Cyber Security Update to NCC Audit Committee

22nd April 2021

Geoff Connell – Director of IMT & Chief Digital Officer

Protect yourself, your family and our communities by being cyber aware

Cyber attacks against the local government sector have increased by 300% in the last 12 months. Security is a responsibility for us all both at home and within the workplace-

- Be cautious of any email asking you to log in to confirm your account or personal details.
- Be aware of emails containing links or attachments. Would you normally receive attachments or links from that person?
- Remember to complete your Online and Information Security training on LearningHub.
- If it JDLR (Just Doesn't Look Right) use the Report Message button in Outlook.

Norfolk County Council

PROTECT OURSELVES. PROTECT OTHERS. PROTECT NORFOLK.

Norfolk County Council

Introduction

- Cybersecurity has grown as a concern for local authorities in recent times, as it has for all organisations and individuals.
- The Covid-19 pandemic response massively accelerated existing programmes of service digitisation and smarter working initiatives.
- It also necessitated a series of rapidly implemented digitally enabled innovations and new ways of working. Many of these involving partnership working and sharing of sensitive data.
- Although these changes were made at pace, not lowering our guard in terms of data and cyber security was always in our minds as sadly cyber criminals were quick to try to use Covid-19 related disruption to launch a new wave of attacks.
- The threats to our networks, systems and data have grown since the onset of the pandemic.
- Our network expanded from hundreds of council business locations to the homes of 7,000+ staff.
- Our reliance on cloud services for delivery of services changed overnight with Teams becoming an essential tool in our daily working lives.
- Digital skills of staff and elected members had to make a step change in many cases to use all the new technologies or use them in new ways.
- Cyber criminals have chosen this time to target councils, NHS, schools and vulnerable people.
- The threat is very real and growing. Local authorities, schools, universities, housing organisations, private sector (large & small companies), charities and individuals have all been compromised in growing numbers.
- The recently published PWC Annual report stated that globally CEOs viewed Cyber security as the 2nd greatest threat after the Pandemic.

Some of the main risks

- We have more online services than ever before, we hold more sensitive data than before, we share data and join up systems with more partners. We use more cloud services & use IoT for innovation.

- Cybercriminals have access to more sophisticated tools at lower costs than before and are happy to target organisations that are already stretched by Covid-19 response work.

- Ransomware attacks, have been successful against multiple local authorities nationally. Also, recently a local housing supplier a small rural Norfolk school had their systems compromised.

- Phishing attacks, resulting in data loss or enabling ransomware.

- Tight budgets may restrict funding to replace legacy IT, invest in cyber expertise, buy tools & support.

- Local government will NOT pay out against successful ransom attacks, this means that disruption, expense and reputational damage could be significant and has been in several well documented recent cases.

Some of the common mistakes

- Not having secure backups.
- Not keeping up with 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.
- 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.

Some of the things we do to protect ourselves

The

- We have deployed all the National Cyber Security Centre (NCSC) Active Cyber Defense (ACD) tools.
- Periodic simulated phishing exercises.   Refreshed & promoted training as well as regular Comm's messaging on the Intranet, lock screens etc. Around 95% of all staff have recently completed the latest training.
- Renewed our secure offline backup facility and got all our backup arrangements independently reviewed by the MHCLG Digital Cyber Programme – they are also funding us to share this with relevant partners.
- 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.
- Implementing safe-links & safe-attachment technologies as well as implementing anti-spoofing technologies.
- Conducting 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.

Summary & Conclusion

- The cyber threat is real and there are no 100% guarantees of cyber security. Therefore we must take all reasonable steps to protect ourselves and prepare to respond in the event of a successful attack.

- The move to more digital provision of services, flexible ways of working, joined up systems and data are essential components of the NCC digital strategy and roadmaps for the 2020s.

- Extended use of artificial intelligence, robotics, sensor networks and other technologic enablers of innovation will provide opportunities for better services, but also additional cyber threats in future.

- NCC is committed to implementing and maintaining appropriate cyber security measures to retain the trust of Norfolk citizens in our ability to protect their data and provide safe, reliable public services.

- The digital strategy and roadmap supports this commitment by making sure that all new digital services have security built in by design and that we minimise the risks posed by unsupported old networks & legacy systems.

- We regularly test our IT defences as well as our response and recovery plans.

- Cyber security is a team effort, that's why we work in partnership locally, regionally and nationally to maximise the security of NCC data and system as well as those of our service delivery partners.