

**Workshop E – With more services going online and increases in cyber-attack, have we got the necessary protection in place?**

Member Peer Conference

Wednesday 6 September 2017

Manchester Town Hall, Manchester

# **Workshop E – With more services going online and increases in cyber-attack, have we got the necessary protection in place?**

**Alison Whitney**, Deputy Director,  
National Cyber Security Centre

**Siobhan Coughlan**, Programme Manager,  
Local Government Association

Chair: **Cllr Peter Fleming**,  
Leader, Sevenoaks District Council

# Local Government Member Peers Conference

Alison Whitney  
National Cyber Security Centre

## We Live and Work in a Digital World

- Many of our residents and businesses expect to be able to carry out their business online with their council and wider government (and where we support those who cannot, we are inputting their information into our systems)
- As public sector employees and representatives, more of us work online both in the office and remotely – accessing different systems, using the internet to get information, etc.
- More of our systems are linked, both internally and externally - as we try join up related services for our residents

All of this makes us reliant on IT

## Why Should Local Government Care About Cyber Security?

- Councils hold sensitive personal data belonging to citizens and staff on line
- Councils provide essential services to citizens via the internet
- Councils are responsible for processes essential to the democracy of the UK that are IT-enabled
- Councils are dependent on IT to run their internal operations
- Councillors hold and share sensitive data relating to individuals who are seeking help
- Councils share sensitive information with partners, e.g. adult social care and health data

All of these services can be vulnerable to cyber threats

# The Threat

## Threat Actors:

- Cyber Criminals
- Hackers
- State Actors
- Cyber Terrorists

## Examples:

- August 2017 Nottinghamshire County Council fined by ICO for leaving vulnerable people's personal information exposed online
- June 2017 Glos CC fined by the ICO for having emails stolen by an attacker exploiting Heartbleed
- May 2017 Global Ransomware attack- WannaCry
- January 2017 Aberdeen City Council website hacked by 'Team System Dz'

## Peer Review - Key Lines of Enquiry and Cyber Security

### KLOE 4: Organisational Leadership and Governance

- Who is the accountable officer / risk owner for cyber security at a senior level within the authority?
- Does the council's civil contingency plan include cyber attacks?
- Is cyber on the risk register?
- Do business continuity and incident management plans recognise cyber security as an issue?
- Is cyber security considered in the council's LRF?

### KLOE 5: Capacity to Deliver

- How is cyber security integrated into technology-based projects?
- Is the authority a member of its regional WARP?
- Are the authority's IT or cyber security staff members of CiSP?
- Does the authority use NCSC's Active Cyber Defence Services? They are free at point of use!
- Is the authority's IT infrastructure and systems regularly patched?

## Sources of Further Information and Support

### Understanding Threats

- Read the weekly threat report on the NCSC website <https://www.ncsc.gov.uk/index/report>
- Join the Cyber Security Information Sharing Partnership <https://www.ncsc.gov.uk/cisp>

### Understanding vulnerabilities

- Sign up to the NCSC's free Web Check service <https://www.webcheck.service.ncsc.gov.uk/>

### Good cyber hygiene

- Does your authority live up to Cyber Essentials? <https://www.cyberaware.gov.uk/cyberessentials/>



<https://www.ncsc.gov.uk>