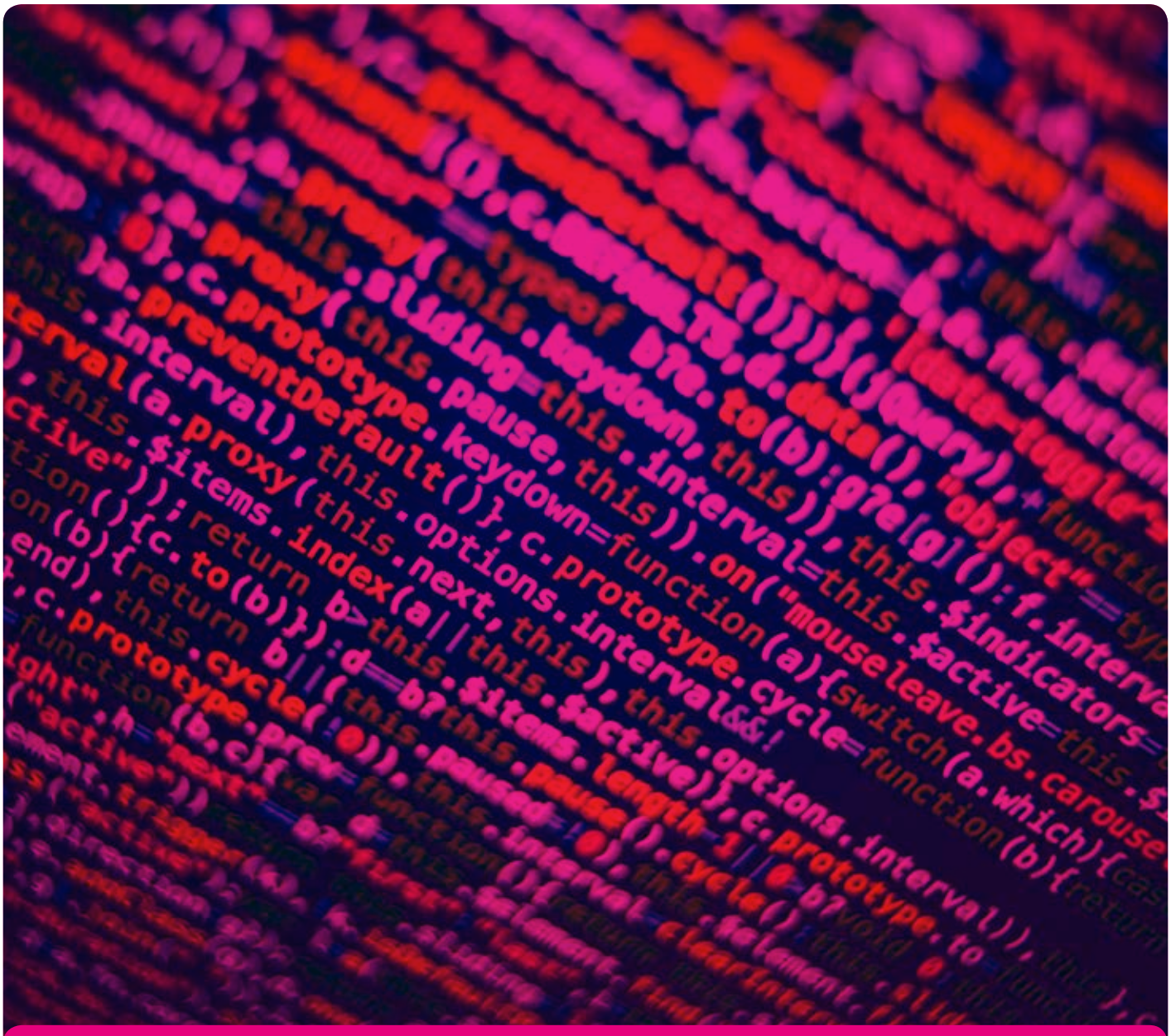
Local Government Association

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