Local Authority Cyber Resilience

UK Authority Resilience & Cyber4Good 2023

Geoff Connell, NCC & CTAG

22nd September 2023

Norfolk County Council

Geoff Connell
CIO & CDO

Chair of LCIOC & CTAG

CTAG & Cyber Resilience in Local Government

- Thank you for inviting me back. This year the focus shifts from “security” to “resilience”. I think this means recognise you are likely to get attacked, disrupted and maybe compromised, so plan to minimise the impact, not just try to avoid.

- We are a year further and the risk of sophisticated attacks from a variety of malicious actors right up to nation state continues to grow, with AI enabled risks emerging.

- Council finances are worse & continuing to worsen, along with increasing demands from residents.

- The threat surface continues to grow through connected places and worsening supply chain risks.

So, not good news from a macro / geopolitical perspective, but there are things we can do.

Cyber security is an arms race, continuous improvement plans should be in place.

It's also a team game.

WARPs, LRFs, Socitm Regions
LGA, DLUHC, Cabinet Office/GDS/PSN/FN4G, CCS, NHS and remember it's a board level risk, not an IT risk.

CTAG (ctag.gov.uk)

- CTAG is where WARP leads come together to share knowledge and expertise with NCSC and other key UK public sector Cyber stakeholders
- Technical Reference group for Socitm LCIOC, NCSC, LGA, DLUHC etc
- Chaired by myself (Geoff Connell), with great support from Cliff Dean, plus CTAG core team of Mark Brett, Matt Smith & Bruce Thompson.
- Thanks to Nik & the NCSC team, Owen & the LGA team, Ben & DLUHC team for expertise & financial support

CTAG activity in 2023/24

- Resourced by Local Gov volunteers and much appreciated funding from the LGA.
- As a convener, bringing together WARP leads and authority cyber leads to collaborate with LGA, DLUHC
- Monitoring LRG Cyber vulnerabilities, highlighting opportunities for NCSC Active Cyber defence solutions, supporting the great work of the Domains team, providing early warning of risks and compromises.
- Providing technical training & skills development
- Providing advice & guidance, for example AI risks & how to get the best cyber security from our existing investments, particularly Microsoft.
- Supply chain security – we are now passively scanning our main suppliers, helping them recognise their vulnerabilities and encouraging them to up-their-game where appropriate.
- Providing our “allies” with a practical sounding board on how best to implement new solutions such as:
  - Post PSN Assurance - DLUHC to introduce the Cyber Assessment Framework (CAF) standards
  - Regional / shared SOC options (as local gov IT isn’t a 24/7 services) – DLUHC & LGA

And finally: my cyber resilience top tips this year

Keep on making sure you are getting basic cyber hygiene right: patching, passwords, permissions, staff skills & awareness, secure backups, NCSC ACD (PDNS, mail-check, NEWS etc).

After getting the basics right, my top 3 recommendations to improve your cyber resilience are:

(1) **Engage** in national & regional support networks through, WARPs, LRFs, NHS ICS and Socitm regional groups, NCSC, LGA, MHCLG Cyber. Also work with appropriate suppliers and external organisations. **Build your networks before the emergency…**

(2) Make sure **cyber resilience is a team effort** inside your organisation. If you keep it to yourself in IT, you own it, alone… This is a **board level risk** management issue, not just a technical one! Report regularly to board, in plain English, assess cyber risk appetite.

(3) Look out for emerging risks: For example, from Smart Places technology, cameras, sensors, published info that might be valuable to an attacker & consider data loss risks arising from AI use (shadow IT, well meaning innovators and experimentation).