UK Authority Resilience & Cyber4Good

Cyber Security During a Funding Crisis

Current cyber threats and opportunities in the context of Section 114 notices. Where will the budget challenges increase risks and what can be done to reduce them at little or no cost?

Geoff Connell - Wed18 Sept 2024

Norfolk County Council

Introduction

Geoff Connell – Director of Digital @ NCC

Chair of CTAG

I’m fortunate to work closely with regional and national (& devolved administration) cyber leads from Local Gov, WARPS, NHS, NCSC, MHCLG, LGA, DSIT etc.

Cyber in a funding crisis…

As we stand today, I think UK Local Gov overall has come a long way over recent years and is generally capable when it comes to cyber security & protecting citizen data (albeit with regional variation and plenty of room for improvement)

I worry that the current extreme (Section 114 level) financial pressures might take us backwards in terms of our cyber defences and resilience.

Consider that the cost to clear up after a cyber event is likely to be much greater than the cost to maintain appropriate defences.

SOC & 24/7 support funding must be at risk, extended backup solutions, staff capacity etc will be challenged hard.

So what can we do to maintain our capabilities and hopefully keep maturing?

Low cost / no cost cyber resilience options

Cyber defence is a team game, so share the burden!

- It’s board level business risk, so make sure your board, execs & politicians understand the current threat levels and your cyber maturity and co-own the risk. Otherwise, they will just assume IT are dealing with it.
- Run simulated incidents to prepare before anything real happens.
- Phish your staff and do training & awareness raising work (it’s not just about failures, it’s about first to log the attack so IT can block / delete quickly).
- Turn shelfware into cyber defences MS E3 & E5 have lots of functionality which you may not yet have deployed. Build a plan to utilise this (and other already licenced) functionality.
- After phishing based ransomware attacks, supply chain vulnerabilities are probably the next biggest threat, so look closely at supplier contracts, codes of connection etc & let’s hold our suppliers to account (within existing agreements).
- Remember it’s still the basics of cyber hygiene that catch us out most often so stay on top of all the Ps – Patching, Passwords, Permissions, Ports, Policies etc.
- There are free to use cyber resources from NCSC (ACD in particular) so use them, why wouldn’t you?
- WARPS are free or low cost to join so share expertise, intelligence & pool capacity with your regional counterparts.
- CAF is more effective for cyber assurance & risk reduction than PSNA to move to it ASAP. MHCLH are offering funding to LAs to help us resource the adoption, not every authority has taken the money! Why?
- LGA have some great resources, so take advantage of them too (over to Jamie…)