North Somerset Council

REPORT TO THE COMMUNITY AND CORPORATE ORGANISATION POLICY AND SCRUTINY PANEL

DATE OF MEETING: 19 JUNE 2018

SUBJECT OF REPORT: CYBER SECURITY

TOWN OR PARISH: ALL

OFFICER/MEMBER PRESENTING: MIKE RIGGALL, INFORMATION AND ICT SECURITY MANAGER

KEY DECISION: N/A

RECOMMENDATIONS

That the panel acknowledges the recent LGA report, *A Councillor's Guide to IT Security*, challenges officers on the responses to the questions posed in the guide and obtains assurances as to the confidentiality, integrity and reliability of the council's IT systems.

1. SUMMARY OF REPORT

1.1. In March the Local Government Association published a report designed to raise awareness amongst councillors of the threats posed to council services by cyber attacks. In spite of an almost complete dependency by councils on IT systems to deliver services, national research suggests that other factors relating to IT, including digital exclusion in the population and poor availability of high speed Internet connectivity, represent a greater level of concern for elected members.

1.2. The purpose of this panel report is to summarise the main themes of the LGA document and to provide some information in response to the key questions which the LGA suggests elected members should be asking of their local authorities.

2. POLICY

2.1. Maintaining reliable IT systems is a key enabler underpinning the entire corporate plan.

3. DETAILS

Background

3.1. Recent well-publicised incidents show how in an increasingly globalised world, public sector organisations can find themselves on the front line at a time when the threat of individual and state-sponsored cyber-attacks has opened up a new front in modern warfare. The worldwide 'Wannacry' attack in May 2017 that in the UK primarily affected the NHS, provided a suitable demonstration of the disruption that can be caused to essential services by attacks on public sector IT systems.

3.2. Although personal data was not breached, the incident had a major impact on patients, many of whom had appointments and operations postponed as a result of the ensuing backlogs.

3.3. Whilst local government was not directly affected in the 2017 incident, reaction to the situation contributed significantly to the disruption. Local authorities shut down computer links to NHS organisations as a precaution thereby stopping the essential flow of information between partners for several days.

3.4. As the subsequent investigation unfolded, it became clear that outdated technology was part of the problem, with research suggesting that 90 per cent of hospital trusts were still using outdated versions of Windows. Whilst Microsoft had made a patch available to protect users from the particular vulnerability exploited in the attack, many computers had not been updated.

Reaction to the Wannacry Attack

3.5. In a bid to learn from the experiences of the NHS, the rest of the public sector commissioned widespread reviews of cyber security to understand whether the failings experienced in the NHS were being replicated across other sectors. The reviews focused not only on the technical infrastructure, but also on management attitude to cyber security and the governance that organisations had in place to oversee security management.

National Security Framework

3.6. The underpinning principles on which national cyber security policy is based are developed by the National Cyber Security Centre (NCSC). This was formed in October 2016, bringing together and replacing CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

3.7. All public-sector organisations are expected to design and manage their IT systems in accordance with the principles of 10 Steps to Cyber Security as published by the NCSC. There is currently no formal requirement for local authorities to be formally audited against this framework as there is for central government departments and any private sector organisation bidding for government contracts.

3.8. The Department for Culture, Media and Sport (DCMS) manages a programme of annual compliance audits to ensure that organisations that connect to the Public Services Network (PSN) comply with a defined set of minimum security standards called the Code of Connection.

3.9. Councils must also comply with a similar set of standards in order to exchange information with NHS organisations either through the N3 network or the new Health and Social Care network (HSCN).

3.10. These annual audits are currently the only formal assessment of a local authority's approach to cyber security.

Supporting Organisations

3.11. Supporting organisations at a national and regional level are many groups focused on improving resilience to cyber attack. Primarily for local authorities this includes the Society of IT Managers (SOCITM), the Local Government Association (LGA), Warning and Advisory Reporting Points (WARPs) and Local Resilience Forums (LRFs). Whilst SOCITM and the LGA largely provide strategic advice aimed at business leaders and senior managers, the WARPs focus very much at the operational and technical levels.

3.12. In March 2018 the LGA published A Councillor's Guide to Cyber Security. The purpose of the document was to highlight the increasing dependency on IT within local authorities to deliver front line council services. Whilst most councillors would recognise this, a recent study undertaken by the Local Government Information Unit titled *Start of the Possible*, highlights that digital exclusion within the population, complex service design and poor Internet connectivity are of greater concern to elected members.

3.13. A Councillor's Guide to Cyber Security outlines the main cyber threats faced by councils and explains the steps that councils should be adopting to mitigate the associated risks. It encourages each councillor to understand and challenge the approach adopted by their own council to ensure that the confidentiality, integrity and availability of IT systems remain assured.

Questions to Ask

3.14. The guide poses a series of key questions that elected members are encouraged to ask of their councils. For the purposes of transparency, answers to these questions are provided in the following paragraphs.

Preventing an Attack

Leadership

3.15. Are your chief executive and leader aware of the issues of cyber security in your authority?

3.15.1. The chief executive officer chairs a monthly meeting of the ICT Architecture Board which is the governance body responsible for IT infrastructure, ICT security and Information Governance in the council.

3.15.2. The Leader is briefed on IT security matters during meetings with responsible officers.

3.16. Does a senior councillor have lead responsibility for cyber security?

3.16.1. Cyber security falls within the Executive Member portfolio of Councillor David Pasley.

3.17. Does a senior officer have lead responsibility for cyber security?

3.17.1. Cyber security falls within the remit of Mike Riggall who is the council's Information and ICT Security Manager. Mike reports to Richard Penska, Head of Support Services.

Governance

3.18. Is cyber security featured on your corporate risk register?

3.18.1. The threat from a cyber attack features on the corporate risk register. This broad risk specifically considers the threats associated with:

- a loss of IT systems resulting in the inability of the council to deliver services, and
- the loss of personal and sensitive personal data from the council's IT systems

3.19. Is cyber security part of your civil contingency plans?

3.19.1. The council incorporates the management of threats from cyber attack and any ensuing response as part of its involvement with the Local Resilience Forums.

3.20. Which, if any, board oversees cyber security activity and policy?

3.20.1. It is the role of the ICT Architecture Board to oversee activity and policy relating to cyber security. This board is chaired by the chief executive and includes senior managers from all directorates as well as representatives from the council's technical partners, Agilisys.

3.21. What data and information standards and protocols are in place?

3.21.1. The remote data centres which house the council's server estate and host most of its data, comply with the international information security standard, ISO27001.

Technology and information

3.22. What kind of processes and tools does your council have in place to prevent cyber attacks?

3.22.1. We get numerous requests each year through the Freedom of Information Act requesting specific details of the council's cyber security defences; we refuse to answer such enquiries for obvious reasons. We can however say that the council employs tools and techniques that would be expected of a local authority to secure its systems, including

- Firewalls
- Intrusion prevention and intrusion detection systems
- Malicious software detection
- Multi-layer anti-virus detection
- Secure configuration and change control procedures
- Controls on removeable media
- Restricted user privileges
- Centralised monitoring of security audit events
- Staff training and awareness

3.23. Where does your council receive information about potential threats from?

3.23.1. The council receives advice in relation to potential threats from the National Cyber Security Centre, the south west Warning, Advisory and Reporting Point as well as through a network of local contacts across authorities and other public sector organisations in the south west. In addition, Agilisys develops its own intelligence through the network of contacts arising from the management of other public and private sector accounts.

3.24. Is appropriate and proportionate training provided to all staff, including scenario exercises?

3.24.1. The authority has to balance the benefits realised by conducting readiness exercises against the disruption to services that this creates. For this reason, we have not conducted wholescale cyber attack exercises however the authority's business continuity plans have been tested following failures in essential utilities including electricity and communications.

3.24.2. Information Security features as a module in one of the mandatory staff training courses which officers are obliged to refresh every year.

What reporting mechanisms are in place for staff to report security concerns?

3.24.3. The ICT Portal provides a number of different scripts that can be used to report a variety of specific security concerns including e-mails suspected of containing malicious attachments or inappropriate content, lost devices, missing data files and unexpected behaviour of IT systems. Alternatively, security concerns that do not fit into a particular category can be raised using a generic form at any time.

3.24.4. The ICT service desk is contactable on 01275 884444 between 8am and 6pm Monday to Friday.

3.24.5. Concerns can also be raised directly with:

- Mike Riggall, Information & ICT Security Manager
- Paul Stickley, Head of ICT
- Karl Holden, Infrastructure Manager

4. CONSULTATION

Not relevant to this report.

5. FINANCIAL IMPLICATIONS

Not relevant to this report. ICT security is accommodated within the planned expenditure of existing capital and revenue budgets.

6. LEGAL POWERS AND IMPLICATIONS

Not relevant to this report.

7. RISK MANAGEMENT

Mitigating measures as detailed in the report.

8. EQUALITY IMPLICATIONS

There are no equality implications arising from this report. It has not been necessary to conduct an equality impact assessment.

9. CORPORATE IMPLICATIONS

The council operates a single IT strategy across all service areas; IT security is managed at a corporate level and security policy affects all officers, elected members and partner agencies equally.

10. OPTIONS CONSIDERED

Not relevant to this report.

AUTHOR

Mike Riggall
Information and ICT Security Manager
01934 426385
mike.riggall@n-somerset.gov.uk

APPENDICES

A Councillor's Guide to Cyber Security
Publisher: Local Government Association
https://www.local.gov.uk/councillors-guide-cyber-security

BACKGROUND PAPERS

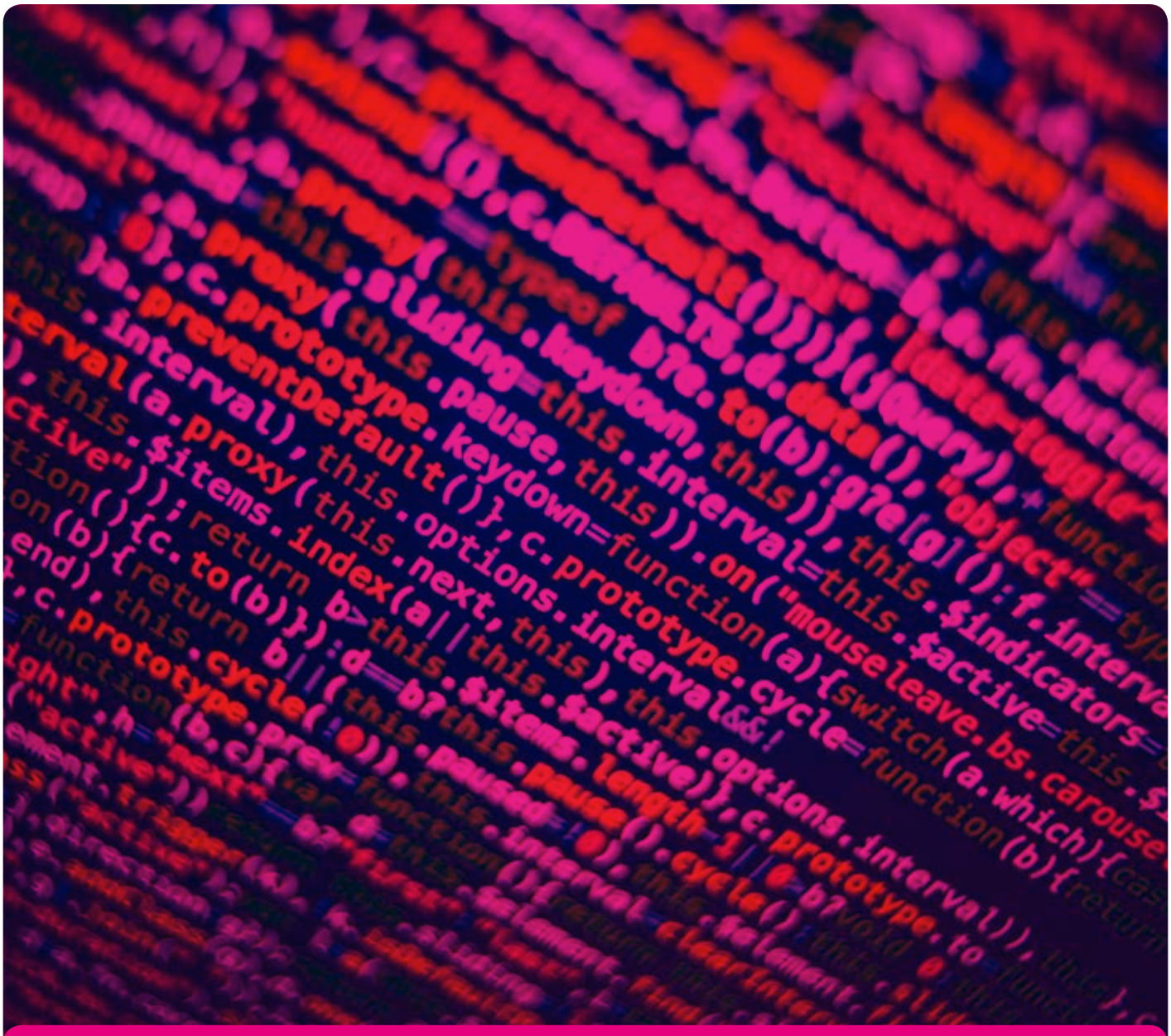
10 Steps to Cyber Security
Publisher: National Cyber Security Centre
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

10 Steps Executive Summary
https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/NCSC%2010%20Steps%20To%20Cyber%20Security%20NCSC.pdf

Start of the Possible
Publisher: Local Government Information Unit
https://www.lgiu.org.uk/report/start-of-the-possible/

Local Government Association

A councillor's guide to cyber security



Guidance

Why cyber security is important

The world we inhabit is changing rapidly. Nowadays, many people rely on the internet for everyday interactions and transactions. The landscape for local government is changing too. In the face of declining funding and shifting expectations, local decision makers need to find new and innovative ways to ensure the sustainability of services. Where councils are on their digital journey varies, but all have taken steps to make more local public services available digitally, move their workforce online, or collaborate in innovative ways with partner organisations – and this trend continues.

Councils are now using an increasing range of technology, from apps and the cloud, to different devices and gadgets.

Councillors carry out much of their council business online: corresponding with residents and local businesses, carrying out case work, and reviewing reports and papers for council meetings.

Protocols and guidance are in place around data handling and sharing, particularly for the sensitive or confidential. Most councils will also have a range of anti-virus tools in place across their systems, managed by their ICT teams. However, as we have seen with recent cyber attacks, including the WannaCry ransomware attack[1] those with criminal or hostile intent will continue to try to breach organisations' security to steal the data they hold and/or damage their systems.

Find out more
For examples of digitalisation across local government: www.local.gov.uk/digitalisation

Whilst the level of threat varies across councils, all possess information or infrastructure of interest to malicious cyber attackers. Councils should consider it a case of 'when' not 'if' a cyber attack will occur. Therefore, all need to continuously review, refresh and reinforce their approach to cyber security.

Not only is cyber security crucial to ensuring services are kept up and running, it is also vital to ensuring the public trust councils with their information. A cyber attack could have very serious consequences, both in terms of disrupting services – many of which serve the most vulnerable – and by damaging a council's reputation. Healthy cyber security is therefore key to the efficient and productive running of every council.

Information
The National Cyber Security Strategy describes 'cyber security' as: 'the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures'. www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

1 www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs

Types of threat

Cybercriminals and cybercrime

Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party, or using directly for criminal means.

Key tools and methods used by cybercriminals include:

- **malware** – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals
- **ransomware** – a kind of malware that locks victims out of their data or systems and only allows access once money is paid
- **phishing** – emails purporting to come from a public agency to extract sensitive information from members of the public.

Hacktivism

Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause. Hacktivist groups have successfully used distributed denial of service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already.

Councillor Joy Allen
Durham County Council

"Online fraud is the most common crime in the country, with one in 10 people falling victim. It's therefore vital that councils move with the times, and this means protecting ourselves from the real and growing threat presented by cyber attackers and investing in cyber security. Failing to do so could have serious and even catastrophic consequences for the services we run and the communities we serve."

Insiders

Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

Other threats include:

- **physical threats** – for example, fire or water damage to key network hubs or equipment
- **terrorists**
- **espionage**.

Councillor Ashley Mason
City of York Council

"We live in an increasingly digital world and our growing reliance on technology means ensuring its security is more important than ever. In York I arranged a workshop in partnership with the Police Cyber Crime Team to explore the issue of cyber security for local businesses and councillors."

What councils can do

Many councils are already investing in a range of measures to protect their systems and the data they hold from potential attacks.

These measures include:

- implementing firewalls and scanning services
- applying government's cyber security guidance, eg **10 Steps to Cyber Security** (www.ncsc.gov.uk/guidance/10-steps-cyber-security) or **Cyber Essentials** (www.cyberessentials.ncsc.gov.uk)
- introducing training for their workforce and elected members
- carrying out health checks, penetration tests and cyber resilience exercises to test their systems and processes, eg **Web Check** – a website configuration and vulnerability scanning service, developed with a number of public sector organisations including councils; this is free to use and available to all public sector organisations (www.ncsc.gov.uk/blog-post/web-check-helping-you-secure-your-public-sector-websites)
- meeting compliance regimes or Codes of Connection (CoCo), which require good cyber hygiene, to connect to government private networks, eg **Public Sector Network** (PSN) (www.gov.uk/government/groups/public-services-network) and the **Health and Social Care Network** (HSCN) (https://digital.nhs.uk/health-social-care-network)
- working with partners across the public sector through participation in **Cyber Security Information Sharing Partnerships** (CiSP) (www.ncsc.gov.uk/cisp), **Warning, Advice and Reporting Points** (WARPs) (www.ncsc.gov.uk/articles/what-warp) and **Local Resilience Forum** (LRFs) (www.gov.uk/government/publications/the-role-of-local-resilience-forums-a-reference-document) to protect their systems from, and put in place plans to respond to, cyber attacks
- putting plans in place to ensure there is the resilience to continue to provide services if and when a cyber attack occurs.

Find out more

Guidance for councils from the Ministry for Housing, Communities and Local Government: www.gov.uk/government/publications/understanding-local-cyber-resilience-a-guide-for-local-government-on-cyber-threats

The National Cyber Security Strategy: www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

The National Cyber Security Centre's glossary of key terms: www.ncsc.gov.uk/blog-post/download-latest-ncsc-glossary-infographic

Councillor Stephen Canning
Essex County Council

"Ensuring the security of our data and systems is integral to ensuring public trust in what we do as a council – our residents must trust us with their information if we are to use to it to transform and improve the services we deliver."

Key questions to ask in your council

Preventing an attack

Leadership

- Are your chief executive and leader aware of the issues of cyber security in your authority?
- Does a senior councillor have lead responsibility for cyber security?
- Does a senior officer have lead responsibility for cyber security?

Governance

- Is cyber security featured on your corporate risk register?
- Is cyber security part of your civil contingency plans?
- Which, if any, board oversees cyber security activity and policy?
- What data and information standards and protocols are in place?

Technology and information

- What kind of processes and tools does your council have in place to prevent cyber attacks?
- Where does your council receive information about potential threats from?
- Is appropriate and proportionate training provided to all staff, including scenario exercises?
- What reporting mechanisms are in place for staff to report security concerns?

Find out more
Find out what the LGA is doing around cyber security:
www.local.gov.uk/cyber-security

Response and recovery in the event of an attack

Leadership

- Is there an agreed lead senior councillor for overseeing the response, continuity and recovery?
- Is there an agreed lead senior officer for managing the response, continuity and recovery?
- Is there a designated lead spokesperson to communicate with staff and the public?

Governance

- Are business continuity plans in place? How regularly are these reviewed?
- Is there an agreed communications plan?
- Are all plans accessible and comprehensible in the event of an attack? For example, hard copies with clear guidance.

Technology and Information

- Does your council have the technical capability – both tools and staff – and processes in place to manage an attack? And is this tested regularly?
- Is there a pre-agreed prioritisation of which systems to restore or sustain? (Eg social care functions first, frontline customer service hubs, etc.)
- How is technical information on the threat or attack shared into national and local systems?

Partnerships

- Is there a Warning, Advice and Reporting Point (WARP) in the region and are you a member of it?

- How will the council work with partner agencies in the event of an attack? Eg accessing support, contingency plans, agreed processes and rules.

Sources

The National Cyber Security Strategy (Gov.uk): https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Understanding Local Cyber Resilience: A guide for local government on cyber threats and how to mitigate them (MHCLG): https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429190/Understanding_local_cyber_resilience.pdf

Local Digital Leadership (Solace): http://www.solace.org.uk/knowledge/reports_guides/local-digital-leadership-joint-position-paper

Glossary of key terms (NCSC): https://www.ncsc.gov.uk/blog-post/download-latest-ncsc-glossary-infographic

To find out more email:
productivity@local.gov.uk

Local Government Association
18 Smith Square
London SW1P 3HZ

Telephone 020 7664 3000
Fax 020 7664 3030
Email info@local.gov.uk
www.local.gov.uk

For a copy in Braille, larger print or audio,
please contact us on 020 7664 3000.
We consider requests on an individual basis.

REF: 11.106