Local Public Sector Cyber Security

UK Authority Resilience & Cyber4Good 2022

5th October 2022

Norfolk County Council

Geoff Connell
CIO & CDO

Chair of LCIOC & CTAG

Cyber & Local Government in 2021 & 2022

- I spoke at Cyber4Good last year and the backdrop in terms of cyber risks are the same, but worse…
- Risk of nation state level attacks is higher
- Council finances are worse & continuing to worsen
- Sophistication of attackers has grown
- Threat surface continues to grow (IoT)

So, not good news from a macro / geopolitical perspective, but there are things we can do at no cost.

Where to look for support….

Good news, there are lots of opportunities to share and work together…

WARPs, LRFs, Socitm Regions LGA, DLUHC, Cabinet Office/GDS/PSN/FN4G, CCS, NHS (under ICB/ICS arrangements)

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 David Cowan, Cliff Dean, Mark Brett, Matt Smith & Bruce Thompson & from LRG+.
- Thanks to Nik & the NCSC team, Owen & the LGA team, Ben & DLUHC team for expertise & financial support

CTAG Focus Areas

- Basic Cyber hygiene take-up: awareness raising, aspects of vulnerability monitoring, adoption & support
  - NCSC Active Cyber defence solutions
  - LGA & DLUHC cyber support offers
  - Engaging “hard to reach” authorities
  - Looking at Schools & Parish Council monitoring too

- Training & skills development

- How to get the best cyber security from our existing Microsoft investments

- Supply chain security

- Post PSN Assurance
  - Reviewing Cyber Essentials Plus (not suitable?)
  - Working with DLUHC on developing “LG” CAF (in line with central gov & NHS direction of travel)

- Regional / shared SOC options (local gov doesn’t generally operate 24/7 services)

And Finally: My Top Cyber Tips for 2022

Local public sector cyber resilience must build upon foundations of **good basic cyber hygiene**: patching, passwords, permissions, etc + NCSC ACD (Protective DNS, 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. **Find friends 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) It's one thing to believe you are ready for an incident but if you don't **test and exercise**, you aren't well prepared. So, practice… (NCSC Exercise in a box is a good place to start).