Local Government Association

Cllr Introduction to…
Cyber Security

Resources Pack

March 2021

www.local.gov.uk

Purpose of this Pack

- On 25th March 2021 the LGA ran a session with speakers on the topic of Cybersecurity
- This pack provides a range of resources relating to that event to help both those who attended at the time and those who didn't
- It contains

The Scope of this Issue

Cybersecurity has grown as a concern for local authorities in recent times, as it has for all organisations and individuals. What are the appropriate responses by local authorities to this threat, and in particular what is the role of councillors in ensuring that their council is making the appropriate decisions to guard against it, and to meet the specific challenge if it occurs?

National Cyber Security Centre

At the event we had a talk from NCSC. For security reasons we cannot include the sides of the talk here. However NCSC have a wide range of relevant resources to share.

- Introduction to Cybersecurity
- A toolkit to guide the discussion between non-technical leaders and their technical experts
- Guidance for Public Sector Organisations
- Guidance for IT Teams around elections

Local Government Association

A Case Example

At the event we discussed an instance of a council that was the victim of an attack. For confidentiality reasons we cannot discuss this in detail here, however some key points to consider are:

- The council had taken reasonable steps beforehand required to obtain assurance about their cyber-safety, this was not a case of negligence
- The attack had an immediate and devastating impact on the council's ability to function, with council areas having to establish back up paper-based systems, and without access to key information eg around social care records; IT teams have had to work exceptionally hard around the clock
- Considerations around investigating the crime meant that the council was limited in its ability to communicate to its residents, an agonising state of affairs for elected members. In addition they came under extremely hostile questioning from the press
- It was vital that the council did not pay the demanded ransom, it's essential that the sector stands in solidarity and does not become seen as an easy target. Moreover it is critical to note that it was unlikely that those demanding the ransom would actually have been able to remove the problem anyway, so the payment would have been for nothing
- Resolution of this issue has taken a year and counting
- Support has been provided from government agencies (eg NCSC) but initial assurances that the council would be compensated for the additional costs involved have not so far been met and there is a real concern about whether they will be – get any such assurances in writing.

Discussion

In breakout groups we discussed a number of aspects about how this affecting the delegates where they are. Some core themes were:

- The importance of prioritising training and education to ensure that staff and members are undertaking good practices around things such as strong passwords and being wary about clicking in links in emails
- Technical policies to lock down equipment and staffing policies around acceptable use
- Concerns about the cybersecurity around bought-in and in-house systems, and their interconnectivity
- The importance that the sector as a whole learn from incidents
- A need for councillors to know what questions to ask
- A recognition that this cannot just be seen as an issue for the IT department.

Expert Speaker - Theo Blackwell

Theo Blackwell was a councillor and cabinet member for digital at LB Camden and was recognised as one of the leading members driving digital change in their authority. He is now the Chief Digital Officer for the Greater London Assembly, advising the mayor. His slides from the session follow.

LGA: Cyber security, key questions for elected members

Theo Blackwell MBE, Chief Digital Officer for London

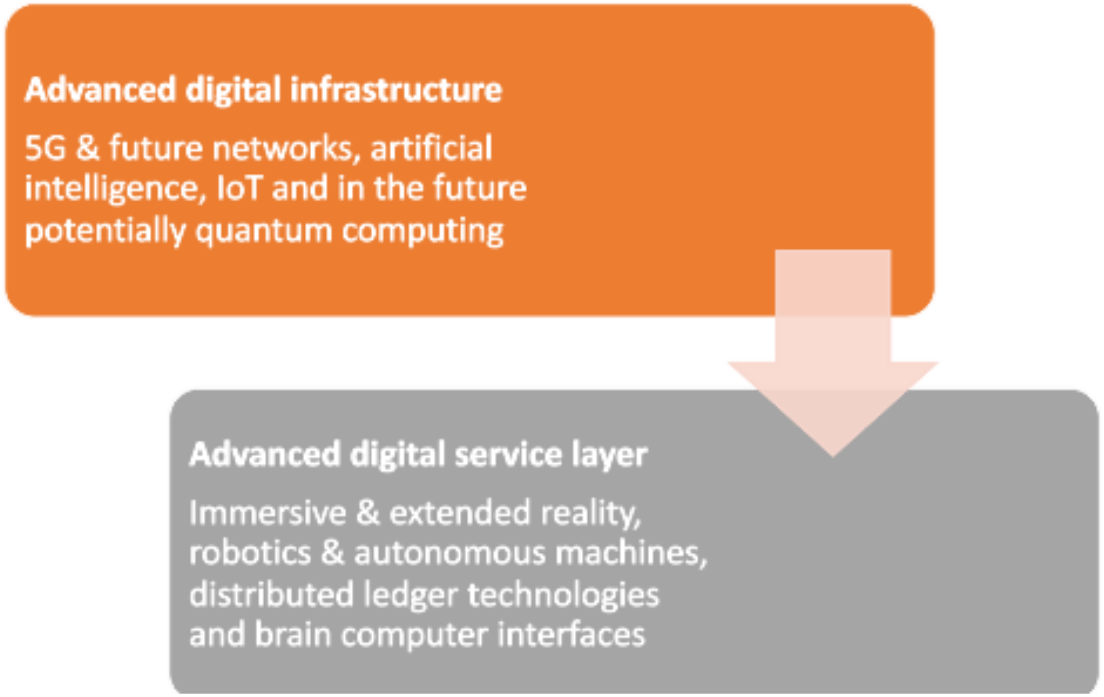
Digital & public services (now)

Even before crisis, almost all services to users (citizens, businesses, staff) relied on IT or digital services

During crisis, even greater reliance on digital services: likely to return to more blended/hybrid working & delivery environment

Councils hold increasing amounts of data in our systems, often sensitive (vulnerability, payments)

Smart Technology: the next 15 years…



Smart cities

- From CAVs mobility services to remote operated cranes and smarter logistics around the city, this new advanced digital infrastructure will enable numerous start-ups to access data, connectivity and intelligent AI services and build new products and applications that rapidly transform how we live and work in the city.

Augmenting the physical environment

- Extended reality (VR/AR/MR), underpinned by real-time data, 5G, IoT and AI, will create the physical internet. "Clickable" London: more interactive & rich with local data for smart tourism, retail experiences to draw people back to the high street

Augmenting the physical self

- This will include haptic feedback, allowing people to click or press buttons in a virtual, touch free environment; through to brain computer interfaces that will help break down barriers for disabled people, for example, the potential to use robotic assistance to aid walking.

MAYOR OF LONDON

Confidence in preventing attacks

Confidence in recovering from attacks

"How will we deliver services if there is no access to IT?"

MAYOR OF LONDON

Key questions to ask of CEOs (as sourced from CIOs)

What is the council's approach to buying/making technology? Does the council have a clear view about its technology estate & approach, including legacy constraints?

How much money is the council investing in cyber security annually (prevent, protect & respond)

To what extent is IT security a cross-organisation priority?

How far through the programme of security improvements is the council?

How do you know that policies are fully implemented, all the time?

Cont..

- How will you find potential weaknesses more quickly than highly motivated & resourced attackers?
- How well do you understand the data you hold and potential risk?
- How are you using retention management to dispose of data you no longer need to reduce risk?
- What's is you council's insurance position against risks?
- Is cyber a standing agenda point for any Executive Management Team & leader meeting?

MAYOR OF LONDON

Observations

Cyber security, like other aspects of digital/IT an **area of expertise** reliant on skilled staff not necessarily part of the very senior management team

Sharing of **threat landscape** improving but channels across local government challenging – case for collective pooling of expertise on regional level?

Cyber security/resilience not yet a common feature across formal Resilience structures

MAYOR OF LONDON

Key Resources

- In addition to the NCSC resources listed on slide 4, the LGA has developed extensive highly relevant resources:
  - This is the link to the main topic area on the website
  - A Councillor's Guide to Cyber security
  - Cyber security case studies from other councils
  - Many other resources that will be relevant to members and also to your officers

Summary: Some Questions to Consider Asking

1. How does my council understand, assess and manage cyber-risk and what policies, processes and tools do we use?
2. Do my council's decision making and scrutiny committees have the regular information they need to make/scrutinize decisions relating to cyber-risk?
3. How do officers back up council data – is this secure and offline?
4. Are staff given training on their role in reducing cyber-risk?
5. Do members receive regular cyber-security updates – including on threats, incidents and near misses?
6. How does my council use the National Cyber Security Centre's tools and services?
7. What are the response, recovery and continuity plans for cyber incidents?
8. Can I be involved in testing these cyber-resilience plans?
9. How would we deliver services if – following a cyber attack – we had no access to IT?
10. How well connected is my council with those who have developed great practice in this area?