LORCA NEEDS ACCELERATOR: LONDON'S SECURITY CHALLENGES AS A SMART CITY

LORCA

In June 2018 the mayor of London published the Smarter London Together Roadmap, led by chief digital officer Theo Blackwell.

The roadmap commits the mayor, together with the Mayor's Office for Policing and Crime and the London Resilience Group, to helping London achieve its smart city ambitions while tackling the cybersecurity risks that a proliferation of networked devices and the move to cloud-based services create.

To understand the security threats and the opportunities for innovation, LORCA brought together members of the Greater London Authority, representatives from London's local authorities and cyber members from our programme.

HELD UNDER THE CHATHAM HOUSE RULE, OUR DISCUSSION UNVEILED A RANGE OF INSIGHTS, CHALLENGES AND OPPORTUNITIES.

01

There's more work to be done on preparing for and managing major cyber incidents

02

Legacy systems make it harder to monitor threats from insiders and state-sponsored actors

03

Risk assessment is disjointed

04

A lack of central guidance for data sharing can cause paralysis

05

Helping staff be security-aware matters

THERE'S MORE WORK TO BE DONE ON PREPARING FOR AND MANAGING MAJOR CYBER INCIDENTS.

Following the NHS WannaCry cyber attack, local government has learned lessons about how a cyber incident differs from other major incidents. But local authorities can be better prepared to respond to the next major attack. Priorities include:

→ **being resilient:** services need to get back up and running as soon as possible to avoid disruption as well as reputational or financial damage

→ **employee training:** attendees admitted that incident preparedness is not a primary part of an employee's role in many instances. Not all staff have the right skills and there's concern they won't be able to recall or implement training when needed.

→ **maintaining the confidence and trust of the public** when an incident is taking place – especially when sensitive personal data is involved

→ **the safety of critical national infrastructure and the public** (when smart transport is involved, for example)

→ **understanding where the physical and information assets are.** There was a view that 75% of the estate was from suppliers. Compromised suppliers would result in key services and processes being unavailable. Understanding where assets are would improve incident response.

→ **improving the quality of testing** exercises in situations where critical assets can't be shut down. There's an appetite for methods than enable local authorities to test and validate response plans that go further than the desktop.

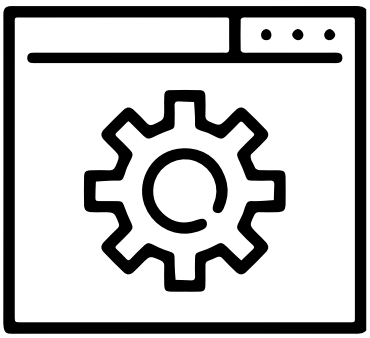
→ **growing collaboration and trust between service providers,** other authorities and the NCSC. Organisations must feel confident that they can share information during and after an incident with partners. Attendees also said that there was a fragmented approach to cybersecurity across the authorities.

→ **building confidence in third parties** and ensuring they're being contracted to follow best practice

However, despite incident preparedness and response being seen as an area for improvement, attendees admitted it's an under-funded area.

"Not all staff have the right skills"

LEGACY SYSTEMS MAKE IT HARDER TO MONITOR THREATS FROM INSIDERS AND STATE-SPONSORED ACTORS.



A major challenge highlighted by the group was the continuous use of legacy systems and outdated technology in the workplace. Because of a lack of funding for the latest malware or threat monitoring software, these legacy systems make it more likely for an employee to unintentionally cause – or fail to detect – a security incident.

The group also felt like there was a disjointed approach to commissioning and procuring goods and services, with some members prioritising security spend less than others.

Without more public funding, the group thought the focus should be on:

- → enabling cross-public sector and local government collaboration to use strength in numbers as a monitoring approach
- → encouraging senior stakeholders to urgently encourage security awareness, risk management and devolved responsibility within organisations
- → understanding the current security architecture and its potential risk flashpoints

“These legacy systems make it more likely for an employee to unintentionally cause – or fail to detect – a security incident”

RISK ASSESSMENT IS DISJOINTED

The group agreed that risk assessment in the public sector is not joined up and there's often a lack of synergy between IT and operational teams.

There's also a tendency for operational and commercial teams to turn to a technical solution quickly rather than creating cultural change.

Participants thought that being able to compare their risks with similar organisations and authorities would help, along with having an agreed external methodology for assessing risk.

"Risk assessment in the public sector is not joined up"

A LACK OF CENTRAL GUIDANCE FOR DATA SHARING CAN CAUSE PARALYSIS.

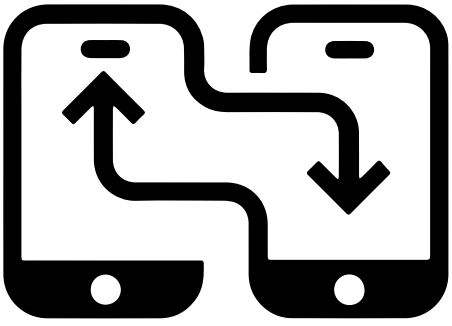
There's also an opportunity to embed privacy by design into operations"

Data needs to be shared between multiple agencies, local authorities, local and central government and third parties to deliver essential public services. But these organisations struggle with being confident that they're sharing data in a way that's compliant with regulation such as the General Data Protection Regulation.

Attendees said organisations are fairly clear on what information they can share in emergency or incident response scenarios thanks to legislation, but things are less black and white after an incident.

A lack of centralised, standardised guidance also creates confusion, with each organisation requiring its own data sharing agreement. For example, the London Fire Brigade has hundreds of agreements.

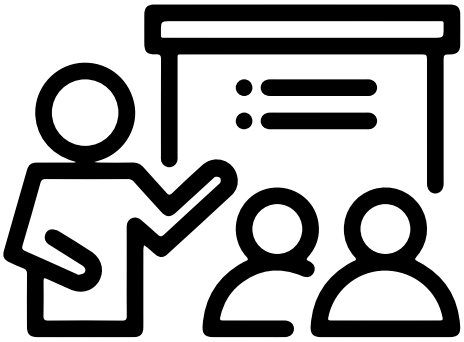
This means compliance is subjective and open to interpretation, which can lead to operational paralysis and poor decision making that costs lives.



There's interest in exploring ways to enable more synergy, whether through working groups, using data sharing templates, creating a central information sharing platform or enabling open source data sharing that aggregates data across organisational boundaries.

There's also an opportunity to embed privacy by design into operations and IT systems so organisations can be more confident that they're sharing data in a secure and compliant way.

HELPING STAFF BE SECURITY-AWARE MATTERS.



When it comes to the public sector maintaining the trust of society, the behaviour of individuals within an organisation is key.

Attendees were more concerned about staff sharing data unintentionally than targeted phishing attacks or financially motivated breaches – especially since training tends to be a one-off occurrence when an employee first joins rather than an ongoing process. And it's hard for in-house IT teams to make sure security awareness is universal when teams are large and employees starting or leaving the company regularly.

An added risk is that these employees are often using old and insecure systems that require them to copy and paste data.

There was an appetite for more effective, always-on training that draws on behavioural science and measures the impact of training on behaviour change.

Other suggestions included aligning security training with wider health and safety training and creating a single cybersecurity training platform.

Finally, there was recognition that cultural barriers (such as a lack of accountability for staff awareness at a governance level) and a lack of internal communications drives are blockers to progress.

> *Employees are often using old and insecure systems"*

CONCLUSION: A DESIRE FOR SECURE COLLABORATION AND BUILDING IN TRUST.

Local government authorities in London want to share information securely, streamline practices and collaborate with confidence. But with such a complex web of organisations involved, and with legacy IT systems in place, there are a number of security and cultural challenges to overcome.

Attendees clearly saw individuals as being at the heart of good cybersecurity, so companies with people-centric solutions that take these operational and cultural nuances into account could play a key role in enabling employees to practice better cybersecurity hygiene.

Our discussions also showed that attendees recognised the link between cybersecurity, protecting lives and earning the public's trust. And thanks to major security incidents involving the public sector, the need to prepare for a major security incident and build in resilience is widely understood.

However, a lack of coordination when it comes to the procurement of security solutions, the fact that the responsibility for cyber training doesn't sit with senior decision makers and a fragmented approach to security among organisations makes it a challenging environment for cyber startups and scaleups to navigate.

“Local government authorities in London want to share information securely, streamline practices and collaborate with confidence.”

CONNECT WITH US

lorca.co.uk
info@lorca.co.uk

Twitter: @LORCACyber
LinkedIn: LORCA Cyber

FIND US

Plexal, The Press Centre
Here East, 14 East Bay Lane
Queen Elizabeth Olympic Park
London, E20 3BS

LORCA