI-related companies harden their OT?**

Securing third-party tech

Resilience and security increasingly come down to key dependencies outside the organization. With on prem tech the past and Cloud and external IT the future, how do organisations ensure security when they rely on vendors who are vulnerable but above leverage with even their biggest clients? And what about security vendors? **What is your advice?**

Developing the next generation of security leaders

If cybersecurity is to change to meet the evolution of our digital world, then so must those who implement it. CISOs cannot cling to an IT paradigm and companies must move away from hiring on false pretences (on budget and commitment) and firing at the first breach. **What does a next-gen CISO look like and are you one of them?**

Detect / prevent malicious insiders

When nation-states decide that cyber-offense is justified, the world becomes strange. One example: banks have been infiltrated by Chinese operatives who understand their control environments to commit financial and cyber crime. CNI is under attack from these attackers and other compromised employees. **How do we stop malicious insiders?**

https://akjassociates.com/event/education

AKJ Associates

Why AKJ Associates?

SECURING EDUCATION

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.**

Why the e-Crime & Cybersecurity Congress Online Series?

SECURING EDUCATION

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

Our end-user community of senior cybersecurity prof3ssionals 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 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 string, engaged relationships with high-level cybersecurity professionals.

Deliver your message to key decision makers

SECURING EDUCATION

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** will be 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 to your online booth, and showcases 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 will keep our **online congresses exclusive and give you the best networking opportunities**.
- 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.

Delivering the most senior cybersecurity solution buyers

SECURING EDUCATION

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.

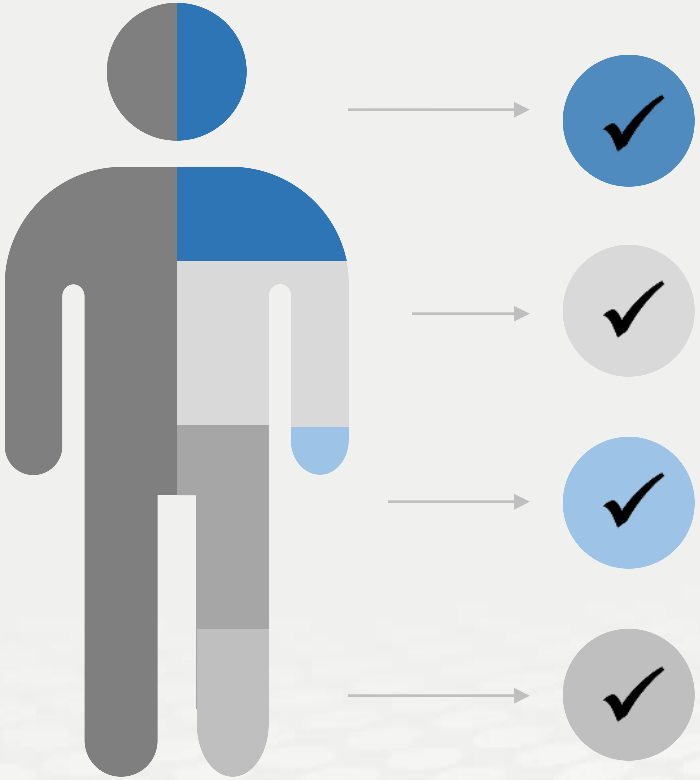
You will have access to the most senior buying audience in the cyber-security market.

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 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

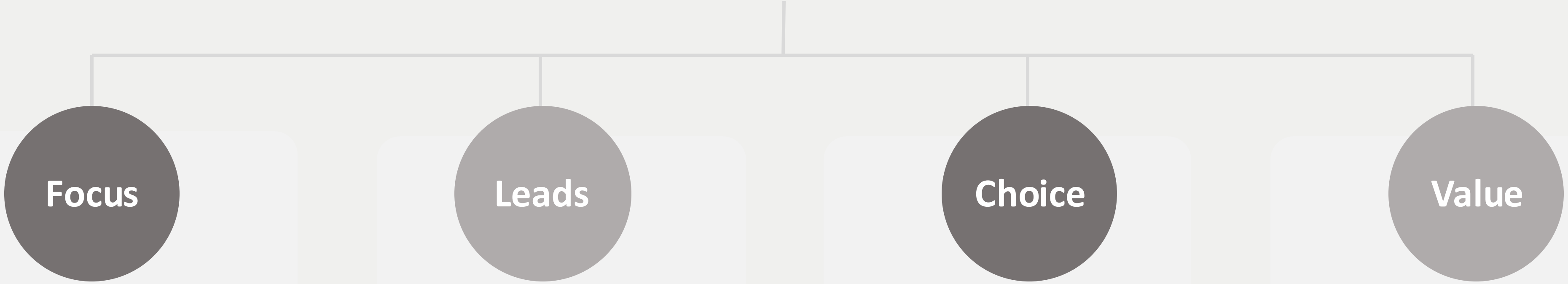
We deliver the most focused selling opportunity

SECURING EDUCATION

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

SECURING EDUCATION

The perfect platform for solution providers to deliver tailored advice to the right audience



Focus

Leads

Choice

Value

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.

Boost sales

Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.

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.

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 EDUCATION

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.

VERACODE

The level of engagement yesterday *[at the Virtual Securing Financial Services Congress]* was outstanding and we have already managed to book 2 meetings as a result, live on the day.

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