Securing the Public Sector: Online

July 3rd, 2025, London, UK

Public sector security: light at the end of the tunnel?

The government seems serious: is 2025 the year in which we start to fund security properly?

AKJ Associates

Good news at last: the government admits it must spend more and quickly too

The head of the National Cyber Security Centre (NCSC), Richard Horne, describes the cyber risks facing the nation as "widely underestimated … What has struck me more forcefully than anything else since taking the helm at the NCSC is the **clearly widening gap between the exposure and threat we face, and the defences that are in place** to protect us.

And what is equally clear to me is that we all need to increase the pace we are working at to keep ahead of our adversaries. We need all organisations, public and private, to see cyber security as both an essential foundation for their operations and a driver for growth. **To view cyber security not just as a 'necessary evil' or compliance function, but as a business investment, a catalyst for innovation and an integral part of achieving their purpose**."

The January 2025 report issued by the Cabinet Office and researched by the National Audit Office was, if anything, blunter when it comes to public sector cybersecurity.

It reports that "**multiple system controls fundamental to departments' cyber resilience were at low levels of maturity** in 2024, including asset management, protective monitoring and response planning."

At least "228 legacy' IT systems in use by departments in March 2024, and the government does not know how vulnerable these are to cyber attack."

And over 50% of roles in some departments' security teams were vacant in 2023-24.

As one spokesperson for the Cabinet Office has told AKJ, "it's a very challenging context. At the same time, be really blunt about it. Government is not keeping pace with this. We haven't done that adequately so far. That's why we need to seriously look at and seriously change the way that we're dealing with it."

So, what does this mean for public sector cybersecurity? Well, it means responsibility for security will be clarified and allocated appropriately. It means that all types of public sector bodies, including arm's length bodies, will have to get their security in order.

But most of all, it means that the government has finally accepted the fundamental importance of cybersecurity as a foundation of national security, a driver of economic stability and growth and a key deliverable in ensuring the safety and security of citizens and the organisations upon which they rely.

The new Cyber Security and Resilience Bill will be introduced to Parliament in 2025. Assuming the government is serious about revolutionising cybersecurity across the public estate, the Bill will usher in a new environment in which security is prioritised and new solutions sought.

There may never be a better time to pitch the public sector!

AKJ Associates

e-Crime & Cybersecurity Congress Online Series: Securing the Public Sector

SECURING THE PUBLIC SECTOR

Key Themes

Securing Arm's Length Bodies – a systemic issue

The neglect of cybersecurity in ALBs is a systemic issue driven by low budgets, weak oversight, outdated IT, and a lack of security culture. ALBs need help to impose cybersecurity standards (e.g., mandatory NCSC frameworks), help with security culture and training and help with incident response and other core security functions. **Can you help them with these challenges?**

A better approach to outsourcing cybersecurity

While outsourcing cybersecurity can improve security posture, organisations must retain key in-house cybersecurity expertise to oversee vendors, ensure clear contract terms and SLAs and regularly audit security providers to assess compliance and performance. **Can you help them adopt a hybrid model, where critical security functions remain in-house while external providers handle specific tasks?**

Developing a risk-based approach to the Cloud

It's hard to square the need for national security with Cloud usage. Major defence contractors avoid it completely. So, what about critical sector such as healthcare or HMRC or nuclear energy or border control. **So, what does a balanced Cloud strategy look like – given the choice may be between crumbling legacy systems and Cloud? How can risks be reduced to acceptable levels?**

Securing legacy technology

It isn't just the EOL of Windows 10 – though that is clearly a big deal. Public Sector organisations need to ensure legacy systems that cannot be replaced are isolated, monitored, and mitigated by compensating controls. **Can segmentation, virtual patching, data encryption, emulation, and secure API gateways help? What are your solutions?**

The ultimate third-party problem

The public sector's dependency on third-parties is complete. Given that this is one of the great unsolved problems in general cybersecurity, how should the public sector go about managing the risk? What should it prioritise in both its own security practices and in its suppliers? **And what kinds of security architecture and solutions should these organisations look to implement asap?**

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 public sector CISOs continuously upskill their teams?**

AKJ Associates

Why AKJ Associates?

SECURING THE PUBLIC SECTOR

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 and Cybersecurity Congress Online Series?

SECURING THE PUBLIC SECTOR

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: Securing the Public Sector

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 and engagement post event, as you 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 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 buyers

SECURING THE PUBLIC SECTOR

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.

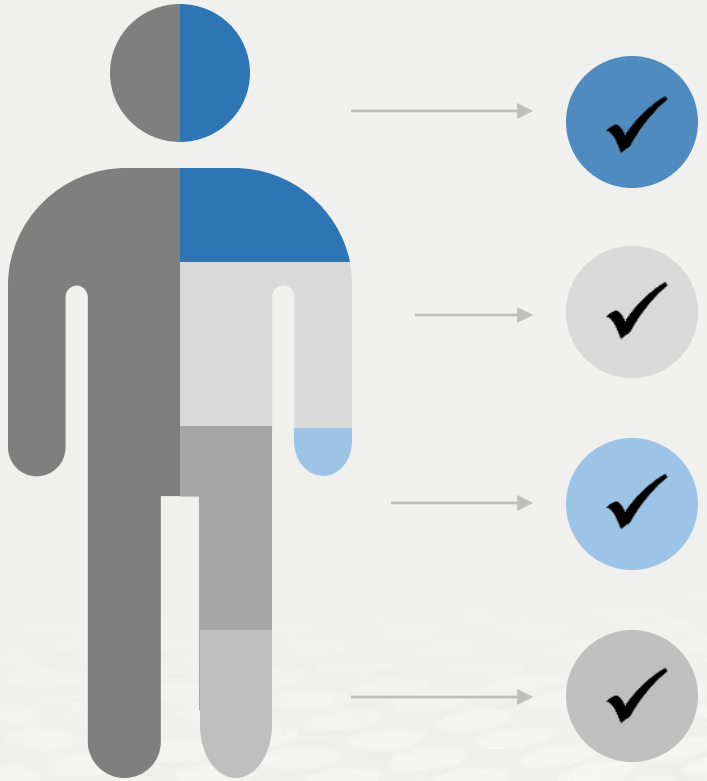
You will have access to the most senior buying audience in the cyber-security market.

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 THE PUBLIC SECTOR

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

SECURING THE PUBLIC SECTOR

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 THE PUBLIC SECTOR

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