Levelling-Up Local Gov. Cyber Security Maturity

UKAuthority Resilience & Cyber4Good 2021

15th September 2021

Norfolk County Council

Geoff Connell
CIO & CDO

Chair of LCIOC & C-TAG

Cyber & Local Government in 2021

- I took on a national leadership role in relation to Cyber security for Socitm because WannaCry hit while I was Socitm President. I have continued to lead on this challenge & chair the Cyber Technical Advisory Group (C-TAG) because it remains a serious threat to the delivery of our services. As a sector we are now better at defending ourselves than ever before, unfortunately our adversaries and the opportunities they are able to exploit are also greater than ever.
- Lindy Cameron, CEO of the UK Government's National Cyber Security Centre, recently warned that ransomware is the key cyber threat facing the UK, citing recent attacks and how they had 'shut down NHS org's, schools & local authorities at great cost to the public purse'. She went on to say that whilst they support victims of ransomware every day, **'turning up to a ransomware incident as the NCSC feels like the fire service turning up to a house that has already burned down'**
- "There are only two types of companies: Those that have been hacked and those that will be hacked." – Robert S. Mueller, III, former Director of the FBI
- Those of us in the technology industry know that no computer system can be made completely secure. Dr Ian Levy
- Bad things happen to good councils. Even well **defended** organisations can get infected with ransomware, so the focus must shift to include **rapid discovery & recovery**, organisational resilience and the ability to bounce back to digital operations
- Covid response caused us to accelerate our migration to digital service delivery and our reliance on technology, but not all authorities are as yet getting all the basics of cyber security right. We need to level up our capabilities.
- C-TAG (Cyber Technical Advisory Group) and works closely with the LGA & MHCLG Cyber Teams, the NCSC and the UK WARP network to maximise cyber security related collaboration across the public sector.

Where to look for Help….

WARPs, LRFs, Socitm Regions
LGA, MHCLG, Cabinet Office/GDS/PSN/FN4G, CCS

- **C-TAG 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, MHCLG+**
- **Promotes uptake of NCSC ACD and other leading practice in cyber & resilience across WARPS & to LAs**
- **Issues tech guides and training, promoting re-use of assets**
- **Thanks to NCSC & LGA for expertise & financial support**

Don’t re-invent the Wheel…

- Leverage security from existing communities and services. NCSC, WARPS, C-TAG, LGA, MHCLG etc.
- We use “The Things Network” worldwide community for our LoRaWAN IoT network (featuring 128bit end-to-end encryption).
- We also get help from our suppliers – Microsoft, Bytes & Capita etc.
- Cloud platforms & standards are your friends. (If configured correctly).
- We need to seek opportunities to partner better with NHS & other public sector bodies to pool public funds & skills more effectively.

Some of the common cyber mistakes

- Not having secure (immutable) backups.
- Not keeping up with patching (turn on auto-patching!)
- Not being on up-to-date / supported versions of software.
- Not being sufficiently vigilant of compromises to suppliers and partners.
- Failing to minimise use of admin accounts and other elevated access privileges (don't allow email access or web browsing from admin accounts).
- Not training staff and raising awareness sufficiently.
- Not deleting / destroying information when it is past its retention date.
- Not testing defenses sufficiently, including penetration testing.
- Not exercising and practicing. It's not just about avoiding compromises, its about how we respond.
- Allowing weak passwords &/or not enabling multi-factor authentication.
- Not making organisational leadership aware of the risks and options to reduce risks.

How we protect ourselves at NCC

The

- We have deployed all of the NCSC Active Cyber Defense (ACD) tools.
- We are active members of the Norfolk Cyber Cell (under LRF), Cybershare East (local WARP), C-TAG etc.
- Periodic simulated phishing exercises. Refreshed & promoted training as well as regular Comm's messaging on the Intranet, lock screens etc. Over 95% of all staff have recently completed the latest training.
- Maintain secure offline backup facility, independently reviewed by the MHCLG Digital Cyber Programme.
- Regular patching & retiring all legacy versions of software and operating systems in a timely fashion.
- Regularly reviewing the cyber security of our suppliers and partners.
- Reducing the number of admin accounts and other elevated access privileges & enforcing complex passwords.
- Conduct regular penetration testing (additional testing recently supported by extra LGA funding)
- Set up Cyber cell for LRF & pooling intelligence across local, regional and national cyber groups including NCSC.
- Undertake multiple compliance assessments inc. PSN, NHS DSP, Cyber Essentials Plus.
- We treat this not just as a technical issue, but a strategic investment issue in skills, capacity, policy etc.

Norfolk County Council

And Finally: My Top Cyber Tips

Local public sector cyber resilience must build upon foundations of **basic cyber hygiene**: patching, passwords, permissions, etc + NCSC ACD (Protective DNS etc).

After that my top 3 recommendations to improve your cyber resilience:

(1) **Engage** in national & regional **support networks** through, WARPs, LRFs, Cisp 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** in 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!

(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).